A thesis submitted for the Doctor of Philosophy degree (PhD) in Cyber Security

Analysis of key challenges in Security Operations Centre (SOC): A novel automated solution to reduce noisy events

By:

Kamal Zidan

University of Gloucestershire

Cyber and Technical Computing

School of Business, Computing and Social Sciences

May 28, 2025

Declaration

I declare that the work in this thesis was carried out in accordance with the regulations of the University of Gloucestershire and is original except where indicated by specific reference in the text. No part of the thesis has been submitted as part of any other academic award. The thesis has not been presented to any other education institution in the United Kingdom or overseas. Any views expressed in the thesis are those of the author and in no way represent those of the University.

Signed: Kamal Zidan

Date: 30/09/2024

DOI 10.46289/LEGU1581

Abstract

The changing current technology environment requires security measures to be in place for IT assets, including hardware, software and networks. These assets work collectively and collaboratively to provide services for orgnisations needs. Hence, security is required more than ever to increase the security posture of firms. Accordingly, cyber security threats are increasing rapidly, and due to this organisations are utilising Security Operations Centre (SOC) to monitor their assets and observe activities by collecting data about malicious events and behaviours. The main purpose of SOC is to defend assets by spotting potential malicious activities and respond to them. This thesis presents the result of an up-to-date literature review and interviews that have been conducted with 5 SOC specialists in the UK to understand the main challenges they face. From the research findings, various challenges are identified when working with SOC. Lack of automation, skills shortages, false positives, poor communication between analysts, and board-level implications are the most highlighted difficulties. Hence, experiments are conducted as part of the research to propose an automation solution to tackle some of these challenges. The developed automation model is trained and tested with datasets that include Windows security logs, Mac logs and Linux logs to classify and predict the occurrence of events based on their features and patterns. Various accuracy results occurred due to testing with different algorithms, including Decision Tree (DT), which produced the highest accuracy of 1 for Windows logs, 0.98 for Mac logs and 0.9425 for Linux logs. The automation solution is presented using interview method with 10 participants from a cyber security and software background for feedback retrieval. Thus, a grid matrix is also developed to evaluate the effectiveness of such an automation model as part of the feedback analysis. Overall, the developed automation solution can be used either by itself to automate logs based on their features and patterns or integrate it with tools such as Splunk to enhance and speed up the detection of events.

Dedication

This work is dedicated to the soul of my late father, may Almighty God bless his soul. The dedication also goes to my mother who constantly supported me throughout my life as well as my studies.

Acknowledgement

All thanks go to my first supervisor Dr. Ali Al-Sherbaz. Also, to my second supervisor and mentor Dr. Abu Alam who offered me all academic and professional support needed to finalise this dissertation. I do owe them for all the support, guidance and patience they provided to me throughout the research. I am also very grateful to all staff at University of Gloucestershire who offered me all help and assistance I needed throughout my study. Finally, I should admit that I am indebted to my family members, relatives, and friends who supported me to complete this academic endeavour successfully. I would like to thank them all for their help and encouraging comments.

Contents

List of Figures

List of Tables

List of Listings

List of Acronyms

ACK Acknowledgment

AI Artificial Intelligence

AMM Analysts Assessment Method

APTs Advanced Persistent Threats

APIs Application Programming Interfaces

ARPANET Advanced Research Project Agency Network

ASCII American Standard Code for Information Interchange

AT Activity Theory

AUC Area Under the Curve

AWS Amazon Web Services

CAB Change Advisory Cab

CERT Computer Emergency Response Team

CIA Confidentiality, Integrity, Availability

CISP Cyber Security Information Sharing Partnership

CLF Common Log Format

CSFC Cyber Security Fusion Centre

CSIRT Cyber Security Incident Response Team

CPU Central Processing Unit

CTI Cyber Threat Intelligence

DT Decision Tree

DMA Direct Memory Access

DNS Domain Name System

EDR Endpoint Detection and Response

ECLF Extended Common Log Format

ECAB Emergency Change Advisory Board

FCAPS Fault Configuration Administration Performance Security

FTP File Transfer Protocol

GPMC Group Policy Management Console

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IEC International Electrotechnical Commission

IDS Intrusion Detection System

IIS Internet Information Services

INSOC Integrated Network Security Operation Centre

IoC Indicator of Compromise

IoT Internet of Things

IP Internet Protocol

IPS Intrusion Prevention System

ISO International Organisation for Standardisation

ISP Internet Service Provider

IT Information Technology

ITSM IT Service Management

JSON JavaScript Object Notation

KPIs Key Performance Indicators

LR Logistic Regression

MAC Media Access Control

MCC Matthews Correlation Coefficient

MDR Managed Detection and Response

MITRE ATTCK Adversarial Tactics, Techniques, and Common Knowledge

ML Machine Learning

MLTK Machine Learning Toolkit

MS Microsoft

NCR Neighbourhood Cleaning Rule

NCSC National Cyber Security Centre

NIST National Institute of Standards and Technology

NMS Network Management System

NOC Network Operation Centre

NGFW Next Generation Firewalls

NHS National Health Service

OODA Observe, Orient, Detect and Adapt

OS Operating System

Pcap Packet Capture

PID Process Identifier

PPT People, Processes and Technologies

PPTGC People, Processes, Technologies, Governance and Compliance

RC Ridge Classifier

RF Random Forest

RST Reset

SANS SysAdmin, Audit, Network and Security

SDLC Software Development Life Cycle

SEC Simple Event Correlator

SOC Security Operations Centre

SIEM Security Information and Event Management

SLA Service Level Agreement

SME Small Medium Enterprises

SOAR Security Orchestration Automation and Response

SPL Splunk Processing Language

SQL Structured Query Language

SSH Secure Shell

SVMSMOTE Support Vector Machine Synthetic Minority Oversampling Technique

SYN Synchronise

TCP Transmission Control Protocol

TIP Threat Intelligence Platform

TISP Threat Intelligence Sharing Platform

TLS Transport Layer Security

UDP User Datagram Protocol

UK United Kingdom

URL Uniform Resource Locator

WWW World Wide Web

W3C World Wide Web Consortium

XML Extensible Markup Language

XSS Cross Site Scripting

Chapter One

Introduction

1 Introduction

1.1 Overview

Almost everyone nowadays has access to world wide web. Organisations and firms use internet to accomplish their day-to-day tasks. As well as individuals are also unable to complete their personal tasks without the adoption of internet. Interacting with internet without considering security aspects can cause harm and unwanted consequences. Hence, cyber security became an essential part that all individuals must be aware of to protect themselves and their companies from negative impact (Sharma et al., 2021). Due to the increasing number of hackers and exploiters, the focus of this study will be more specifically on cyber security aspect. Security Operations Centre (SOC) is an entity/body with several components that have features and abilities to monitor the network and provide protective measures. The motivation of this research is to investigate SOC and its implemented practices.

SOC is an organisational unit that is responsible for threat detection and risk mitigation. To enhance a firm security aspect, SOC combines processes, technologies and people (security analysts) via complex structure to prevent potential threats. SOC has always faced various challenges such as lack of experienced analysts, complexity of technology, inadequate level of threat detection automation process, and more importantly dealing with privacy regulations, as SOC tends to collect data for security purposes (Vielberth et al., 2020).

The main purpose of this research is to study SOC challenges by reviewing previous literature and conducting interviews with SOC specialists in UK. Also, to analyse different types of logs including Windows security, Mac and Linux logs using Python programming language in order to extract valuable information that can help in mitigating noisy events such as false positives. Another motivation is to propose an automation model that can be used by organisations to overcome the different highlighted aspects of SOC challenges.

This introduction chapter provides an overview of the topic alongside research questions. Research problems are also part of the chapter in order to justify how objectives are achieved based on the questions. An outline of the document is added to highlight the thesis structure.

1.2 Background

Organisations have started to realise the importance of having cyber security prevention measures and tools at workplace due to the growth of cyber security breaches. With the development of computers and networks, cybersecurity existed since 1970s (Eskelinen, 2022). Nevertheless, due to the expansion of threats level, it became a vital matter to be addressed. It deals with information and data traveling through an asset, perhaps emails and files. Inadequate physical or digital security can lead to data breaches. The need for digital security was recognised with the development of one of the first viruses called "Creeper". It was developed by Bob Thomas and had the capability to pass through the advanced research project agency network (ARPANET) as part of an experimental process. As shown in Figure 1.2.1 below, infected devices will display the phrase of "I'M THE CREEPER: CATCH ME IF YOU CAN" (Eskelinen, 2022).

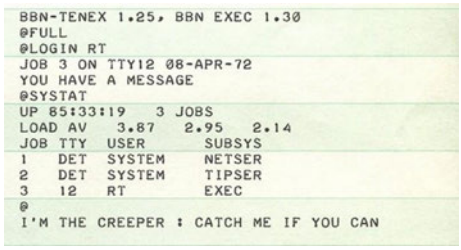


Figure 1.2.1: I'm The Creeper: Catch Me If You Can (Eskelinen, 2022)

Accordingly, Ray Tomlinson who found email system designed a program called "Reaper" which was able to detect and eliminate the virus Creeper. As a result, Reaper was classified as one of the first anti-virus software plus first self-replicated program which led to the development of the first computer worm. In fact, Reaper was created by the redesigning of Creeper. Hence, it is identified as self-replicating worm (Eskelinen, 2022).

Majid and Ariffi (2019) added that cyber-attacks have started in 1960s with the occurrence of hacking event on the frequency of phones systems. Moving towards 1970s to 90s the concept of cyber-attacks and their occurrence was to appreciate the technical skills that an actor has where courage and recognition are recognised. Referring to skills that an attacker held during the past, attacks performers used to be known as kiddies' scripts or amateur attackers. This due to their aim and goals in trying to show off the skills that they have to obtain more gratitude and appreciation. The growth

and forward moving of the world have shifted the aim of cyber-attacks into variety of reasons.

Nowadays, cyber-attacks have evolved where hackers tend to build malicious software to disrupt processes, steal data such as personal identifiable information (PII) and gain illegal access into systems (Majid and Ariffi, 2019). The expansion of the 2000s era has also changed the attackers' goal by moving into targeting large financial firms via the usage of sophisticated tools. Cyber crime is more organised than before where malicious events become sophisticated and focus on particular victims. It should be highlighted that the main purpose of the spread of cyber threats is to target large business firms, governmental organisations, and specific individuals (Majid and Ariffi, 2019)

Another example that explains the progress of cyber-attacks is a malware acknowledged as "ILOVEYOU" which occurred in 2000s period (Majid and Ariffi, 2019). The malware exploited vulnerabilities in windows operating systems where it had the ability to distribute through emails and caused a global financial loss of up to 9 billion American dollars in a month. Afterward, during 2003 a malware known as Slammer infected machines connected to networks. It expanded throughout memory processes causing network traffic to drop and paralysed systems of the affected target. For 5 days the financial loss was estimated of up to 1 billion American dollars (Majid and Ariffi, 2019).

Cyber security guarantee organisations assets and appliances. The implementation of cybersecurity frameworks protects information and equipment connected to the internet from cyber-attacks. Cyber security system is a combination of advanced tools to defend assets and appliances from unauthorised activities such as data theft, alteration, or deletion. With the evolving of sophisticated threats, advanced technologies can be developed to serve security measures of cyber security systems. Nevertheless, cyber security is a vital characteristic nowadays as it relies on technological computerisation which involves wide range of industries, accounts, and more different aspects (Nalanagula and Roy, 2022).

Majid and Ariffi (2019) stated that protective approaches in cyber security are split into two classes including internal and external aspects. For instance, if an incident occurred on a country level, the cyber crime that is performed by the actor will be judged based on particular law at the national

rank which might be a mechanism to reduce and deal with the pervasive of cyber threats. Nonetheless, corporations are required to take cyber security defensive actions throughout technical and non-technological methods to protect their assets and infrastructure. From a technological perspective the deployment of access control polices, intrusion prevention systems and firewall can be applied. On the other hand, a non-technical mechanism can be implemented via the non-disclosure agreement to prevent the loss of sensitive data.

Majid and Ariffi (2019) also included that organisations believe in the implementation of cyber security defensive measures to detect threats. Therefore, when an attack is identified then a response can be established to provide remedial actions. Adding to that, disciplinary acts can be applied in order to effect on the human factor to perform and obey laws. This is an effective way to reduce errors and vulnerabilities that can provide the attacker the advantage to exploit targets. A well implemented security infrastructure is required to deal with advanced cyber-attacks. A continuous risk assessment can be implemented to encounter threats via different steps such as creating policies, execute organised maintenance on frequent basis and practices to defend an IT infrastructure. A combination of risk assessment, various stages can be applied which are known as preventive, detection and correction to enhance the cyber security within an organisation.

Accordingly, the cyber security world is increasing rapidly and changing quickly where organisations are constantly facing cyber-attacks. Cyber security and information security are usually mentioned by individuals to refer to the same meaning. But in fact, both terms have different meanings. The CIA triangle (Confidentiality, Integrity and Availability) is associated with information security where these aspects must be considered by firms in order to protect electronic and hard-copy information. Hence, information security is often associated with physical security alongside the usage of technology as well. On the other hand, cyber security involves with the same approach as information security, but it is slightly different where it focuses on technological side such as: protecting electronic data alongside physical devices that are used to defend these data (Calder, 2020).

Additionally, Yin et al. (2020) defined information security as *"a process to prevent data in transmission, processing, or storage from being disclosed, imitated, tampered, repudiated, and stolen"*.

Cyber security can also be referred to techniques, polices and processes that are used to safeguard cyber space that involves individuals or organisations. It includes hardware, software and network systems connected with each other to keep information safe. Protecting enterprises data from malicious attacks such as illegal access or data theft is the main reason of why cyber security is founded since relying on computer systems has grown dramatically. Therefore, the main purpose of cyber security is to keep users in a safe environment and to respond to any potential threats at all times. It can be a challenging task for firms either government bodies or normal organisations where some of cyber threats target all types of data like financial or political information (Seemma et al., 2018).

SOC analysts are required to carry out some manual check in order to protect systems and networks. Some of the key areas is to troubleshoot, analyse and examine different network packets information. As part of the responsibilities, analysts are expected to have and acquire basic knowledge of diagnose and identify activities of network nodes in their organisation. For instance, checking for IP addresses and network connectivity can be carried out using various commands such as ipconfig, ipconfig / all, ping, netstat, tracert. Refer to below screenshots that show the outcome of the mentioned commands that are entered in a mixture of simulation environment and personal device where some of the IP addresses are made invisible to protect personal devices.

Ipconfig and ipconfig /all provide information associated with the physical address, IPv4 and IPV6 of the current working machine as depicted below in Figure 1.2.2.

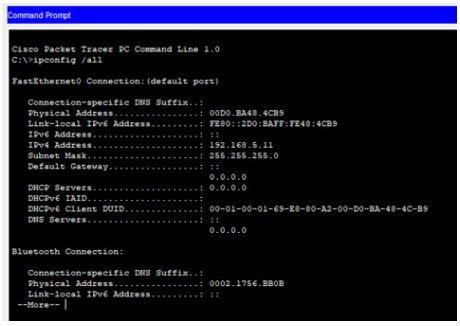


Figure 1.2.2: IP Configuration

Analysts and network defenders use ping command to check whether the destination/targeted machine is on the network or to troubleshoot further if an issue occurs in terms of connectivity. A successful ping result return with arrived packets and 0% loss as shown in Figure 1.2.3 below.

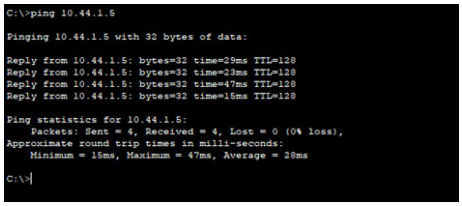


Figure 1.2.3: Address Ping

To retrieve the current statistics of a network, netstat command is useful where it displays information including TCP (Transmission Control Protocol) connections and ports that the machine is listening to as shown in Figure 1.2.4.

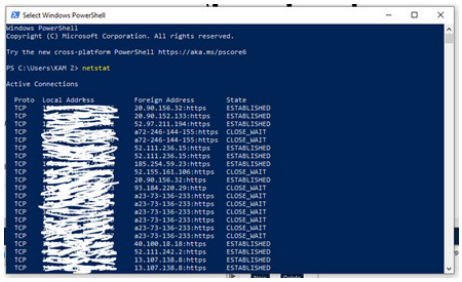


Figure 1.2.4: Network Stats

Analysts can analyse network traffic using various tools. In our experiments we used Wireshark to capture and analyse live data. Every packet on a network includes information about controls and users' data. Source, destination IP and MAC addresses are amongst the details found in the header part of such a packet. Refer to below screenshot 1.2.5 for further details. Therefore, SOC analysts are expected to know how to analyse these packets and retrieve useful information. There are three panes in Wireshark the top one includes the packet list where the middle one includes the details of any selected packets. The last pane includes packet information in byte format.

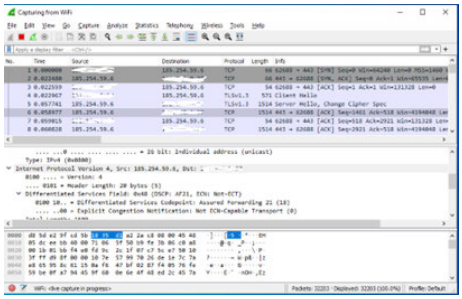


Figure 1.2.5: Packet Capture

SOC analysts and network administrators must be aware of the configuration of network security policy management and its implementation. In windows, there is a main tool to handle policies which is known as group policy management console that can assist administrators in dealing and managing with group policies throughout the firm.

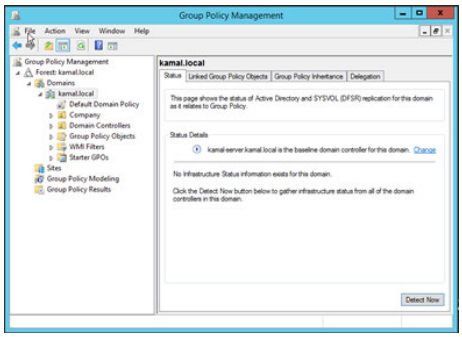


Figure 1.2.6: Group Policy Management

An analyst can configure policies according to their organisations perspectives. They can use Group Policy Management Console (GPMC) to administrate group policies across the enterprise. Below screenshot 1.2.7 provides an illustration of how accounts security policies are configured on domain/server and set to meet specific requirements. Accounts are enabled to meet complexity requirements and meet minimum password length as shown in the highlighted in the right pane of the group policy management editor.

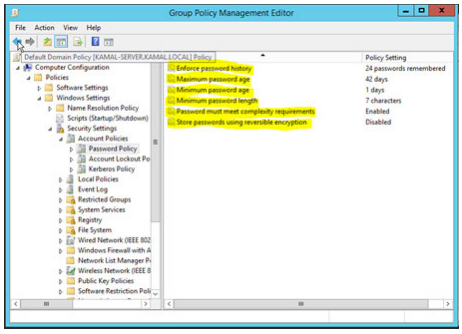


Figure 1.2.7: Group Policy Management Console

Based on an enterprise policy, there are unnecessary services that can be running behind the scenes where analysts must be aware of. These services can expose systems into the risk of being exploited by unauthorised users and attackers. Knowing what and how to disable and deactivate the spotted unnecessary services is essential for analysts in order to protect their systems. Below screenshot 1.2.8 is an example of services running on the system and how to start/stop a particular service in windows systems.

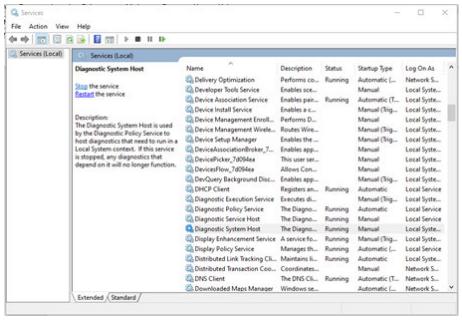


Figure 1.2.8: Services Details

Knowing the information associated with hardware and software configurations on an organisation network is essential to perform the required diagnoses when needed. Thus, Analysts and network defenders must be aware of these details and information to carry out their defensive tasks.

For instance, in windows, Microsoft System Information which is also known as MSInfo32 is able to collect information about devices and computers connected to the network. Auditing duties are conducted using this tool to know existing configurations on a particular windows system. Fig-

ure 1.2.9 below depicts MSInfo tool that shows system information including operating system name, version, and all other details.

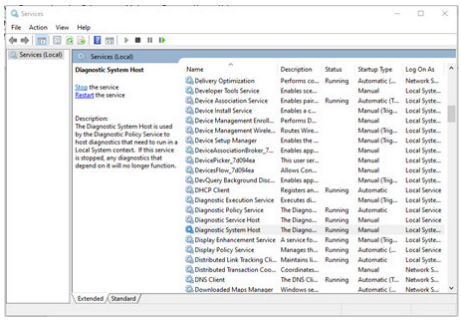


Figure 1.2.9: MS Information

Accordingly, on the left pane hardware, components and software sections can be expanded to view subcategories in more detail. Devices that share the same resources can be seen in conflicts/sharing sub section as shown in Figure 1.2.10 below. Also, DMA which is associated with Direct Memory Access that transmit data amongst system memory and hardware devices by avoiding passing throughout the CPU can be seen. Meanwhile components section includes information related to multimedia that are associated with appliances such as audio and video codecs. In contrast, installed drivers and their performance can be found in software section as highlighted in Figure 1.2.11 below.

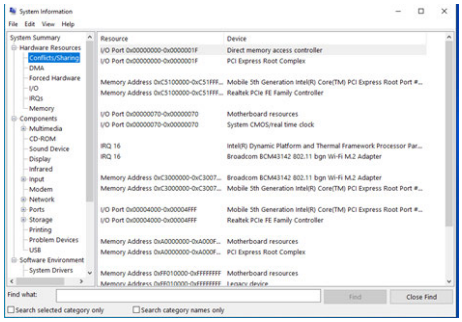


Figure 1.2.10: System Information

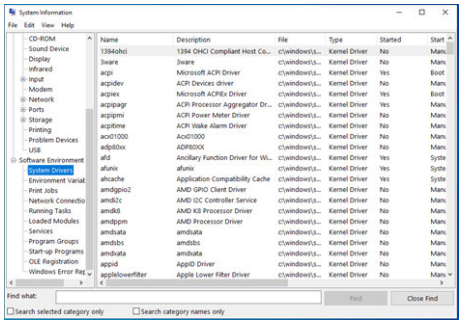


Figure 1.2.11: System Drivers

Based on organisation policy security analysts have the ability to block or allow traffic from or to the organisation network by setting specific rules using firewall software. It is a tool in Microsoft windows that assist in filtering inbound and outbound packets traffic. Knowing how to configure inbound-/outbound traffic rules is an essential task that network administrators must be aware of. This helps in protecting systems from being exploited by malicious traffic. Figure 1.2.12 below is an illustration of windows defender firewall where it shows the firewall is turned on plus additional information including configured incoming connections and active networks.

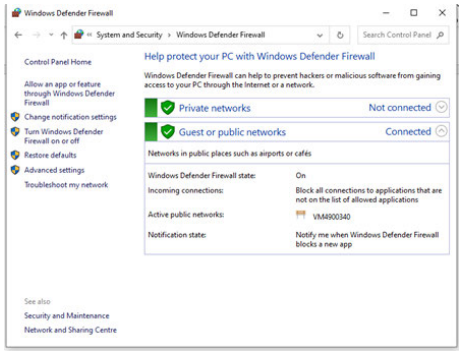


Figure 1.2.12: Firewall

By clicking on advanced settings on left pane, inbound/outbound rules can be configured as shown below in Figure 1.2.13.

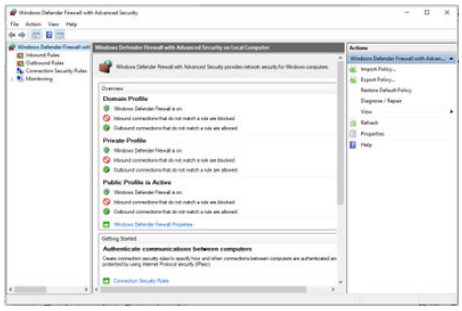


Figure 1.2.13: Inbound\Outbound Rules

In our experiment we created both inbound and outbound rules to block port 80 connections which is related to HTTP (Hypertext Transfer Protocol) connections that is responsible of transmitting unsecure http requests and responses.

Following the steps that are shown in below 1.2.14 - 1.2.18 screenshots an inbound rule is created to block connection from port 80 (HTTP). However, we have followed the same steps in creating the same outbound rule.

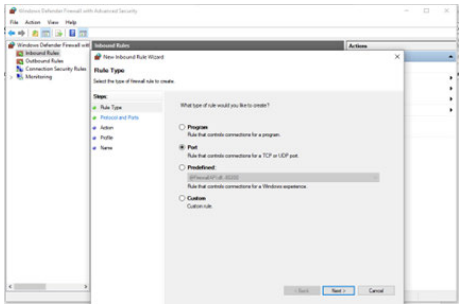


Figure 1.2.14: Inbound Rule Port Block

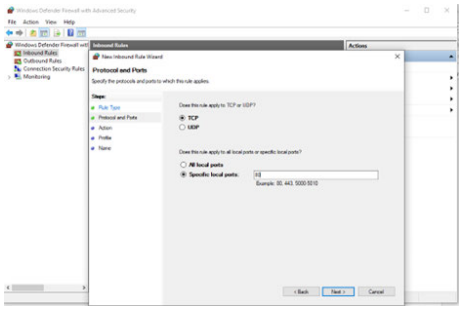


Figure 1.2.15: Specific Port Selection

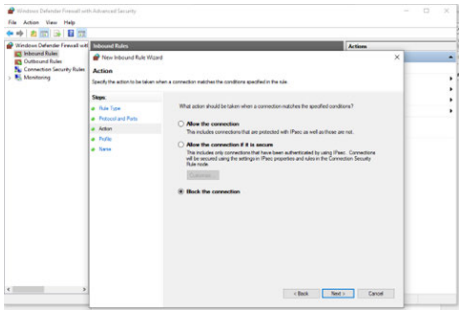


Figure 1.2.16: Action Details

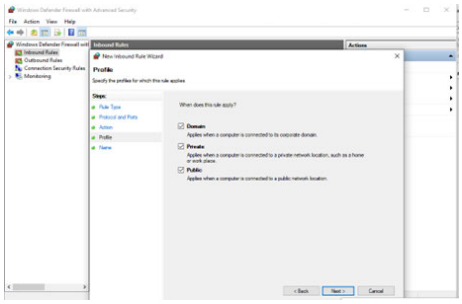


Figure 1.2.17: Profile Details

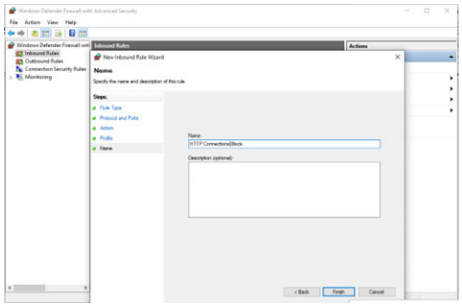


Figure 1.2.18: Inbound Rule Name

By finishing creating rules and assign appropriate names to them as shown above, below Figures 1.2.19 - 1.2.20 depict the created rules as highlighted in yellow with their given names.

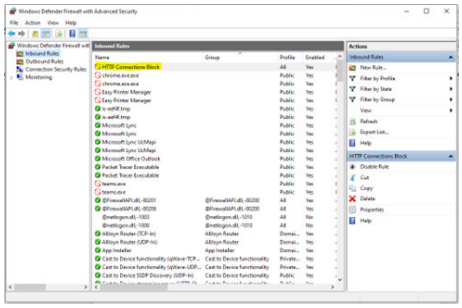


Figure 1.2.19: Inbound Rules

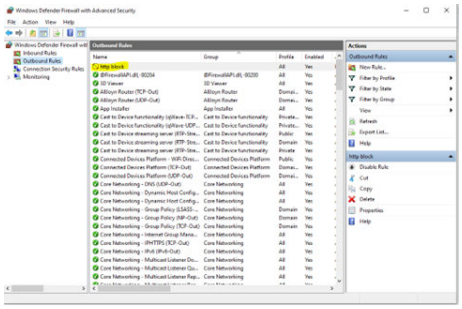


Figure 1.2.20: Outbound Rules

Based on the created rules HTTP connections are blocked. Therefore, we tested them by trying to access google translate using HTTP at the beginning of URL. As shown below in Figure 1.2.21 the connection is blocked and accesses are prevented.

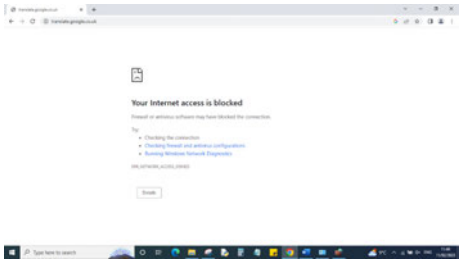


Figure 1.2.21: HTTP Google Translate

In contrast using Hypertext Transfer Protocol Secure (HTTPS) permits the access to the page and the request is successful as shown below in Figure 1.2.22. This is because inbound/outbound rules that are associated with HTTPS were not created where HTTPS port number is identified with 443 unlike HTTP port number 80.

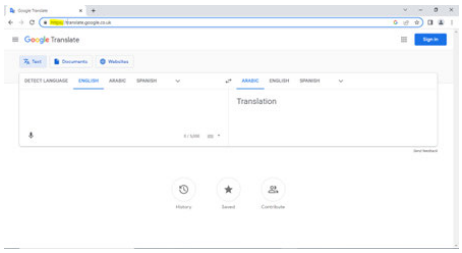


Figure 1.2.22: HTTPS Google Translate

Furthermore, evidence of cyber security threats conducted by the researcher. EC-Council environment is used for performing various tasks on virtual labs to avoid and prevent any data protection regulations impacts or confidentiality breaches. Threats experiments are carried out to support the background of the research. They help in understanding some of the key attacks methods more clearly.

For instance, SOC analysts must be aware of attacks such as SQL injection. It is one of the most known vulnerabilities that target websites and application level. It can lead to unauthorised access to sensitive information, modifying, stealing, or deleting data from databases. Arbitrary SQL queries are executed to carry out such an attack (Sadeghian et al., 2013). The following Figure 1.2.23 is an example of vulnerable website that shows orders list under the name of bob.

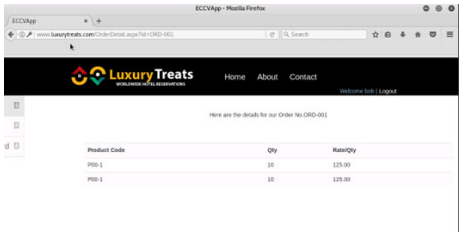


Figure 1.2.23: Vulnerable Website

When adding ' or 1=1;– to the end of the URL more data about orders are disclosed as shown in the below Figure 1.2.24.

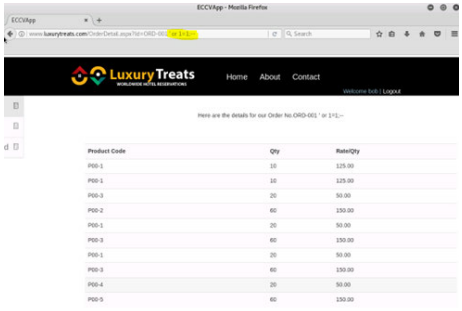


Figure 1.2.24: SQL Injection

This entail that the SQL attack is carried out successfully using the mentioned statement. Injecting ' or 1=1;– to URL makes the condition always true which permit access to unauthorised data. The carried-out experiment is a simple one and exploiters use various types of SQL injections techniques to bypass validation. Any occurrence of SQL injection must be treated as indicator of compromise. Therefore, tools like sqlmap can also be utilised to carry out SQL injection. Analysts are supposed to understand these threats and developers as well to make their applications and network more secure against these types of attacks (Sadeghian et al., 2013).

Another type of application-level threat is Cross Site Scripting (XSS). SOC analysts must recognise these types of attacks to protect their organisations websites from such attacks. The World Wide Web (WWW) includes various types of technologies such as client side and server side. Web applications are developed on these technologies to provide facilities to users. A lot of websites are exposed to XSS attacks due to improper validation where

an attacker manages to inject JavaScript or any other type of executable code on the client side. In fact, web applications are becoming the main platform of providing data and services to users over the internet. Hence, attackers are targeting web application due to the valuable and precious information they hold (Gupta and Gupta, 2017).

Figure 1.2.25 below depicts JavaScript code alert message that is typed into comment box to test whether the website is vulnerable to XSS or not.

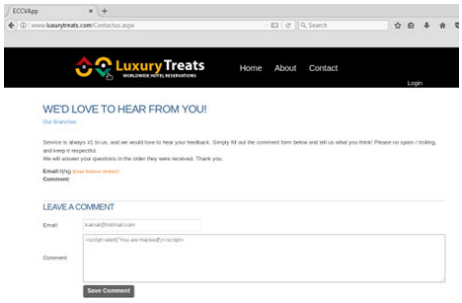


Figure 1.2.25: Cross Site Scripting

By clicking on save comment an alert box appears on the browser as illustrated below in figure 1.2.26 which indicates the website is vulnerable to XSS.

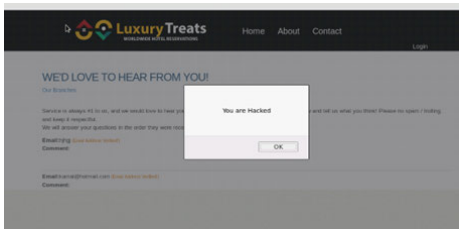


Figure 1.2.26: Cross Site Scripting XSS

Any occurrence of XSS must be treated as Indicator of Comprise (IoC) and it is vital to be picked up by SOC analysts to investigate. The ongoing existence and development of modern web applications expose them to be high targeted. Developers are required to implement best defensive measures by using proper validation and code practices (Gupta and Gupta, 2017). Accordingly, SOC provides defensive layer against these types of attacks in the absence of secure practices implementation. The above example is a sim-

ple one but can lead to more sophisticated attack where malicious link can be sent within the executed code <script>alert("You are Hacked")</script >to a user using phishing technique by convincing them that the link is received from a genuine website.

Network level threats are also part of the technique's attackers tend to execute. Any occurrence of such an attack is treated as indicator of compromise. SOC analysts are required to detect these types of attacks at early phases to avoid any upcoming threats. There are several techniques can be used to scan networks, but in this lab, we used SYN and UDP scans. According to Zhang et al. (2015) SYN scan sends packets to the targeted machine port to recognise whether that port is open or closed. Pros of this scan type that SYN does not require to conduct full TCP scan. In contrast, the disadvantages of it that SYN scanner uses its own IP address to send packets where firewalls are able to detect and prevent them.

An IP address of a remote machine that is hosted on virtual lab is scanned to show the outcome of it. The address is 10.10.10.12 and as shown in Figure 1.2.27 below a SYN scan is conducted on the targeted machine using nmap tool in Linux to retrieve services information that are running on it.

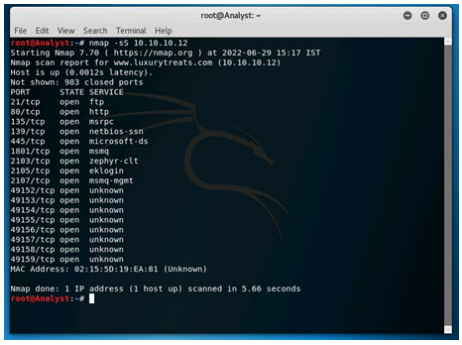


Figure 1.2.27: Network SYN Scan

An attacker can retrieve valuable information from scanning networks such as running services, their states, and open/closed ports. Another performed scan is UDP scan where 137 port is shown as opened in Figure 1.2.28 below. An open port means that an attacker can use it for further activities. Thus, intrusion detection systems and firewalls can be configured in advanced where network scanning attempts can be found in logs. By

analysing these logs SOC analysts are able to investigate further.

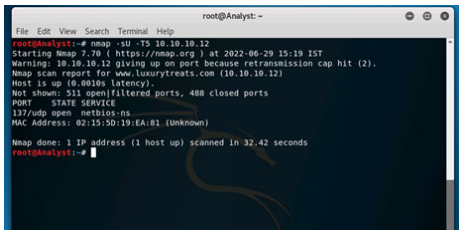


Figure 1.2.28: Network UDP Scan

After identifying open ports an attacker can conduct brute force attacks on the target machine to gain unauthorised access. Brute force is a type of host level threats where combinations of various usernames and passwords are entered until the correct combination is figured out. There are different automated tools used to carry out brute force. Stiawan et al. (2019) added, several devices use File Transfer Protocol (FTP) to transfer data over network. FTP is often setup incorrectly which leaves devices exposed to high risk of attacks. Thus, Hydra is the tool being used by the researcher for testing purposes. The command that is typed to carry out the test is shown below in Figure 1.2.29 in first line considering FTP port is open. Userlist.txt and pass.txt are files contain various usernames and passwords where Hydra is the brute force cracking tool that try different sequences.

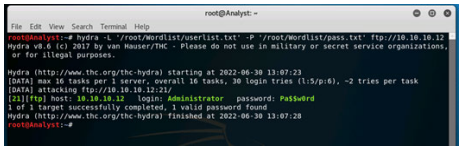


Figure 1.2.29: Hydra Tool

The occurrence of failed login attempts from the same IP address then successful login is indicator of compromise and SOC analysts must be aware of it. For instance, in windows security event logs, attempts can be stored for further investigations by analysts. There are tools SOC analysts can use to monitor network activities. Packets that are generated from network traffic are captured via these tools for the purpose of analysing networks for any indicators of compromise. Wireshark is the tool that is used for analysing the sample captured data on virtual lab. According to Zhang et al. (2015) an attacker can scan the network to check whether a port is open or closed

via using TCP scan or TCP half scan attempt. SYN packet can be sent to the target then if the port is open SYN + ACK is replied back.

Otherwise, RST packet is returned which indicates the port is closed. TCP SYN scan attempt is one of the common scans attempts where the scanner can build some knowledge around the status of a returned port. As any techniques it has disadvantages of which the scanner machine will use its own IP address where rules can be set up in firewall to prevent any future attempts by the same IP address.

In contrast, conducting SYN + ACK scan usually attempted to detect if there are any firewalls where RST reply means that the target machine is alive. As depicted in Figure 1.2.30 below SYN packets are sent to the target machine which has the IP address of 10.10.10.12 and SYN + ACK packets are replied back via different open ports such as 139 & 135. Any occurrence of TCP half scan or any other network scans are treated as indicator of compromise and must be further investigated.

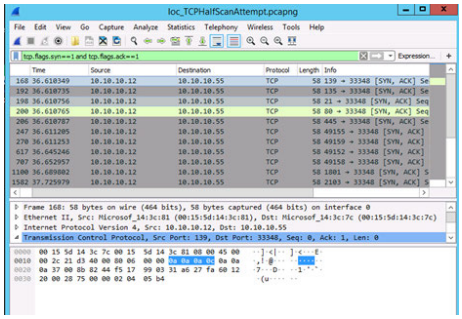


Figure 1.2.30: Wireshark

Additionally, monitoring and logging logs can be tracked in windows operating systems. Different events and activities are traced throughout these logs. In windows event viewer the recorded events are classified as application, security, setup, system and forwarded events. Detecting attacks and understand flaws and anomalies can be achieved throughout log files which indicate how important they can be. Hence, SOC analysts also expected to be aware of windows operating systems mechanism and the location of where these types of logs are stored.

For example, failed and successful logins to systems are captured via these logs. Any occurrence of logs that include failed login attempts must

be treated as indicator of compromise. Berlin et al. (2015) added that relying only on anti viruses and IDS tools can be ineffective in detecting more sophisticated threats. As a result, organisations are moving towards utilising endpoint instruments to have more in-depth picture of the enterprise low level events, but not all enterprises are able to maintain the required resources for the implementation for such detection tools. Therefore, authors approved the usage of windows audit logs where they can provide sufficient information to robust the detection process of malicious events.

Figure 1.2.31 below is the event viewer tool in windows that is used by the researcher personal device. As depicted, there are loads of event logs that can be analysed. By clicking on each event, information, and details in regards of it are displayed for further investigation.

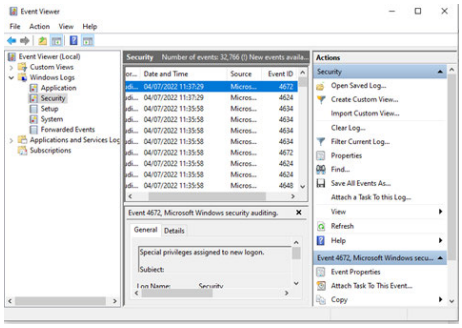


Figure 1.2.31: Event Viewer

Also, the stored logs in windows can be found in the following location path C:\WINDOWS\System32\winevt\Logs as shown in below Figure 1.2.32.

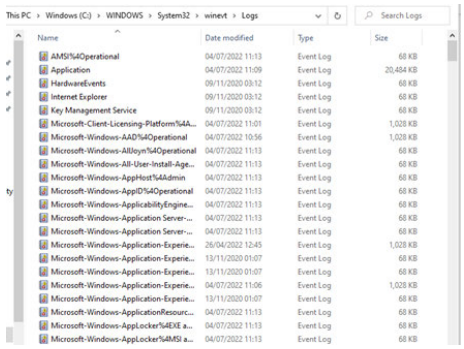


Figure 1.2.32: Windows Logs

Not all events logs are required to be invigilated. However, the monitored logs can be different depending on the operating system as windows logs are differ from Linux machines etc. For windows machines Mutemwa et al. (2018) emphasised on the importance of monitoring windows security logs on domain controller. Windows application logs are also suggested to be part of the monitoring process which assist analysts with information in regards of installation or uninstalling of applications. Applications logs are useful as they allow SIEMs to gather data to monitor particular servers including Domain Name Sever (DNS), databases and anti-viruses. In contrast, Linux systems and applications store logs that can be found in the directory of /var/log/. Protecting the integrity of these logs can be encapsulated with specific access permissions depending on the user privileges.

Moreover, windows include different services such as Internet Information Services (IIS) manager tool which is a web server that help in detecting any anomalies behaviours. SOC analysts are able to retrieve useful insights in regards of services and contents by monitoring IIS logs. For instance, IIS logs provide details of the user who visited the website and the content that have been viewed. IIS also offers an easy and secure platform to host websites and other applications. Nevertheless, information can be shared on the internet amongst users. Enhancing web security posture and isolating applications automatically are some of the key benefits of IIS. The speed of a website can also be increased by the dynamic built in cashing functions. Technically, administrators use IIS web server to manager various websites and applications. Hence, SOC analysts are expected to use it as part of their role to administer websites. They can also use it for allowing or prohibiting websites owners to upload and download files using

file transfer protocol. Isolating websites is a feature that can also be used by preventing interference between two websites on the server. Configuring web applications that are developed in different technologies such as PHP and automating administration tasks using windows PowerShell can also be achieved in IIS server. Overall, IIS reduce security risks on an organisation website (Microsoft, 2016).

In Figure 1.2.33 below IIS manager is used in EC-Council virtual lab, as depicted the vulnerable luxury treats website is given the ID of 2 in IIS windows2012 web server.

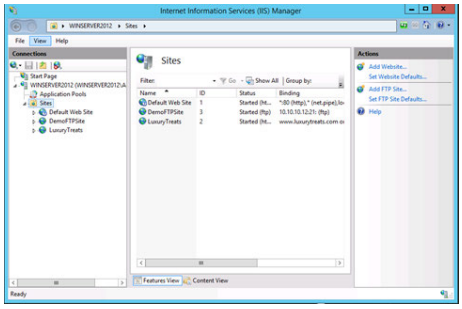


Figure 1.2.33: Internet Information Services

SQL injection attack is conducted on the vulnerable website via adding ‘ or 1=1;– to the end of URL. In logging tab of the website logs can be found in the following path %SystemDrive%\inetpub\logs\LogFiles as shown in below Figure 1.2.34.

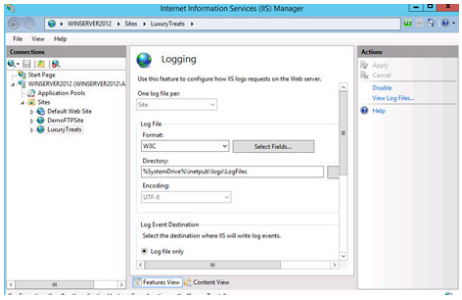


Figure 1.2.34: Internet Information Services (IIS)

By navigating to the mentioned path, log files then can be investigated as shown in below Figure 1.2.35 which indicate that ‘ or 1=1;– is being

added to the URL alongside other information of the user who did it and IP addresses.

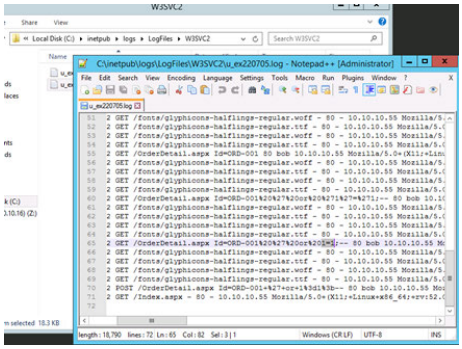


Figure 1.2.35: Log File

With the large amount of generated data, attackers often act like genuine users where they try to encapsulate their malicious activities within data. The in-place security mechanisms might not be able to detect them due to various reasons such as lack of sophisticated detection abilities. Organisations are required to have more advanced tools to detect and differentiate genuine behaviours from anomalies to protect their infrastructure. Intrusions detection systems or intrusion prevention systems are the type of tools SOC analysts are suggested to use as well as part of the SOC umbrella. There are several IDSs either commercial or open source (Shah and Issac, 2018).

Accordingly, an IDS is only sufficient enough if it has the ability to distinguish between anomalies and legitimate traffic. Figure 1.2.36 below is an illustration of how packets are collected from the network then analysed through the process set by Snort IDS which is an open-source model. Having a solid IDS helps in reducing the number of false positive alerts as well as detecting threats (Shah and Issac, 2018).

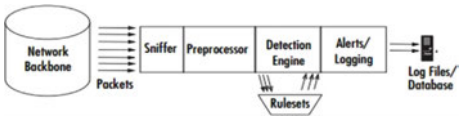


Figure 1.2.36: Snort IDS Architecture (Shah and Issac, 2018)

For the EC-Council virtual lab, Snort is used which is an IDS tool that

can be implemented with the required detection rules to analyse and detect legitimate and nonalignment behaviours. Snort is set up to detect different activities such as scanning the network using Linux Nmap tool in terminal. As shown in Figure 1.2.37 below, logs are collected and stored in alert.ids file then it is analysed to provide information about the scan's attempts. In fact, any occurrence of network scans attempts must be treated as indicator of compromise and analysts must proceed further.

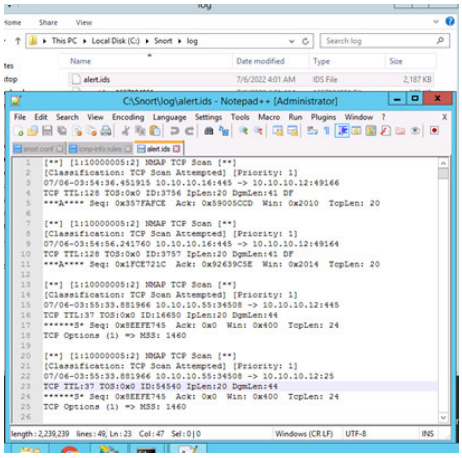


Figure 1.2.37: Alert.ids File

Collecting and gathering these number of logs from different devices can be very difficult task to achieve. Splunk is a SOC tool where all logs can be gathered and sent to a centralised location for further investigation and analysis. More attacks are conducted on the targeted machine to produce logs in Splunk which are displayed next. Nevertheless, after conducting a brute force attack on the target machine 10.10.10.12 the user was able to login using ftp command as shown in Figure 1.2.38 below:

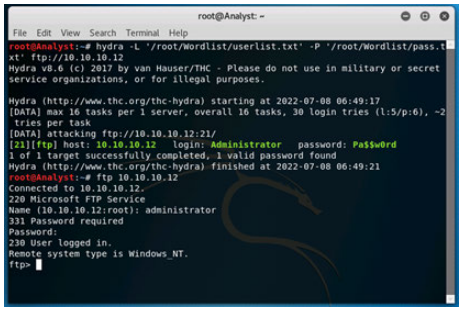


Figure 1.2.38: FTP Login

As added at the beginning the website is vulnerable to SQL injection. Hence, sqlmap tool is used to scan the target to retrieve more information as shown in Figure 1.2.39.

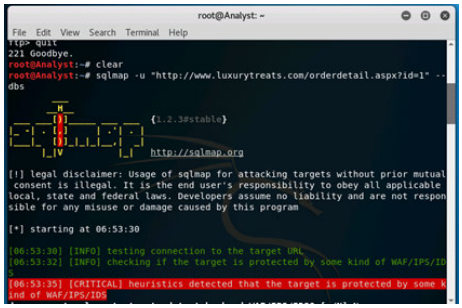


Figure 1.2.39: SQLmap

The results in Figure 1.2.40 shows that there are 8 different available databases that are connected to the website.

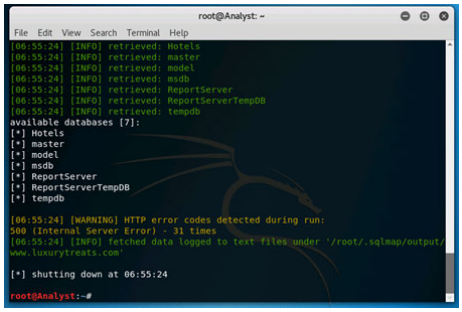


Figure 1.2.40: Databases

The hotels database then scanned using sqlmap as well to retrieve tables names that it includes as depicted in Figure 1.2.41 below.

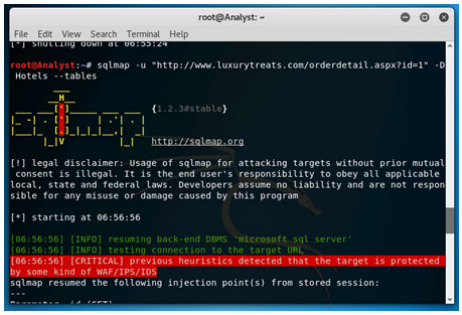


Figure 1.2.41: Hotel Database

Several tables are retrieved in Figures 1.2.42 below, and next step was to extract the columns inside customerlogin table to get into users' credentials as displayed in Figures 1.2.43 - 1.2.44 below.

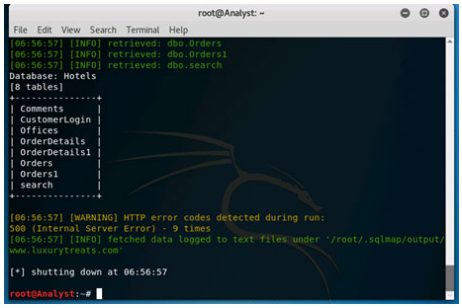


Figure 1.2.42: Database Tables

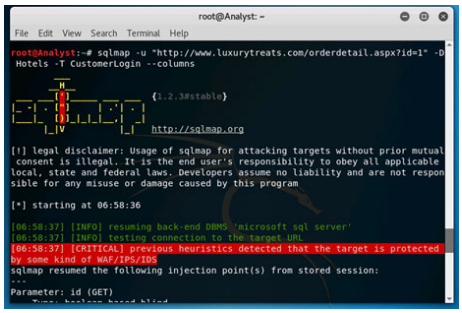


Figure 1.2.43: Columns Extraction

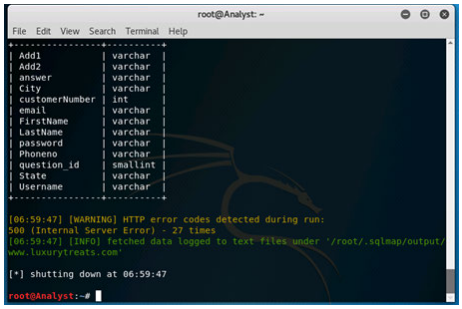


Figure 1.2.44: Columns Details

After retrieving columns details then customerlogin table is dumped using –dump flag that is added to the end of sqlmap command as typed in Figure 1.2.45.

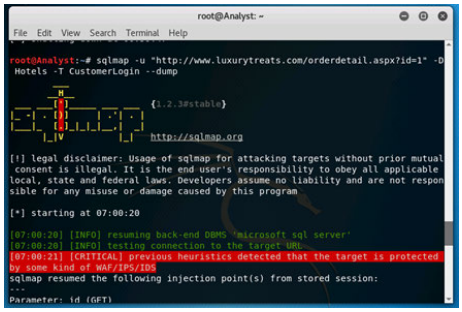


Figure 1.2.45: Dumping Function

Users' details alongside their usernames and passwords are extracted as part of the process which shows how an attacker can take an advantage of sql injection vulnerability in a website.

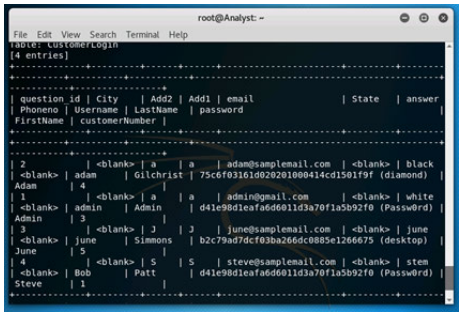


Figure 1.2.46: Users Details

Accordingly, the previous steps are conducted to display how these attempts can be logged in a centralised location such as Splunk to detect and take further protection actions. After configuring Splunk in EC-Council virtual lab, the above attempts are logged into the platform as shown in Figures 1.2.47 - 1.2.53 below. Details of the attempted network scans, sqlmap scans, the injected sql query and other malicious attempts are displayed and further investigations can be taken to gather as much details as SOC analyst can about the nature of such a threat.

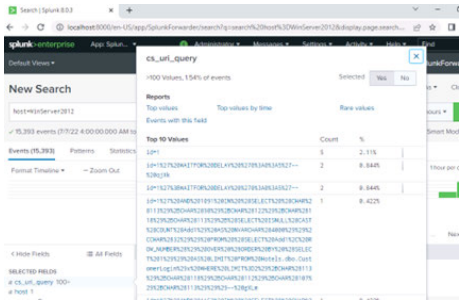


Figure 1.2.47: Splunk I

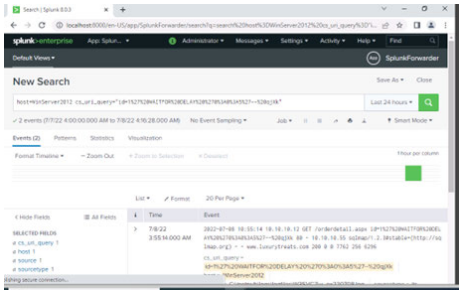


Figure 1.2.48: Splunk II

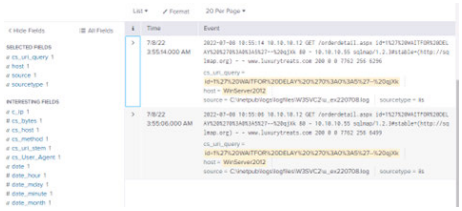


Figure 1.2.49: Splunk III

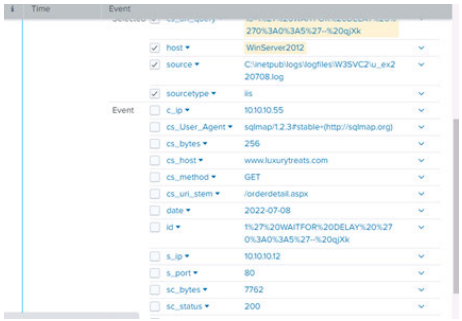


Figure 1.2.50: Splunk IV

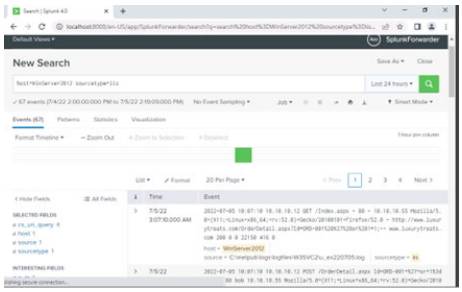


Figure 1.2.51: Splunk V

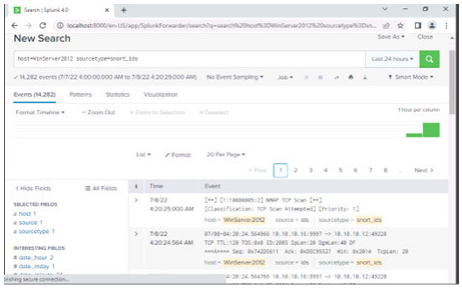


Figure 1.2.52: Splunk VI

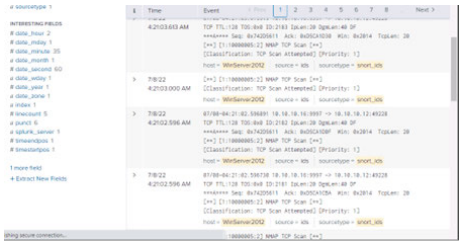


Figure 1.2.53: Splunk VII

SOC provides an enhanced protection layer where it combines various cyber security defensive tools to respond to threats and UK National Health Service (NHS) attack in 2017 is an example of the breaches that indicated the need of effective threat mitigation techniques (Ghafur et al., 2019). Therefore, the background of the study is to assess SOC and examine its challenges to propose the required solutions that will help in mitigating their occurrences. (Agyepong et al., 2020a).

1.3 Research Problem

Identifying research gaps is essential to propose solutions to the highlighted problems. The solutions are part of the research contributions that the researcher delivered. As mentioned, the motivation of this thesis is to examine SOC challenges and to highlight the importance of logs/alerts in mitigating false positives that are generated. For this research there are different tools that are used for studying SOC, but the main focus is on python automation process where some of the experiments are carried out to automate logs.

The technical aspect of experiments is not highlighted in many research

papers based on conducted literature by the researcher. Hence, this supported the theoretical part of the research. Interviews are conducted as part of the research to generate primary data and theoretical findings can be utilised as common challenges by organisations to propose the best effective measures based on their requirements. More importantly, the proposed automation model is the main contribution in automating logs and flag them based on their specific patterns. As well, feedback on the model is retrieved from interviews conducted with cyber security and software developers to evaluate the model.

This thesis includes the required recommended solutions to avoid challenges and maintain quality usage of SOC. Attacks samples experiments are carried out using different virtual labs to complement the research and understand how they could occur and how analysts are able to create rules for them to be figured out quickly.

1.4 Research Questions

- What are the main challenges faced by SOC and how to automate processes for effective analysis of threat detection?
- How can automation minimise false positives which can distract SOC analysts from analysing real security threat?
- How to evaluate that an automation solution is effective for threat detection?

1.5 Aims and Objectives

A lot of organisations are still experiencing data breaches and threats which cause unwanted consequences. The aim of this research is to investigate SOC challenges with focusing on mitigating noisy events such as false positives or false negatives. Explaining how automation can be applied to reduce risks. The objectives of the research as follow:

- To investigate key challenges within SOC via literature and interviews.
- To improve exiting techniques and implement new techniques to reduce the number of false positives and negatives using automation.
- To evaluate the efficiency of the implemented automation techniques based on preset criteria.

1.6 Thesis Outline

Thematically, the outline provides a background of SOC alongside the importance of applying automation to detect threats effectively. Threat detection is included as part of Machine Learning (ML) to highlight how ML can be applied to detect risks. Data collection is mentioned and followed by ethical concerns that might arise which ensure the researcher is prepared in advance for any consequences. This thesis consists of the following chapters:

Chapter One: Introduces the background of the research. It also defines the research aims, identifies its objectives and outlines the research questions.

Chapter Two: Provides a literature review relevant to the research topic. The research gap is identified as part of SOC challenges to lead into achieving the research aims and objectives.

Chapter Three: Includes the process of collecting relevant data. Research methods and methodology are outlined, explained and justified.

Chapter Four: Includes findings from interviews. It also incorporates the analysis and discussion of the interviews findings and literature in regards of SOC challenges.

Chapter Five: Contains experiments carried out alongside the developed automation solution.

Chapter Six: Sums up the research. Conclusion, recommendations, limitations, and future research are outlined in this chapter.

Bibliography: Comprises the sources and references used for this research.

Appendices: Includes the details of the papers that have been published as part of this research.

Chapter Two

Literature Review

2 Literature Review

2.1 Introduction

This chapter includes information about SOC. An up-to-date literature is reviewed to gather the required data from trusted published sources. The architecture design of SOC is explained alongside its implementation requirements. Automation and Machine learning (ML) are added to highlight the importance of them in minimising fake alerts. Also, to understand how events correlations can help in defining the relationships amongst security events. Additionally, inefficiencies and challenges that impact on SOC effectiveness are mentioned to develop future recommendations.

2.2 Security Operations Centre (SOC)

SOC is a unit that can be used for events detection and responding to incidents associated with cyber security threats via monitoring, detecting, examining and reporting on anomalies. Well-known, unknown and new activities are part of SOC tasks that organisations looking to have in their security environment. There are variety of reasons firms and organisations must utilise SOC such as situations awareness including hardware and software assets. Controlling vulnerabilities, threat detection and prevention where SOC provides the ability to detect when an unauthorised individual has breached a specific asset plus its capabilities of identifying vulnerabilities on the monitored estates (Mutemwa et al., 2018).

SOC is able to monitor the events that are logged on the network to take protective actions when needed. In fact, cyber-attacks are becoming more complex and causing major disruptions to their targets. Planned cyber crimes are being conducted via sophisticated tools. Hence, the need of advanced centres that can process large amount of information is required (Alharbi, 2020).

For example, introduced technologies like 5G might increase the speed efficiency alongside latency improvements but also expose security risks. More assets and devices will be connected with each other which will put networks under the risk of security threats. Security vulnerabilities are required to be assessed and addressed clearly as a failure in cyber security is high likely in a network that include massive number of appliances and devices. Hence, the need of tools that can process and analyse large set of

data is required more than ever nowadays (Eskelinen, 2022).

The term of SOC can be defined as unit that includes analysts, processes and technology. Experts and specialists are the analysts that required to have skills in regards of understanding their companies polices and how network devices operate. They are also responsible of making decision on whether an attack is real or fake in order to implement an effective responding plan. Processes include organisation policies, standards and methods that need to be adhered by analysts. An organisation is in need to identify its SOC scope as it is an essential aspect for it to work efficiently. The last category of SOC is technology which involves all devices such as hardware and network components plus software that are in control of keeping network safe and dealing with alerts and records (Alharbi, 2020).

Onwubiko (2018) explained SOC aspects by mentioning various processes concepts. Set of rules can be identified and set by stakeholders in order to draw actions and steps required in the occurrence of an incident. These rules are referred into playbooks either incident response or recovery playbooks depending on their requirements. Gathering events by threat intelligence and monitoring network traffic are referred as sources.

On the other hand, log source is the device, tool or network infrastructure that generate information and provide logs that include various details about specific event. Firewalls and intrusion detection systems are related to security enforcing function that include preventive systems. For example, IP packets that are passing an observation point in network are defined as network flow, where an observation point is referred to the location of where IP packets can be identified. Threat intelligence is usually linked with the ability to track and observe activities on the network from various sources such as Indicator of Compromise (IoC) threats. IP addresses, target, location, domain, threat actors or organisations involved are part of the information that can be gained via threat intelligence. The term of log collection is associated with generated events and logs from different IT tools that are often stored in a main repository. Determining the relationships amongst the mentioned terms (playbook, sources, log source, threat intelligence, log collection) is referred to a process ontology that uses analysis to identify the nature of an activity by gathering details throughout the detection of anomalies, respond and recovery (Onwubiko, 2018).

An ontology-based graph can be used to represent the relationships that

assist in understanding of how cyber incidents can be identified on monitored assets as shown in below Figure 2.2.54.

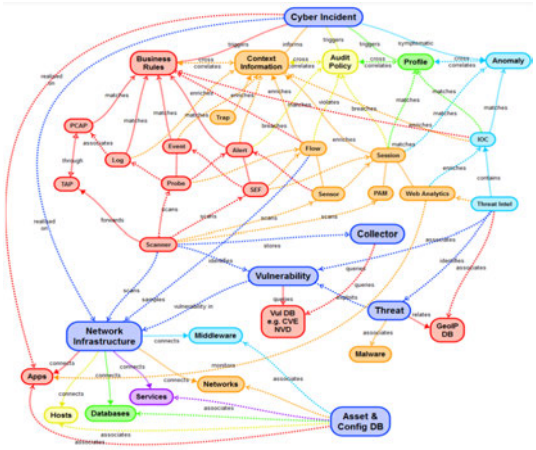


Figure 2.2.54: Anthology-based graph (Onwubiko, 2018)

The graph is described as a hierarchy of different layers connected with each other. The detection logic layer aims to focus on detecting incidents by generating alerts that includes information about an event or attack. Sources layer includes information and evidence from different sources such as logs, alerts, and IoC. Analysing such evidence is effective when it matches predefined rules to help in recognising the impact and nature of such an attack. The controls layer aims to provide protective measures to automatically stop an attack by detecting its existence. For example, firewall can be part of the controls by blocking a port to stop an incident from happening. It can also produce an action log that can be analysed and merged with other various threat intelligence sources to recognise and assess the situation. There are other sub-layers of the proposed hierarchy, they consist of collector, vulnerability, infrastructure, threat, and asset. Storing scans outputs is part of the collector layer to detect vulnerabilities related to scan reports. Connected assets, services, network infrastructure and any data they could held as part of their configurations are included in the network infrastructure entity. A threat such as malware is an example of the information that are associated with threat sub-layer. Geographic IP address is an example of the details that threat layer can provide to map the source of a threat and vulnerabilities that might occur on the monitored environments (Onwubiko, 2018).

Vielberth et al. (2020) stated that there is a lack of a common term of SOC, as it can be described differently such as network operations centre or security intelligence centre. But authors summarised the definition of SOC as follow *"SOC represents an organisational aspect of an enterprise's security strategy. It combines processes, technologies, and people to manage and enhance an organisation's overall security posture"*. The word of security operation is to implement a safe cyber environment by analysing threats and responding effectively to infringement occurrences. Platforms that are employed to detect and respond to cyber threats are usually called SOC. It can also be referred as security intelligence centre which highlights the importance of data identification as well as the technical aspects of SOC (Han, 2021).

2.3 SOC Types

There are various types of SOC, an internal one which is separate from the IT operations team. Combining IT team with SOC team fall under the umbrella of an integrated SOC. The other type is called outsourced SOC where organisations use providers to deal with their security aspects. Consequently, some organisations have already security systems such as: Security Information and Event Management (SIEM), but it is likely to occur only in large companies. Therefore, Small Medium Enterprises (SME) have probably just started to recognise the need of sophisticated security monitoring systems which can integrate with their current infrastructure. Enterprises can decide to implement any type of SOC depending on their needs and policies, but in fact security operations needs to be separated from other infrastructure in order for it to work comprehensively and efficiently. Security operations require huge number of logs and records that needs to be normalised and reported to the responsible security management team to set robust response plans to threats (Weissman and Jayasumana, 2020).

Organisations can decide to choose various types of SOC either in-house or outsourced. According to Tureczki and Szenes (2021) outsourced SOC usually linked with advantages that include high process and more efficient cost plus the provided supervised services. On the other hand, outsourced SOC might also be exposed to potential risks as only a slice of controlling procedures will be outsourced. It is essential for decision makers in organisations to take the responsibility where a dedicated SOC is needed to fulfill the rest of the business controlling measures. Dedicated or built in SOC known for its compatibility in having full control over the organisation monitoring

measures. It provides a comprehensive picture of the SOC elements such as: people, software and hardware devices. Implementing in-house SOC is associated with difficulties where experienced analysts and enhanced technologies are required. Hence, this can increase the total cost where only large sized firms might be able to afford it.

The increasing number of cyber security incidents and their damaging effect have pushed decision makers in organisations to build centralised SOC. By observing the state of network devices, SOC is essential to immediately detect malicious events and take actions accordingly. It is an important defensive barrier to fight the ongoing cyber war, as it behaves as vigilant eye by monitoring assets via collecting logs continuously. The ability to report real-time data is an effective SOC solution that draw understanding picture about the assets security situation . Nevertheless, a built-in SOC offers a real-time monitoring environment which is effective in detecting, containing, and responding to vulnerabilities (de Céspedes and Dimitoglou, 2021).

Organisations are benefited from having a centralised SOC, but the required infrastructure and resources to manage it is also significant where it can be high costly and resource consuming. The main features of any SOC include the management of logs, visualisations and reporting events. These three components integrate with each other as the gathered data are required for visualisations where they can be deployed to report incidents. In fact, traffic logs need a vast processing storage before passing them to the visualisation stage via the adoption of various techniques. Logged information can be useful to provide meaningful graphs about the current situation so analysts can then determine the overall security health of the network assets (de Céspedes and Dimitoglou, 2021).

An organisation can use multiple SOCs but in fact when more than one SOC is being deployed then a function must be implemented to interpret the outputs and send the digital value to decision makers to improve controlling measures. The required function is often fulfilled by Cyber Security Fusion Centre (CSFC) which creates a bridge between SOC and management team. With CSFC in the middle the output can be translated to an understanding value for management (Tureczki and Szenes, 2021).

Sievierinov et al. (2021) categorised SOC into three different models. The classic SOC model which is responsible of monitoring the IT system of

an enterprise to detect any suspicious activities. One of the disadvantages of this model is the inability to track an event sequence across the system. A classic SOC use correlation rules to inform analysts of any previous incidents. It also relies on the implementation of SIEM tool to produce statements based on correlation guidelines. There are two types of the classic SOC. The first one operates on normal working hours 9-5 which requires minimum staff skills including 2 workers, 2 analysts, 1 architect and a manager. The 24h model requires more staff which can be up to ten operators alongside one analyst and a manager. An internal classic SOC team is able to provide a comprehensive picture of the current threat landscape of an enterprise. At the same time the large number of false alerts are generated due to the low degree of processing data in regards of security incidents. According to Sievierinov et al. (2021) implementing an in-house classic SOC is suggested for mature cyber security organisations.

The MDR model is another type that refers to managed detection and response. It is usually associated with outsourced SOC. The focus of this model is more on monitoring external events that might have been occurred due to admins faults or errors. Threat intelligence platform and database are part of the MDR to analyse gathered threats data to manage the development and rules of spotting incidents. Experience of up to three years and knowledge of various operating systems alongside scripting programming languages are required for staff to have in order to run SOC-MDR efficiently. Reasonable cost and scalability are some of the advantages that managed security services providers can offer to run outsourced SOC. Threats are not only being detected but also responded to where the criticality is assessed to inform enterprises about an event. Lastly, a mixed SOC-MDR model is an effective solution in detecting and auditing complicated information security matters. The difficulty of implementation and high cost must be considered as well. The core of SOC-MDR consists of event management and knowledge base platforms which generate vast amount of data (Sievierinov et al., 2021).

2.4 Tools used in SOC

To provide a secure cyber environment, SOC usually depends on set of systems. These tools are designed with the goal of collecting, analysing and visualising information in an understanding way for analysts to investigate incidents effectively. Security Information Event Management (SIEM), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Next-

Generation Firewalls (NGFW), Endpoint Detection and Response (EDR) and Threat Intelligence Platforms (TIP) are some of the tools that are part of the entire SOC as Kiiveri (2021) stated.

SOC tools operate by collecting logs and data generated from several systems sources. Records and logs are produced from security products such as IPS or antivirus software. Also logs that are coming from operating systems and applications. Collecting logs by gathering data from sources then store it in a centralised location plus the ability to construct log correlation amongst various events are the main functions that SOC is able to provide. It offers continuous access to previous information and present the gathered data in readable reporting format. Hence, the deployment of AI and ML in SOC solutions are required now more than ever to enhance the detection techniques and improve the automation to respond to security incidents more effectively (Hristov et al., 2021).

Log management is a vital tool of SOC in analysing real-time traffic. Log data is described as a type of an event that keeps record of certain activities on an operating system, networks or any other appliances. SIEMs are the usual log management tools that complement SOC as an overall term. It is important to highlight that a log will contain information such as date, time, users, type of operation and if it was successful or not. SIEMs are useful and assist holistically in optimising security posture due to investigations and reporting capabilities (Eskelinen, 2022).

Building event modelling depend on the security metrics that SIEM use in order to have an overview of the events that are being generated from variety of sources including hosts, servers, and endpoints. Therefore, a risk analysis procedure will be provided as part of the processes. SIEM contains important methods while considering zero-day threats and recognised incidents. Delivering security solutions is done by SIEM as it utilises analytical approaches and interactive evaluation that support the delivery of these solutions (Mutemwa et al., 2018).

One of the well-known SOC tools is Splunk SIEM. It consists of three main elements: Search bar, Indexer and Forwarder. Each component has its own role to deliver a comprehensive SOC solution. Figure 2.4.55 below provides an illustration of Splunk main components.

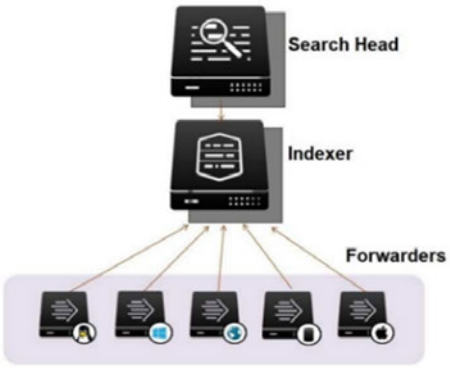


Figure 2.4.55: Splunk Components (Hristov et al., 2021)

Hristov et al. (2021) stated that the indexer is utilised for storing and processing generated logs to help in analysing the data and search for particular logs when needed. Splunk has its own language when searching for events. It is defined as Splunk Processing Language (SPL) similar to SQL queries. A user is required to type the queries into the search bar in order to retrieve the required information. This can be provided in various formats such as reports, charts or even on dashboards. The final component is forwarders where logs are being collected and forwarded to indexers.

The adoption of Splunk has many advantages that helps SOC analysts to benefit from these logs. For instance, Machine Learning Toolkit (MLTK), plugins and other ML models libraries can be installed in Splunk to detect potential threats based on the extracted data. Cersosimo and Lara (2022) used a free Splunk license and download MLTK model to achieve their results. They implemented a model of DNS requests using Splunk ML kit to identify anomalies behaviours. Random Forest (RF) and Decision Tree (DT) algorithms are trained for detection. The results revealed that an accuracy of up to 88% is achieved via RF where 87% is associated with DT algorithm. The availability of ML models in Splunk also provides an interactive interface which assist in removing complex barriers that are related with ML. In Splunk, data can be visualised in a human readable way and commands are built in advance to apply ML models from various open-sourced algorithms. Splunk offers an easy data driven solution to utilise, apply and train ML models as well. SOC analysts are able to locate and discover threats more efficiently using Splunk as it can index data from several sources and store them in a centralised searchable location. Furthermore, SPL offers users with features to clean data and identify outliers. Data can also be

visualised in different types of charts which offer analysts the privilege to constantly interact with the aggregated data.

On the other hand, a lot of organisations are also moving towards cloud to store their data instead of traditional data centres. Implementing solid security measures is required to protect cloud infrastructure. According to Ananthapadmanabhan and Achuthan (2022) threat model is often used as a method to enhance the security aspects of several platforms. An integrated threat model and threat intelligence system via the adoption of Splunk is developed by researchers which shows the effectiveness of Splunk in detecting threats. The integrated model is capable of detecting threats and live events that are happening on cloud systems. Gathering raw data from cloud logs is the aim of the model to detect cloud behaviours. The current threat models usually tend to understand of how an attack is occurred in a system. However, the proposed model assists in categorising threats depending on attackers' behaviours in past cyber-attacks that occurred on similar cloud systems.

MITRE ATT&CK framework is used by authors for developing the model in Splunk. Adversarial tactics, techniques and common knowledge are the meaning of ATT&CK. This paradigm aids in understanding potential threats scenario after the occurrence of an attack within cloud systems. Figure 2.4.56 below depicts data movement withing the model. As shown, threat model and threat intelligence models are integrated via Splunk plugin. The threat model is connected to Amazon Web Services (AWS) with a plugin that use AWS policies, this justifies the link amongst cloud and Splunk. JSON which is JavaScript Object Notation syntax plugin is used to connect threat intelligence model to the containers of AWS. This helps in diverting the outcome of threat intelligence to Splunk dashboard. The overall picture is displayed on the dashboard of the integrated plugin in Splunk via the implementation of AWS polices and JSON syntax (Ananthapadmanabhan and Achuthan, 2022).

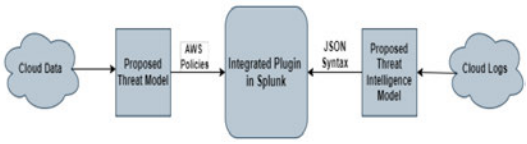


Figure 2.4.56: Integrated Model Data Flow (Ananthapadmanabhan and Achuthan, 2022)

The merged integrated threat paradigm using Splunk provides security protection on cloud systems to detect live potential threats. In contrast, one of the disadvantages of the proposed model using Splunk is that it can only be effective on cloud infrastructure and cannot be applied to traditional systems (Ananthapadmanabhan and Achuthan, 2022).

Accordingly, Splunk SIEM offers a variety of different ML algorithms that can be useful if they applied accurately. DensityFunction is an example of an effective algorithm provided by Splunk. It can be trained depending on parameters being set at training and end levels. Lambada () is a parameter that can be set to be responsible of input data that the training will be depending on. The parameter can be referred to any information classification for sampling purposes. For instance, identifying password attack attempts can be done via setting the parameter to either day and night or sign of the week etc. Then data can be grasped according to the fact of now is day or night, more specifically the probability of such an attack can be either lower or higher depending on the set parameter. Establishing an accurate and clear detection of abnormalities cannot be completed without the need of extra noise removal of the training sample. Any expected activities from legitimate, known assets and principle of operation are amongst the noise that can be abandoned. These types of expected irregularities events can be included as exemptions in order to not interrupt with the algorithm learning process. On the other hand, dealing with few data points is usually linked with high likely of noise (Venherskyi and Karpiuk, 2021).

Another example of a SIEM is an open-source tool which called Wazuh. The tool includes a centralised platform that deliver management, control and threat detection functions. Shatnawi et al. (2022) added that SIEM is a system that comprises significant technologies to deliver substantial security posture to threats atmospheres. Therefore, a SIEM that can meet and fulfill the requirements of an organisation must be selected wisely.

Nguyen (2022) utilised SIEM known as Odin Sight in their research. It includes capabilities of controlling and managing the overall infrastructure of an organisation. One of the benefits of Odin that it has the ability to collect data either on dedicated network or cloud services. Imposing policies and correlating relationships amongst data are part of the advantages of this SIEM according to authors' research. Accomplishing such tasks begin with data gathering from security systems on an organisation network. This can include network appliances, operating systems, applications assets and users' behaviours. The collection of logs is accomplished in a real time environment to allow analysts to detect threats and respond to them immediately. Accessing Odin SIEM can be achieved via secure access to either an application software or using web browser.

In addition, Lalos (2022) emphasised on the most significant reported concern by SOC which is the large volume of security alerts. Author added that an alert might not be associated with critical problem, and it might be often related to a false positive event which can be ignored. To be able to identify and ignore such alerts, analysts are required to have the needed experience to detect them. However, even with the existing experience, the high number of alerts makes it difficult task to achieve. Therefore, automation can be a solution for this problem. For this purpose, Security Orchestration Automation and Response (SOAR) is also part of the SOC tools that can be implemented to automate processes and reduce responding time. In fact, the definition of SOAR is the collection of tools and software that have the ability to provide services to a SOC in few main aspects. Vulnerability management, threat and automation of SOC are part of the areas that SOAR is able to offer. It is known as a layer that deliver security processes and enhance SOC automation. SOAR does not only include tasks such as scanning for threats and managing logs. Nevertheless it can also help in prevention. Analysts are able to select between potential auto responses in order to deal with a current threat by the adoption of security automation that can be provided by SOAR. The usage of such software help analysts to concentrate on genuine threats rather than distributed by re-occurring events that can potentially get automated.

Gartner in 2017 presented the definition of security orchestration to elaborate on the functions that are provided by the evolved technologies. This included engagement amongst incident response, automation and other related plugins. SOAR technologies are defined by the researcher as tools that allow the collection of data from variety of end points to enable the func-

tion of threat analysis and triage. In turn it leads to an effective incident investigation, definition, prioritisation and that can be retrieved from the combination of analysts and machines efforts. Another author known as Jon Oltsik also mentioned on the adoption of SOAR technologies by cyber security defence teams during previous years. Implementing SOAR tools can increase the automation in SOC specially at tier 1 level which could result of reduction in analysts at that level. The emerging technologies could also enhance and improve tier 1 analysts by providing them with up-to-date tools that have the ability to face sophisticated incidents. It is essential to highlight the benefits that can be provided by SOAR tools comprises of the ability to view data and share it in an effective customised prototypes solution. This helps in understanding an incident pattern and recommending defensive process that have been implemented previously (Lalos, 2022).

Hence, SOC tools and its plugins offer a range set of advantages including user friendly platforms to analysts who have less expertise in the field. They also boost experts‘ abilities. Therefore, such tools can act on behalf of analysts where needed (Lalos, 2022).

Accordingly, network traffic is constantly increasing and SIEM tool is an essential component of the entire SOC but to be able to detect upcoming activities, a threat detection system is also required to be added to SOC (Bienias et al., 2019). Threat detection complements SIEM's duties but it is also an important element to increase efficiency and functionality. The implementation of threat detection must fit with the organisation network environment. Therefore, any random applied algorithms might not be effective enough. On the other hand, confidentiality and privacy issues can occur due to the gathering of data traffic from several network systems. Bienias et al. (2019) emphasised on the importance of deploying an applicable anonymised algorithm.

The implementation of threat detection is a complex task, and organisations can take years to achieve the expected outcome. There are different basic suggested methods that can assist in threat hunting. Primarily, the collection of logs from various systems is necessary to be fed into a centralised location. SIEM and IPS or IDS are also supposed to be part of SOC tools. As well, a response team is needed to deal with IoC that are collected from reports (Bikov et al., 2021).

2.5 SOC Architecture

As any type of technological system, various components collaborate with each other to illustrate the architecture of a SOC. Shahjee and Ware (2022b) stated that different elements are added together to produce holistic picture of SOC. That can be used to determine the vision and security tactics of an organisation. SOC represents the combinations of People, Processes and Technologies (PPT). Governance and compliance are also added to PPT as PPTGC to manage the security aspects of firms. Both PPT and PPTGC frameworks can be followed to manage an organisation real-time security environment. Various functions and duties are blended to depict SOC as the main immune centre. There is a tiered approach that is followed when dealing with events. This approach can be either of analysing incidents or escalate them to experienced analysts for more in-depth investigation.

Figure 2.5.57 illustrates the SOC architecture design. The first element is data collection where data traffic is gathered from different sources and endpoints such as; firewall and other network devices. The collected information then filtered and merged via data processing component. Correlations techniques are also applied to analyse data in an event and knowledge base. Visualising data after applying correlations is essential to provide an understanding portrait of any potential threats and suspicious activities. The architecture of SOC design is summed up using the 4 main components which are Data Collection, Data Processing, Correlation Analysis and Visualisation (Shahjee and Ware, 2022b).

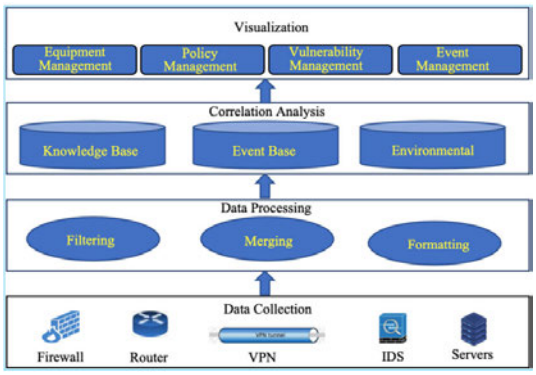


Figure 2.5.57: SOC Architecture (Shahjee and Ware, 2022b)

Shahjee and Ware (2022a) proposed a framework called "INSOC" that

consist of SOC and Network Operation Centre (NOC) in an integrated form. They added the PPTGC (People, Process, Technology, Governance, Compliance) technique to the development and design of Integrated Network Security Operation Centre (INSOC) to classify its strategies and operations. By following the best approaches of establishing complex IT infrastructure environment, the proposed model divided into three different layers as shown in Figure 2.5.58 below. It starts with a physical data source level then a Fault Configuration Administration Performance Security (FCAPS) layer alongside the last layer which is related to situational management.

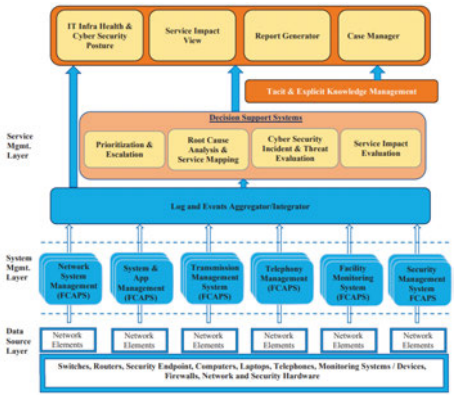


Figure 2.5.58: INSOC framework (Shahjee and Ware, 2022a)

As a result of adding work methodologies of both SOC and NOC the layers have been established. The data source layer is mainly act as awareness provider to the INSOC where network endpoints and assets are connected to it. Hardware, software and different events and logs are being used by the Network Management System (NMS) level for surveillance objectives. However, the generated data are being linked into the service management layer by alerts collector for analytics purposes. In the high management system, NMS performs operations of surveillance on various aspects of the integrated network assets such as detecting faults, assessing performance and managing security based on the FCAPS layer. Hence, it performs similar to an immune system. The generated logs and events from various network and security systems are then being sent to the situational service management level for more related analysis processes. Lastly, when logs are received by the situational layer, its responsibility is to ingest all inputs to assess and decide on the overall situational picture for such an event. This layer also has capabilities in recovery methods and decision making. Managing in-

cidents, detecting auditing and analysis are the overall tasks that can be performed under this layer via the collection, correlations and storing data in a centralised centre. As a result of adding work methodologies of both SOC and NOC the layers have been established. The data source layer is mainly act as awareness provider to the INSOC where network endpoints and assets are connected to it. Hardware, software and different events and logs are being used by NMS level for surveillance objectives (Shahjee and Ware, 2022a).

According to practitioners, to run such a framework, resources including data centres and critical infrastructure are required to put together the convergence strategy. Nevertheless, INSOC model is useful in decreasing the number of generated tickets and assisting helpdesk technicians as most of the data load will be based on a single platform that integrate both SOC and NOC. Relying on one main data centre that collect information and distribute it through a grouped INSOC tools is an advantage of the model instead of waiting on both SOC and NOC to process data individually in separate circumstances. The grouped functionalities and operations allow INSOC users to share knowledge with each other in terms of addressing gaps, vulnerabilities and fixing errors smoothly via the integrated INSOC approach. Overall, the below points are the summarisation of the effectiveness of the framework:

- Enhancing network and security strength.
- Improvements in Service Level Agreement (SLA) by reducing time wasting and effective response time.
- Overcome the shortages in skilled analysts in enterprise by sharing training on the job level.

Consequently, if both NOC and SOC have not been merged accurately and optimally then the overall framework will not be sufficient enough (Shahjee and Ware, 2022a).

2.6 Building a SOC

Suggestions on building SOC are gathered based on the National Cyber Security Centre (NCSC) guidance that was published on the 23 of May 2022. There are various aspects that need to be considered when building a new SOC or improving an already existing one. Operating model, onboarding,

detection, threat intelligence and incident response are the aspects addressed by NCSC (2022).

Considering the design of an operating model when building a SOC is essential to highlight the assets that are required to be monitored. Offering the same monitoring quality to all assets could be difficult task to achieve. Thus, liaising with the current IT team is required to gain in-depth details about the current state to prioritise SOC tasks. This helps in drawing a picture about threats that could be faced to develop a target operating model that fits with requirements and assist in understanding how different components will operate together to deliver an overall security posture. Threats and requirements can change over time due to various reasons. Due to this, an operating model is suggested to be developed where it can adapt to any changes. Threat profile is also highly recommended for shaping the approach that will be taken for threats detection. It can be different as small firms require lower threat profile than larger organisations that require their SOC to respond to more sophisticated attacks. Hence, the types of attackers and threats are advised to be considered as part of the operating model. Outlining the required operating model is useful to understand the threat level scope and indicate attacks that might take a place (NCSC, 2022).

After establishing an operating model, onboarding process comes into place. The meaning of onboarding is related to logs that are collected by SOC for monitoring purposes. It is an essential element that can be either added to a new SOC or to an exiting one as the scope of logs can change over time. The process of onboarding can be executed via collecting common log sources or gather each available one. By identifying log sources, this helps in gaining in-depth and valuable knowledge about any anomalies activities that can cause harm. Onboarding can be implemented for threat detection and respond to an incident as well. Logs are categorised into different types. For example, application logs provide details about users' activities, whereas network logs include information about devices that are connected to an organisation network. Authentication logs are also important type as they can identify the location and time of users who have logged in to a system. If unauthorised access occurs, then warnings are generated as a result. Firewall and access control are part of security control logs that are also recommended to be collected. These types of logs provide priceless information about malicious activities. Therefore, onboarding is a vital component that must be considered (NCSC, 2022).

Systems are exposed to attacks and detection approach is needed. Commercial, use-cases and data mining are suggested for threats detection. Anti-malware or IDS/IPS are some of detection technologies that are related to traditional commercial detection tools. Detection tools are supposed to have regular updates and ML plus threat intelligence that can be deployed to apply new guidelines. In some cases, information or data can be transferred via SSH (Secure Shell) outside business hours and to monitor these types of activities a custom detection use cases are required. Use case rules are usually utilised via SIEM where a searching process is implemented automatically to identify similar logical pattern based on the rule being searched. As a result, alerts will be generated in real-time based on the collected data from log sources. Indicating the behaviours of malicious activities is the main aim of implementing use-case detection rules. The amount of data being processed by organisations can be large and complex where it needs for data mining or log analysis techniques. The use of data mining help in detecting malicious events where the attacker has managed to escape alert or detection tools. Unauthorised connections, large traffic volume and irregular files transfers are also rules that can be developed using data mining logics to discover undetected compromises. Attacks are not effective based on one action, but in fact exploiters usually carry out their attacks using a mixture of methods. The implementation of data mining and advanced log analysis are crucial in identifying threats. SOC users are expected to understand the life cycle of successful attacks to apply sophisticated logics to discover them (NCSC, 2022).

According to the NCSC (2022) guidance threat intelligence or TI is described as the basic knowledge of malicious activities as well as understanding attackers' technical tactics and methods more in-depth. Implementing in house TI functions for detecting threats is not required if an organisation relies on commercial tools for detection where the vendor is responsible for. Otherwise, it is essential to think in advance and stay ahead by developing use-cases rules and alerts. TI is beneficial for providing valuable information when it comes to onboarding. Another aspect is included by the guidance which is the sharing of intelligence. No matter what approach is being used for threat detection; it is essential to share information to stay alert of threats landscape. NCSC provides a service called Cyber Security Information Sharing Partnership (CISP) for UK organisations that are bounded by cyber security. Only registered UK organisations and government are able to share cyber security threats information amongst themselves in a protected and private environment. Storing, correlating and managing threat

intelligence is achieved via Threat Intelligence Platform (TIP). The platform enables automation for detecting IoC by connecting to SIEM tool. There are various types of TIPs and it depends on whether an organisation is using commercial tools or not. Implementing threat platform is beneficial to increase SOC value by feeding it with a wide range of intelligence (NCSC, 2022).

Schlette et al. (2021) described Cyber Threat Intelligence (CTI) as a combination of security data and incidents reports that can be considered as the foundation level to start CTI. There are different categories of CTI including IoC, strategies, methods and approaches. It is vital to mention that vulnerabilities, threats and the exploited victims can be added into the CTI list. Malicious IP addresses and malwares can be the most known models of CTI but in fact any action or activity information that can be associated with cyber threat is referred into CTI. The concept of processing related knowledge from monitored data generate comprehensive analysis about particular cyber situation can be indicated as CTI. This also comprises the sharing of information and collaboration with partners.

Accordingly, the main purpose of CTI is to provide another layer of defence by enhancing the security assessment and advance the protective security methods. The use of threat intelligence focuses on decisions makers and security operations that can benefit from it. One of the most essential aspects is the sharing of information where CTI concept can be linked into SOC. It is often included two groups at least such as the supplier and client. For instance, referring to supplier it consists of group of security analysts and their security vendor where they can create CTI related information or evidence. The consumer of CTI then can derive this evidence as external cyber threat intelligence for additional usage. In addition to this process, platforms and communities can exist such as a centre for information sharing and analysis where it gathers and disseminate information to its members via the utilisation of Threat Intelligence Sharing Platform (TISP). As an outcome, SOC analysts can also be able to generate and derive cyber threat intelligence on behalf of their business (Schlette et al., 2021).

In order to triage alerts efficiently and smoothly an incident management must be added to SOC package. A solid management is essential to distinguish between alerts and genuine incidents as an alert does not necessarily has to be an actual incident. Primarily, analysts are supposed to understand and grasp the knowledge about the detections use-cases that are

in place and their purposes. Alerts must also be designed to extract as much information as possible from log sources and present them on a screen. In fact, the more details are presented the quicker an issue can be escalated to be resolved and investigated. As well, minimising false positives based on improvements feedback. Most importantly, triage paths are needed to be clear, and records must be up to date. By understanding how the system performs, alerts will be easier to triage and anomalies can be spotted effectively. Analysts can also be offered the ability to work on different SOC roles to help in getting familiar with systems that are being monitored. Overall, when triaging or investigating an incident, it must be recorded and kept for SOC accountability or for future quality assurance checks. This ensures that any false positives are not being ignored and assist in responding and dealing with similar upcoming incidents (NCSC, 2022).

Incident response is conducted within limited time under high pressure where the environment is constantly changing including large amount of processed information. It is required to have a collaboration amongst analysts, processes, and technologies to draw a situational awareness about specific threat. Ahmad et al. (2021) described the environment of incident response as dense socio-technical atmosphere. This means that individuals judgment and decision making are needed to control the density and complexity of an incident. The aim is to employ situational awareness to bridge the gap between the efforts that are utilised by threat actors to execute their attacks and the efforts that are exerted by events responders to protect their organisations assets.

Nguyen (2022) highlighted the guidelines set by the NIST framework for security log and monitoring management. NIST stands for the National Institute of Standards and Technology. Firstly, log management infrastructure typically consists of hardware and software that are responsible of storing, analysing and processing data logs. Different functions are expected to be provided by infrastructure to support and maintain the access to these logs as well as log parsing, log archival or disposal where needed. Planning the management of logs is vital and is also outlined by the guide. Consistency is the key to a successful log management. Creating an efficient and reliable management plan in advance is important to increase the quality and also to meet organisations requirements in managing generated logs.

Operating log processes is expected to be backed up by standards that are already justified amongst system infrastructure administrators. These

standards help analysts in understanding logs they are responsible of. Log sources configuration, log analysis, responding to identified events and maintain data storage are some of the main key operational functions of log management. NIST guide provides significant information for organisations to implement, architect and manage their log data either in-house or by outsourcing it (Nguyen, 2022).

For example, NIST publication of 800-92 offers a log management guidance on the implementation procedures that need to be followed in terms of logging and auditing. Whereas NIST 800-94 provides suggestions on how to control and construct IDS/IPS systems. For malware detection improvements of devices including desktops and laptops, NIST publication of 800-93 recommends instructions to boost an existing structure of malware prevention and its reaction facilities. Last but not the least, the NIST supplementary publication of 800-61 is associated with handling threats. It delivers essential procedures on how to establish event management system, controlling, managing and responding to incidents smoothly and adequately (Shatnawi et al., 2022).

A study revealed that SMEs are generating huge amount of events data on daily basis where only up to 5% of the generated logs are analysed. This expose organisations to possible attacks. An overload is also impacting on cybersecurity resources due to alerts information produced in a machine friendly readable approach instead of human readable format. Users' activities and other behaviours are recorded continuously on systems. For instance, a higher education body includes up to 3000 workers and up to 40000 students produce up to 200 million events per year. In fact, less than 20% of these logs are investigated where the team only consist of approximately ten experts according to Afzaliseresht et al. (2020).

With the overwhelming volume of data alerts, not all of them are required to be analysed, but efforts and time are needed to be put by analysts to verify whether an event is false positive or a legitimate threat. Other factors are coming into a place where analysts are suggested to be supported by knowledge outside security logs to assess the scale of such a risk. The risks of in-house assets can be identified via local domain knowledge where an external risk would be assessed by global domain knowledge. An example of a local domain knowledge is a sever that can be used by an organisation for testing and can be categorised as non-critical host. Events generated from the local server can be ignored unless a critical breach arises. When a breach

occurs on a local server then other servers connected to it could be under a risk where further analysis is required even if an alert is raised by the connected servers. Primarily, a protection strategy must be adopted from the knowledge retrieved from internal aspects of an organisation. In contrast, global domain knowledge is obtained from external factors. It means that in order to keep on up to date with the incremental number of advanced attacks, an automatic knowledge is required to be generated from several external resources. If not, a complex log might not be prioritised appropriately which will lead to a late responding process and further escalations. Realistically, attackers usually modify and change their behaviours towards repetitive attempts, but on the other side an expertise knowledge may not be often improved at the same level as an attacker in the current atmosphere. As an outcome, any occurrence of a new breach is recommended to be dealt with more in-depth analysis of the threat actor's attributes (Afzaliseresht et al., 2020).

2.7 SOC Evaluation

The emerge of continuous sophisticated cyber security attacks contributed to the need of an effective SOC to detect, monitor and respond to them. Evaluating SOC characteristics is driven by several aspects. The quality of SOC services and facilities can be assessed against various factors. The common standards of an effective SOC include high skilled analysts, rigorous policies and processes, effective SIEM, active events analysis or reporting and applying threats intelligence methods. SOC maturity factors contain qualitative and quantitative aspects. The quality of logging events, how fast SOC can recover from incidents and how it can respond to them are qualitative considerations. The quantitative maturity levels consist of the number of true positives and false positives that are generated. The amount of data that are analysed per hours, minutes, or seconds. Also, the volume of utilised analysis metrics (Onwubiko and Ouazzane, 2019).

Adding to above Schinagl et al. (2015) indicated that SOC activities are clustered in several main areas. The intelligence activity or function which is similar to Computer Emergency Response Team (CERT). Experienced analysts are expected to be part of it where they can exchange knowledge amongst internal and external parties to monitor patterns and investigate results. Another function is the baseline security where security analysts are responsible of scanning different network components for any known vulnerabilities to maintain high level of security. The main task of baseline

is to supervise and operate the efficiency of tools such as IPS, firewalls and other detection systems. Monitoring traffic and identifying malicious activities are part of the monitoring function to process large volumes of logs then filter them via the implementation of dynamic rules. The key challenge here is to customise it to only process relevant events that are discovered. Nonetheless, penetration test function is part of the clustered activities. Performing such a test helps in understanding how the system will respond to breaches and what are the consequences of an attack. The last function is the forensic one. For instance if an investigation is conducted by law agencies, then analysts can assist in gathering electronic data as evidence. Therefore, for each of the mentioned functions their objectives of activities can be transmitted into requirements depending on the availability and experience of analysts.

Saraiva and Mateus-Coelho (2022) highlighted various fundamentals for an effective Cyber Security Incident Response Team (CSIRT). An up-to-date tools and guidance are required to maintain high quality of service. For instance, a small number of high valued capabilities are much better than high number of low-quality capabilities. It is also essential to have trust amongst organisations and their partners. In some cases, CSIRT might require sharing information and details amongst their organisation partners and without the trust aspect their activities can be ineffective. The CSIRT must also cooperate with government, national stakeholders and other national bodies for an effective interaction and sharing of sensitive information on critical platforms. Without the required resources and their efficiency, the response team would not be able to react to potential and new threats.

Threats exposed organisations to massive loss of customers loyalty, credibility, and accessibility. The main responsibility of SOC technology is to collect, aggregate, detect, manage and deliver useful solution. Data collection is a requirement for SOC to boost the monitoring framework. The analysis allows to triage incidents correctly and use system more effectively. It is also important to make sure tools in SOC are selected based on an organisation need (Dun et al., 2021).

SIEM collect data from various endpoints then correlate them to provide analytics based on the gathered information. The manual review of logs can be complicated and challenging task. Adding to it the vast amount of false positives which reduce the efficiency of threat detection. Obtaining the required balance and achieve the most of SIEM system can be accomplished

via the effective building of SOC (Bikov et al., 2021).

SOC strategy is suggested to be supported by the overall organisation strategy. It is difficult to have an effective SOC in place without having a cyber strategy. An efficient SOC is usually based on coherent governance and clear understanding of roles and responsibilities. This makes it sufficient enough for reporting and escalating issues. Teams that are responsible for different tasks are suggested to be under one controlling umbrella authority. This is useful for operations quality. Having more than one SOC governing authority increase the level difficulties of tasks where SOC already includes complex challenges (Onwubiko and Ouazzane, 2019).

Saraiva and Mateus-Coelho (2022) highlighted the following as part of SOC functions:

- SOC ensures organisation IT infrastructure and assets are recognised.
- It guarantees the protection and security of the monitored systems and applications.
- SOC ensures threats and vulnerabilities are detected and identified; therefore, they can be mitigated in advance.
- Potential threats actors who intent to harm the firm can be spotted.
- It provides incidents triage, investigations, management and information reports about the estate of assets.
- It helps in creating risky profiles for individuals who are known as suspicious to the firm.
- Violations of policies, events analysis, patterns and trend investigations are also amongst the functions in identifying a compromise or a threat (Saraiva and Mateus-Coelho, 2022).

Taqafi et al. (2023) divided the tasks of SOC into various duties. These duties are called functional domains and they can vary depending on an organisation needs. To begin with intelligence function, it is the primary function of SOC where information associated with threats are gathered to make decisions. Information is received via reports either internal or external monitoring feeds where analyses on threats is executed. Compliance and vulnerabilities scans are essential to avoid unwanted security consequences.

Hence, baseline security domain is another functional duty of SOC to spread awareness in an IT environment and to warn intelligence team for any required decisions. Responding to events is required, therefore, monitoring and response functional domain is responsible for this task.

Organisations can use security incident and event management systems to observe the network traffic by analysing behaviours. As a result, potential risks can be identified on early stages to prevent security mishap. Identifying security gaps in a system can be achieved by applying penetration testing functional domain. It is part of SOC domains to help in testing targets for any weaknesses or flaws. The last domain is forensic investigation where it is carried out as a result of an incident that impacted on the targeted system. Examinations and investigations are part of it to identify the reasons behind such an event and threat actor. Evidence such as proof of an incident investigation must be in safe place if passed to local bodies. Files contain logs or hard drive are examples of such evidence (Taqafi et al., 2023).

For a productive SOC deployment: strategy, value, structure, alignment, prioritisation and investment elements must be considered by organisations. SOC is an essential component for businesses, through the usage of it an organisation can meet its objectives by monitoring services and reducing the risk of security breaches that can cause heavy fines and penalties. The value principal can be achieved when cyber security support businesses to meet their objectives. In fact, having a robust cyber security measures in-place can be used as an advantage to win new business market shares nowadays. Alignment factor means that an organisation is advised to align its functions to their main objectives to assist SOC in providing effective security monitoring. SOC is presented as central function and the organisational structure is required to empower it to be more efficient and useful. Onboarding cyber security must be prioritised for the most critical systems where SOC can play a key role in regards of having a risk-based approach that ensure the risk management (Onwubiko, 2021).

Overall, SOC can be recognised as a business investment but in reality, cyber security investments are not expected to generate financial income. Organisations can recognise the importance of SOC when a cyber attack is prevented which could‘ve exposed the company to unwanted financial losses. SOC investment can be approached as cost-saving opportunity that can be gained throughout the avoidance of services downtime, potential penalties and fines. Reports that show analytics and visualisation on the number of

attacks that have been prevented plus successful compliance must be notified to stakeholders to recognise SOC investment principal. Due to the role that SOC plays in helping organisations achieving their goals and objectives, it is an outstanding business investment that can influence positively on the overall performance. SOC must be identified as business function alongside the fact of it is being an IT system (Onwubiko, 2021).

Adding to the above, small firms with limited time and funds require different approaches to establish a successful SOC. Merging the most essential tools and resources into a workflow model to easily manage them via small teams. Assets identification, assessing vulnerabilities and SIEM functionalities are amongst the capabilities that small organisations resources must have. Strong passwords policies and access control measures ensure vulnerabilities are patched effectively alongside protective events. With the occurrence of Advanced Persistent Threats (APTs) that is refereed to attackers have access to more sophisticated kits, the importance of detection and prevention become more obvious. Adversaries aim to target organisations for the goal of establishing ongoing undetected presence of an attack on the targeted assets. Delivering proactive and effective prevention measures against these types of attacks is a challenging task not only for small business but also for large ones. The required resources for SOC environment must include the abilities to protect, detect, mitigate and share intelligence with various SOC societies (Mihindu and Khosrow-shahi, 2020).

SOC play a key role in reducing financial impacts on businesses. It is essential for organisations to identify their own cyber security strategy in advanced before starting building such a SOC. Current objectives and concerns are required to be highlighted to fulfill the goals of having an effective SOC. Deciding on the required infrastructure and tools are amongst the objectives as well as the required staff and skills (Eskelinen, 2022).

Having SOC in place can guarantee a detection rate close to 100% by 24/7 monitoring operations. Responding time to an incident can only be a smaller piece of the average time of threat detection. SOC solution is a big advantage towards security posture and regulations compliance (János and Dai, 2018).

2.8 SOC Analysts

SOC often operates using tiers system, where tasks are assigned according to individuals' skills. Entry level tasks are allocated to first tier analysts and more complex duties are sent to higher tiers. Security analysts who track incoming alerts and validate if they are real are part of Tier 1. They pass on tickets to Tier 2 when needed. Tier 2 includes specialists who respond to events as they conduct in-depth investigations to propose remediation suggestions. Individuals who have superior knowledge on the enterprise network and how it works alongside skills in threat intelligence and malware engineering are usually called Threat Hunters. They are referred to as Tier 3. They are also responsible of investigating and continuously search for new threats that have not been detected yet. Nevertheless, it is essential to have a SOC manager in charge of the resources and to be the first point of contact with clients and other organisations when required (Nugraha, 2021).

Monitoring, identifying, and reporting cyber security events are expected tasks to be performed by analysts. In fact, analysts are the key role in delivering the services of a SOC. Based on theoretical viewpoint, Activity Theory (AT) is a term that is used to understand the activities and functions performed and followed by analysts (Agyepong et al., 2023).

The proposed theory can be applied into any individual action with the assumption of that action is either goal or objective directed. An absence of an objective eliminates scheduled actions based on the AT aspects. AT emphasis that human actions are not performed individually but in groups. Applying AT into SOC is vital to justify the work amongst analysts and to execute operations effectively. Incident triage rules, playbooks, standard procedures and other related rules must be obeyed and followed by analysts to achieve their goals and objectives. To gain their aims, security assets such as SIEM, firewall and IPS/IDS are the tools that analysts depend on when dealing with operations. Therefore, the operation of a SOC is divided into various levels including tiers 1,2 and 3. It is vital to highlight that processing the required analytics does not always being completed using the tiers approach. The tier level architecture might not be existed in a non-hierarchical SOC environment where all analysts are required to have a comprehensive skill set to carry out their duties (Agyepong et al., 2023).

Analysts are also known to be part of the blue team of an organisations network where they constantly monitor activities. With the occurrence of

alerts, any critical event is firstly reported to different groups including red and purple teams then patching will be carried out on the reported vulnerability (Aung et al., 2020).

Enormous cyber security threats can occur at any time where a lot of automated defensive measures are adopted to defend infrastructure. IPS/IDS, SIEM and antivirus systems are part of the automated tools that can be developed to protect appliances. The majority of businesses have implemented SOC to acquire a centralised control systems over their network and to manage their vulnerabilities gaps. But SOC rely on the human aspect in delivering processes based on the collected data by the defensive tools. Analysts are supposed to evaluate these data and provide situational awareness of such an event in order for the response team to act upon a threat in an efficient and appropriate manner. Zhong et al. (2018) indicated that in order to retrieve a situational awareness there are numerous concerns to be raised. Is the network currently encountering a threat? if so, how did it take a place? as a result, what are the next stages to be taken by threat actor? these are the questions that are highlighted by authors.

Providing answers to these concerns can be clarified by carrying out effective data analytics according to Zhong et al. (2018). Analysts are able to explore the immense gathered data from various sources to slowly grasp knowledge. The most essential task of analysts is data triage due to its effectiveness in spotting outliers to reduce the noise and refine data. By applying different rules techniques, malicious events can be identified for additional investigation.

There are a variety of operations that can be conducted by analysts to carry out data triage. A filter process can be applied to filtrate data based on set of rules. Then, a select operation can be used to detect the data of concern. A search process can also be added to operations in order to search for data with particular attributes. Retrieving an overall division of network logs that require additional analysis can be gained with a combination of the mentioned operations that are useful in grouping out unprocessed data sources. Data triage is a vital process for analysts to examine data for the identification and detection of malicious activities on the network. It is the first phase of the analysis where analysts are expected to conduct immediately and quickly. Exploiters currently carry out cyber attacks using multiple stages over a longer period to obtain their main goal. The triage does not only include long and tedious analysis but also require analysts

to have significant skills that they gained from prior events (Zhong et al., 2018).

2.9 Types of Logs

With the ease of use and the rely on networks, network traffic have become one of the most standard data that can be gathered as input for IPS/IDS purposes. Information associated with network might not be visible internally and in some scenarios, it will be depending on internet service provider ISP. Identifying threat actors addresses and paths can be classified by the usage of packet capture files which can be illustrated by either Pcap, tcpdump or Wireshark systems. Pcap library exists as open source which explain its usefulness and success. Based on the period of a particular detection project, various datasets are often presented and made visible as Pcaps for the purpose of detection evaluation (Debar, 2019).

According to Debar (2019) Pcaps require large amount of storage space where they can be reserved for research and forensics aims. The existence of Pcap library depends on network interface, which means that an interface is required to be available in order to collect the traffic as well as packets that are not directed to the network. Even with the popularity of traffic packets logs, there are variety of obstacles that are required to be highlighted when dealing with Pcap file format.

The number of Pcap files can be enormous which make it complex and limit the capture of any technical process or investigation. Therefore, sensors usually examine traffic from network in real time without recording the running packets. The size is also a challenge where Pcap library often retrieve IP packet headers only. The existence of header information only can reduce the effectivity of tracking such a packet which limit detection methods. Data that is distributed through network are usually recorded in segmentation or fragmentation basis. This requires a software that has the ability to rebuild application data stream where some information could be missed in terms of initial stages or ends of a communication. Also recording timestamps rely on an external software that can add timestamp to packets as their headers do not contain record of time details. One of the most important aspects when analysing Pcaps is examining the application layer. For instance, trusted transports like TCPs include information that need to be highlighted such as if a connection has been established or not. Thus, at an application level where TCP/IP is presented, details might be unreliable

in headers or require a knowledge of the logic of such an application where it is almost difficult to understand or acquire (Debar, 2019).

On the other hand, application logs such as web server logs, files and documents are some of the types of logs that illustrate an event stream about particular activities on a specific system or application. Comparing to system logs, applications logs are closer to realistic and accuracy because of the details that are being produced. These logs are originally created for the purpose of system controlling and debugging. Therefore, they are clearly written texts and understandable. With the existence of syslog infrastructure applications are capable of sharing logs. An example of a log file is known as auth.log which comprises information about user connection despite the approach that has been used to establish that connection whether it used SSH or different method (Debar, 2019).

Accordingly, Common Log Format (CLF) and Extended Common Log Format (ECLF) are common sources of information that can be presented by web server logs. In fact, these formats are generated by various servers such Apache web server. Documents that provide normalisation standards do not exist in this type of format similar to Syslog. For example, the standard of W3C is associated with draft as it is an easy and straightforward to analyse. Any information about a request that has been made by a client plus the response from the targeted server are stored in W3C format. There are challenges related to this format in terms of lack of information about the server. For instance, the generated log is stored locally on a machine once a request is being made. Then, server logs are written once a response is being generated by the server. Therefore, an attack would‘ve already been happening when a sensor obtains log details. As a result, IPS/IDS cannot be fulfilled with this information only and they require interceptors to be in-place in order to stop or change a request content (Debar, 2019).

Application-level information also include files/documents that can be identified either over the network stream or located in systems. They consist of documents contain information generated by various applications. In fact, threat actors usually find it an effective way to plug malwares into application-level documents formats such as PDFs and office documents. These types of documents provide interesting opportunity for attackers to exploit targets via including malicious code in them. The distribution of malwares documents can be performed via emails or internet where a trace can be identified of such an exchange to uncover embedded malicious code

like JavaScript code. Regardless of the type of document whether it's a PDF or TLS certificates, in some situations, it can be difficult to analyse information in documents. Hence, attackers can expose risks via these gaps and vulnerabilities. Documents that are acknowledged as rich document formats are recommended to be presented in well written texts to avoid unmistakable interpretation. This can reduce the gap space for attackers to execute their threats. Nevertheless, the usage of such documents as source of information to detect malwares have grown more than before (Debar, 2019).

The variety of operating systems also generate logs for different purposes such as identifying and removing errors by the process of debugging. In some cases, OS logs can be ineffective for IPS/IDS due to the absence of rigorous. An example is a Unix accounting system that will only register the first few characters of a user's activity. As a result, a command path can be missed which expose difficulties to identify activities associated with identical names at various locations (Debar, 2019).

In contrast, kernel logs monitor the internal activities and operations of an OS. They are known as endpoint protection that target different number of devices as they developed into a universal term for antivirus instruments. This underlines the main issue of not only providing protection to systems but to applications as well. For example, browsers and mail client do not only transfer data but can execute malicious and untrusted codes that are supplied by external sources. Kernel logs depend on dedicated interceptors to identify activities that they only intent to investigate (Debar, 2019).

More in-depth information that can include reports of boot processes on Unix/Linux assets or on the core kernel activity are usually associated with the infrastructure of a Syslog. Another example of a system log is acknowledged as Syslog. It includes valuable amount of information and data sources that can be used for many purposes. The primary source of these types of logs is known as Syslog protocol. A Syslog is generated from a detected source where it comprises time-stamped text message. System log usually consists of different segments that introduce variety of details on particular activity. Details of the occurrence of an event on specific date and time are often provided in text format and counted in the time-stamp segment of a Syslog. Hostname information also provides details on the asset that generated the log which could be an IP address or an identical name. The name of the program that produced the log is associated with

the process header. One of the most important types of information that can be identified is the priority of a log. This contains details about the classification and seriousness where its severity normally considered in a scale format. As any log an ID of it will be included in the PID details of the log (Debar, 2019).

Overall, the message part of a Syslog is provided in an ASCII 7-bit format. Categorisation and orientation of logs are also facilitated by the Syslog usage. The storage of these information can be found in variety of locations. For instance, in Unix/Linux OS they can be identified in /var/log/ path or directory. A Syslog can also be a protocol that is able to run on User Datagram Protocol UDP/513 port. This is useful to simplify the transmission where UDP is able to be resistant and robust. More precisely in difficult network circumstances where messages could be dropped but UDP would not drop its capability. Nonetheless, the usage of UDP need restricted segmentation and the recommended size limit of a Syslog message is usually equal to 1000 bytes. Accordingly, centralising events and alerts in the implementations of SOC can be depended on Syslog due to its extreme effectiveness (Debar, 2019).

2.10 Automation and Machine Learning (ML)

Demertzis et al. (2018) stated the key purpose of SOC is to be able to analyse large set of data and correlate other categories of events. Authors also mentioned traditional network monitoring software solutions are producing huge number of false positives due to the lack of accurate prediction processes. Manual processes can provide hackers with the advantage of having more time to accomplish their malicious activities. Thus, SOC analysts are required to apply automated mechanisms to help them in detecting threats.

Venherskyi and Karpiuk (2021) added variety of cyber security threats can be detected via applying ML methods. Abnormal activities, brute force attempts, malware infections and more other network traffic monitoring are the benefits of ML. Organisations can save a lot of cost by applying certain algorithms that have high accuracy of identifying anomalies. SOC is currently facing a huge challenge in finding a balance between the huge number of generated events to the smaller number of professionals and skilled analysts. There are a lot of questions that are still and will be asked in terms of the number of events. For example, how alerts can be reduced and if so, what is the main input sources for analysts?. Part of the answer

can be found by correctly applying correlations rules. Also, reducing the number of false positives can play a huge difference in SOC development. Analysing datasets and using calculations such as deviations is a significant approach in reducing the harm of threats by early detection. In analysis, statistical thresholds can be ignored to increase the quality of correlation rules. However, some of the data can change quickly which will results to inconsistency and less quality. Hence, after analysing such data, it is effective to apply ML algorithms to generate better quality results.

A lot of organisations are operating their SOC by relying on SIEM. It is identified as effective control tool that have the ability to automatically collect large set of events in real time environment and analyse them based on predefined rules. The produced events are classified differently based on their type to prepare an effective response to each of them. Threats that are generated can be presented differently on security appliances via tickets. Predefined rules and signatures are usually implemented to describe threats classifications and events. The set of signatures are mainly used to deal with a huge number of alerts such as decreasing the number of false negatives which are genuine attacks that are categorised as normal alerts. In contrast the number of false positives is rising which are events that classified as threats events, but they are not. In fact, SOC analysts do not have the ability to react on all of the generated events as the number of tickets can be extremely overwhelming (Kim and Kwon, 2022).

Kim and Kwon (2022) added that analysts are often able to respond into up to 29% of the detected tickets where 40% of these tickets can be recognised as false positives. Establishing successful data classifications models can be difficult for different reasons. For instance, a huge set of data including security events are required to train such models. The required time for training and amendments might be needed when a new threat occurs. This makes it hard to act on events in real time scenarios. Any types of responses delays expose SOC to fail in implementing effective defensive measures. Efforts have been set now and before to implement efficient threat detection approaches based on AI and ML which would help in mitigating the number of false positives. Neural network models such as Naïve Bayes, Decision Tree and Support Vector Machine (SVM) algorithms can be used for threats classifications.

A sufficient effective model cannot be established without highlighting both threat classification and model learning. Responding to new attacks

such as zero-day threats is part of the learning process that is required to build valuable classification prototype for SIEM. A successful defence system is associated with the learning time and updates. It is vital to consider the time that is required for threat classification and learning. In threat classification, the expectations are to quickly detect and identify threats that are produced by assets. If not, then the targeted systems will be exposed to vulnerabilities. In some cases, threat classification cannot be applied into environments that include devices with law performance processors. Hence, it is important to apply models that have capabilities of quick classification (Kim and Kwon, 2022).

Kiiveri (2021) emphasised on the need of new tools to adapt on the change of cyber security threats environment. The emerge of technologies such as: IoT and cloud has increased the attacks landscape. As a result of that, cyber security tools that support automation like SOC are required to fulfill security gaps where automation is set as high priority for most firms. The key element of automation in security tools is to improve detection and monitoring abilities and not to replace security analysts. Security skills shortage is another fact of the need of implementing automation where market is in high demand of cyber security professionals. With the implementation of SOC, productivity can be increased to detect and respond to malicious activities.

Lack of skilled employees and absence of effective automation processes are amongst the reasons of SOC failure according to SANS institute survey. The survey defined SOC as a combination of people, processes and technologies that work towards defending organisations IT assets. Various North American and European organisations were targeted to achieve the outcome of the survey. Organisations and SOC leaders can benefit from the outcome of the survey to optimise their current SOC or to build knowledge about establishing a SOC from the scratch. The reality is that automation processes are still not efficiently implemented as they sound. It will take more time to be fully relied on as technologies change continuously. Therefore, AI and machine learning have proved to be useful solution in supporting both skilled and less skilled analysts (Crowley and Pescatore, 2019).

Huge number of alerts are generated constantly via SOC. Engel et al. (2021) suggested that grouping similar alerts based on similar issues is one of the automation that can be implemented to support analysts in resolving

the same issues more efficiently. Alerts that are part of the same source and are regenerated for the same reason can be classified into a specific alert sequence, which in turn can also be categorised into alert groups. Alongside the adoption of grouping policies, minimising more incoming alerts can also be achieved by AI. The services of AI can verify incoming alerts, then group each alert with already saved ones. AI can also provide suggestions then verify the suggestion to change the group of an alert accordingly.

There are benefits to achieve from the verification process, where AI services can be enhanced for future grouping. Changing the group based on AI service suggestions is more efficient instead of creating a new group every time an alert is being generated. This helps in reducing time and increasing the quality of work by investigating more alerts throughout the day. However, not all incoming alerts can be grouped together because a similar attack or incident can take a place at different time on another location. Rule-based values such as time or location is also effective for new generated alerts in order to not group them together with an existing alert that already have been investigated and closed. Therefore, more clustering for incoming alerts is required by the AI services (Engel et al., 2021).

Specialists agree on the need to develop and improve cyber security defence environment via AI and ML algorithms. AI defensive measures provide better performance of detection cyber risks. Mathew (2021) added that the future of cyber security defence is ML which is part of the AI. It is important to enhance information systems by learning from data without the need to use precise programming approach. Implementing algorithms to extract data and search for patterns are the mathematical methods that ML is normally based on. There are several ML algorithms that are commonly used such as Association Rules, Bayesian algorithms and Decisions Trees. However, cyber security solutions are more focused on ML algorithms nowadays due to the ability in clustering practices to provide a clear picture of the probability of attacks.

AI can also be referred to the ability to use intelligence by criminals to conduct more sophisticated attacks. On the other side organisations require AI to implement more advanced measures to counter these threats. Defensive techniques that use AI have revealed their capabilities in handling modern cyber security attacks (Google, 2025).

Achieving high accuracy in detecting almost all threats is impossible to

achieve. The utilisation of ML methods helps if appropriate techniques are executed. The need of ML in SOC is increasing rapidly due to numerous reasons. Many organisations suffer from the lack of high skilled analysts which lead to inefficient threats handling. Systems are required to be continuously monitored 24/7. Therefore, analysts are in need for ML models that can correlate and gather data from systems traffic. Correlating the correct needed data can be a complex task. Analysts must be aware of the importance of aggregating the right data that can help in providing an overall view of a specific problem. The cost and time are also part of the facts that ML needs to be applied for. Employing too many analysts can be time consuming and expensive. Some significant alerts can be ignored and this problem can be solved via already implemented ML techniques (Sopan et al., 2018).

ML have the ability to continuously learn from data aggregation and correlation. Training and inference are two different stages of ML. Obtaining the expected results can be achieved by the training phase where ML models utilise labeled and unlabeled data. Supervised models are often associated with labelled data that contain labels to attain the desired outcome. On the other hand, unsupervised models are used in the case of when unlabelled data are being utilised. Achieving the expected results can also be done by the inference phase where the already trained models are consistently observed and executed in a real-time environment (Feng et al., 2017).

A generated log can describe a message that is associated with activities on the network that lead to state alterations. Any occurrence change might consist of time, date or a label that detect the location of the change. Events that share similarities in terms of purpose, function and structure are often recognised by the event type label. Malicious activities and actions are usually included in a security alert which is an event that comprises details about unexpected behaviour that could expose gaps and vulnerabilities. It is known that security events are regularly produced by security assets such as IDS/IPS, firewalls and antivirus software. The establishment of framework between events is always performed by event correlations. The aim of correlations is to detect and recognise the meaningful of events in datasets. Similarity-based, step-based and mixed correlations methods are classifications of the correlations approaches that can be executed (Levshun and Kotenko, 2023).

Mixed approach is linked with the adoption of variety of correlation tech-

niques. It provides independent processes that prevent each algorithm from taking over the other. More precisely, mixed correlation method utilises different algorithms where each of them is unable to have predominance. Similarity based methods are widely disseminated in cyber security processes. They have the capabilities to evaluate and provide comparisons based on events characteristics. Any identical attributes can be calculated via the adoption of mathematical functions such as Euclidean or Manhattan, correlations factors and more other functions. Identical events that correspond to the same kind of threat is the primary key of similarity correlation method. In contrast, step-based correlation approach corresponds to the creation of chains that contain series of events, actor's behaviour and analysis of links amongst different events. Without any previous knowledge this type of method is able to identify similar security actions in accordance with chain signatures and classify event series based on statistical affiliations. The required source of knowledge for this type of method is achieved by utilising threats scenarios and vulnerabilities repositories. With the implementation of step-based correlation approach, it can be split into two sub-methods of casual based and data mining. Using statistical analysis to identify certain patterns in datasets is known as data mining. Analysing the fundamental structure of events to retrieve chains where preceding procedures define the upcoming ones. Accordingly, there are differences between data mining and ML. Mechanisms that contain methods of Bayesian network, classifications and regression analysis are part of the data mining wider area of AI. Therefore, ML is one of the fields of data mining (Levshun and Kotenko, 2023).

Figure 2.10.59 below depicts the categorisation of some of AI correlation frameworks based on event knowledge which also described as the state of art according to Levshun and Kotenko (2023). The stated models included rule-based, semantic, graphical and ML as part of used labels in ML approaches. A rule-based model is usually associated with the normal relationships amongst events. In fact, it relies on knowledge repository that comprises specific rules that assist in matching events characteristics. It can be summarised as a description of knowledge based on rules to evaluate and combine security events. Semantics frameworks are different where particular conditions are used based on specific language syntax. Semantics rules help in distinguishing correlation between input and output data. For example, an event can be recognised based on set of characters that represent a particular word and formal grammar in existing language. Thus, the knowledge description based on language syntax and semantics is the

definition of semantic based technique.

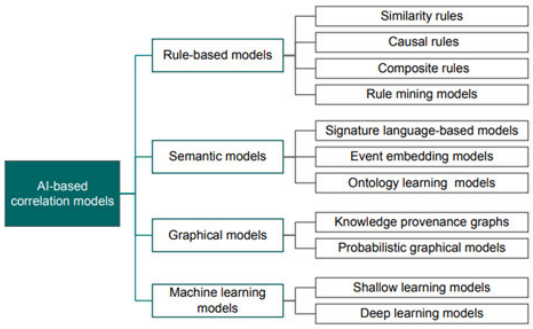


Figure 2.10.59: Artificial Intelligence Correlation Frameworks (Levshun and Kotenko, 2023)

In contrast, graphical models are often used to define some knowledge about events via utilising graphical networks. Nodes that illustrate objects are applied to find the relationships amongst these objects. Hence, graphical models are defined as the representation of knowledge by using graphical networks. ML frameworks are associated with the analysis of events by applying intelligent techniques. For instance, clustering is part of these methods that represent data values. ML models are effective as they permit the process of a large number of data knowledge about certain event analysis. They utilise frames to represent data where the frame is the AI structure that contain values and attributes. Consequently, a data structure that represent knowledge of events collection including their properties and values is the known definition of ML models (Levshun and Kotenko, 2023).

Establishing a context amongst new captured events and previous detected ones is the process of correlation. This helps towards the analysis to determine the next steps that an attacker could take. The aim of AI security event correlation models is to identify and predict future threats based on their nature. Levshun and Kotenko (2023) also added that events correlations can face a challenge of hiding anomalies. The detection of multi-step threat is challenging as an attacker can conceal his/her movements. Drawing a full knowledge of an attacker's behaviour is usually challenging even with the detection of such an attack. Therefore, events correlation models can suffer from the loss of data. Unsupervised malicious detection approaches can also be misled to distinguish the legitimately of an event. By providing events background and their semantics, this can help in analysing attack-

ers' behaviours to resolve this type of challenge. According to Levshun and Kotenko (2023) outlining variety of behaviours is an effective technique to use.

Sopan et al. (2018) investigated alerts with SOC analysts from cyber security organisation. The analysts use cloud platform to monitor alerts that are triggered from various systems based on IoC approach that is created by cyber security specialists. The web platform allows analysts to review raw data of alerts plus request more in-depth details of an alert to distinguish if it's real or false. Based on the investigation, an alert can be categorised as threat or false positive.

Authors have built a ML model using the approach of categorising alerts as genuine or false. The aim of the model is to offer analysts with alerts prediction approach using ML that adopt similar features to an analyst mind model. Also, to spread confidence amongst analysts to use the model. Another aim is to validate the model and receive corrections from stakeholders to enhance the prototype performance. The identified alerts worked as training data for the founded model. Figure 2.10.60 below illustrates the structure of the model. The workflow begins with a system to detect signature-based alerts from various endpoints then deliver them to analysts. In the proposed model, alerts are sent through ML technique that specify the reality of an alert. The alerts then marked with prediction labels and provided for further investigation. Combining raw data of alerts, prediction labels and analysts' investigations, an overview of the model performance is then presented to shareholders (Sopan et al., 2018).

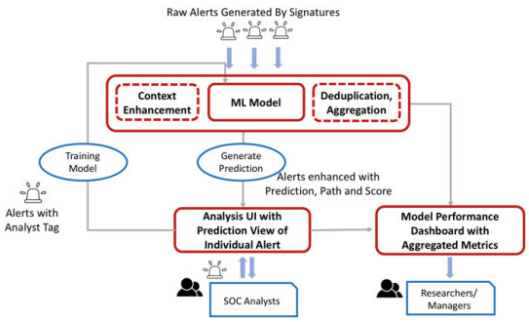


Figure 2.10.60: Machine Learning Model (Sopan et al., 2018)

The user interface of the model presented prediction model for alerts

when tested but it has been changed to threat score instead to make it more clear to analysts. The expected score of such an alert is presented as 70% false positive probability and 30% threat probability. The results of the model are associated with conducted feedback with analysts. Based on the feedback an automation rule for investigations decisions is created to match all the predicted alerts. An alert is predicted and tagged as 93.1% confidence that it is a false positive but in fact it is a malicious one that is detected by different tools such as Virus Total. The set features are not efficient to cover all alerts. Another alert is predicted with 60% false positive probability but it was clearly a malicious one. As a result, the model is not sufficient enough for new alert types, as the misclassified ones were not used in the training dataset. The new alerts have new signatures that can lead to incorrect prediction by the model which would stop analysts from using it. Sopan et al. (2018) admitted that the occurrence of new signatures alerts exposed the model to failure. The authors recommended in the future to implement a confusion matrix that can provide an overview of similar alerts with similar signature before the prediction process. The matrix can include details of such an alert with same signature of inaccurate predicted one and how the model behaved when the prediction took a place.

Overall, the model is not effective enough based on the feedback and the results. According to Sopan et al. (2018), they have conducted 6 interviews which lasted 1-2 hours with experienced SOC analysts. The results and the number of conducted interviews is not enough to say that an enhanced solution have been implemented and all SOC analysts can use. The model can assist in some cases where an occurred alert already been used in the trained data.

Ndichu et al. (2021) developed an approach that automate threat alerts and highlighted the issue of imbalance in appliances alert data. Neighbourhood Cleaning Rule (NCR) is used firstly to identify false positives. Support Vector Machine Synthetic Minority Oversampling Technique (SVMSMOTE) also applied to produce true alerts for training objectives. Then the alerts are classified via the adoption of Decision Tree (DT) and Random Forest (RF). Up to 8 systems were utilised to generate the alert data to present the model's ability of reducing the demand of manual analysis. Figure 2.10.61 below depicts the delivered approach to detect critical alerts from imbalanced multi-appliance threat alert logs.

Figure 2.10.61: Critical Alerts Detection Approach (Ndichu et al., 2021)

Accordingly, the amount of security alerts are decreased significantly, but Ndichu et al. (2021) added that different approaches can be used for future studies to enhance precision metrics such as; probability tuning and mixture algorithms. They added that an appropriate labeling of data can improve the process of decreasing the amount of false negatives and false positives which also lead to an enhancement of threat detection (Ndichu et al., 2021).

2.11 SOC Challenges

When building a SOC, it is recommended to establish a central point that works as location to monitor security events in a real-time environment. Independent monitoring and detecting threats modules are solutions provided by SOC to help managing various layers of network activities. Integrating these modules can be delivered as complicated solution to threat detection problems. An example of the problems is data traffic identification that is associated with unusual user behaviour. In this case, network traffic module can be applied to protect the system from potential threats. This can be achieved by creating profiles in advance for any protected system, where the profile provides information of the system components when it is believed as secure. Applying such a module is one of the challenges that analysts face (Bienias et al., 2019).

The evolving threats require advanced technological solutions to forbid threat actors from carrying out their attacks. AI helped improve their tactics to overcome traditional defenses. Hence, it increased the challenges on the cyber security team (Jurgens and Cin, 2025).

Oesch et al. (2020) conducted a study on the usability of ML by SOC analysts. Participants of up to 6 analysts were part of the study that was sponsored by the US navy. Various challenges associated with usability flaws are identified such as usability violations of the design of user interface. Analysts are also found to not trust and mishandling the generated scores by applied tools which resulted analysts of clear lack of mental model. Un-

expected findings in regards of analysts' performances included that there was no correlation amongst analysts' level of education and their experience working with SOC. Thus, having in-advanced knowledge and personal attitudes can impact either positively or negatively on the usage of ML tools.

Based on the findings that included tools misuse and the inability to follow a user interface design, recommendations were suggested by researchers to improve the usability of ML tools. SOC users are suggested to be involved in the Software Development Life Cycle (SDLC) of ML tools so valuable tests can be conducted during early phases. Different levels of experienced analysts can play a key role in providing effective evaluation before the entire release of such a tool. ML tools are not useful enough if analysts are unable to interpret the scores that are produced. This is also mentioned in Sopan et al. (2018) work where the user interface prediction score was amended to threat score instead so analysts can clearly understand it. Therefore, vendors are required to ensure that comprehensive interpretation tests are validated prior and while using ML tools to guarantee the effective usage of them (Oesch et al., 2020).

As part of analysts' operations they also interact with other SOC specialists including incident response team, penetration testers and cyber forensics experts. Analysts are expected to present high level of performance. Any lack or inadequate performance can impact negatively on the productivity of SOC operations. Key performance indicators that are also known as KPIs are often being used by SOC managers to evaluate analysts' performance based on certain criteria that could be set by stakeholders. Studies showed that difficulties could be faced by SOC stakeholders in terms of fairly and equally assessing performance as Agyepong et al. (2023) stated.

The current and existing performance methods are insufficient and challenging. Agyepong et al. (2023) used the term of SOC stakeholders to identify various roles in SOC environment. This include incident management manager and SOC supervisors who can be involved when performing KPIs with analysts. There are other gaps and problems that occur in performance measures where different elements of operations do not get recognised by SOC stakeholders. For example, the quality of an analysis and managing false positives. Failing to consider the priority of a handled alert in a performance metric is amongst the concerns as analysts are supposed to evaluate alerts based on their severity and priority. Ignoring logs priority and only assessing performance depending on the overall number of actioned events

can reduce the overall quality of SOC processes (Agyepong et al., 2023).

This can expose analysts to be lazy and only deal with easy and low severity events. An overall picture of analyst performance could be missing in existed measures which could lead to the feeling of efforts ignorance. In different scenarios, SOC managers only emphasis on the quantitative achievements to action large number of logs whilst ignoring qualitative aspects including the quality of triaged events. The absence of an efficient method to assess and evaluate performance can expose risks to both SOC stakeholders and analysts. Agyepong et al. (2023) proposed a method called Analysts Assessment Method (SOC-AMM) that can be useful to enhance the evaluation aspects of an analyst performance. The method provides a comprehensive and systematic approach to acknowledge vital elements of various functions. The quality of an event analysis and reports can be evaluated effectively using the method. Both experienced and junior analysts who face difficulties from incidents analysis operations can be benefited from SOC-AAM.

Figure 2.11.62 depicts analysts' operations and the expected goals. These objectives are also identified as analysts' functions. They are vital to be identified and highlighted for developing and implementing a method that can outline the overall performance. These recognised functions can be utilised as a set standard for analysts' performance evaluation. When assessing the performance, it is essential to have a sufficient evaluation approach that include a set of well-specified criteria. A method is recommended to contain analysts demands and their experience. On the other hand, this can expose challenges due to the variations amongst SOC where they can be different from each other. Monitoring and detection, analysis, responses, reporting, vulnerabilities, intelligence and all other objectives are the core functions of analysts that have been classified to be used in evaluating performance. They are expected to perform real-time monitoring of various network traffic including user behaviours and activities. Detecting false positives and false negatives would help in noise reduction that can be overwhelming for both analysts and sensors. Moreover, observing security assets such as firewalls to identify any policies and user activities breaches (Agyepong et al., 2023).

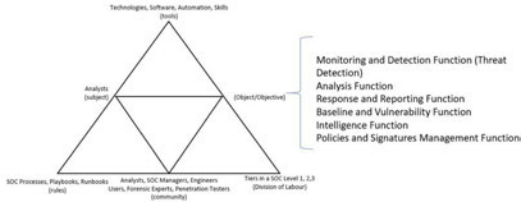


Figure 2.11.62: SOC Analysts Functions (Agyepong et al., 2023)

SOC is developed and used by all sectors including private and public organisations. Even with the growing usage of SOC and being a broad research subject there are still gaps that have not been effectively and adequately highlighted. One of the key areas that need to be addressed is the satisfactory metrics when evaluating analysts' performances and highlighting the challenges that they are exposed to. Agyepong et al. (2020b) agree on the need of applying improvements on metrics that are set to measure analysts' functions. In prior studied situations some analysts were not satisfied with the implemented metrics as they claimed that they do not holistically consider various elements of their tasks and functions. Regardless of the issue, there are little efforts from scholars to examine the current metrics for further enhancements.

SOC can fit in to any environment that uses IT infrastructure. The need of SOC implementation is not only linked with traditional business firms and organisations. Its usage is versatile and expanded to also include maritime field. The digital revolution provided substantial advantages to maritime industry but with also exposing it to more sophisticated cyber-attacks. Raimondi et al. (2022) added that the number of cyber-attacks that target maritime systems have increased rapidly emphasising on the current complex threat environment. The infrastructure of vessels' traditional operation technology is currently connected with up-to-date information technology components. Hence, SOC can play a key role in addressing the lack of updated threats reports and develop vigorous countermeasures methods. One the other hand, employing SOC in maritime also poses challenges such as the lack of domain knowledge expertise but it can be resolved by delivering comprehensive training.

Monitoring infrastructure and hands on integrated navigation systems can be part of the training which assist in controlling the environment. Mar-

itime infrastructure can be associated with well-known information systems. Thus, SOC can operate efficiently and engage smoothly according to maritime perspective. Nonetheless, some of the infrastructure can be distinct from the traditional ones and SOC maritime operators are required to adapt accordingly to improve their knowledge in such situation. In SOC environment, analysts are usually distributed within a tiered structure based on their knowledge and experience. This structure is also implemented in the maritime context as Raimondi et al. (2022) mentioned in a paper related to training maritime SOC teams.

Events correlation can be applied into logs to find the relationships amongst alerts that have been previously produced for future processing. It helps identifying the most meaningful alerts in the generated dataset. The main goal of it is to provide quality to dataset by reducing the number of events and interpreting them. There are different challenges occur when developing such an approach "logs correlation". It is important to not only detecting anomalies but also to be able to follow their footprints. Due to some technical and systems implications, it is often hard to define the overall picture of an event logic. More specifically if an organisation uses large complex of distributed network. Attackers are able to hide their trail by maneuvering their actions (Kotenko et al., 2022).

Hiding abnormal patterns in log correlation is one of the challenges that being faced by analysts. Describing the cause of events can be difficult when alerts are generated from tools such IDS/IPS as some of the information can be insufficient. This often leave a gap between high level of system behaviour and low level of audited logs. The usage of signature correlation approaches is usually required to be renewed constantly to keep updated with threats patterns and specialists' rules. Creating a security knowledge base platform and review it regularly can be quite challenging. It is also difficult to analyse large amount of data and correlate them specially when different systems are generating them. The need of sophisticated digital resources is vital to process data and correlate them accordingly (Kotenko et al., 2022).

By recognising the mentioned problems, Kotenko et al. (2022) proposed future ranges of research to improve events correlations methods which can be effective in encountering challenges. First of all, it is important to study attackers' behaviours by considering the semantics of alerts. Such an analysis study helps in identifying similar patterns based on attackers' attributions. It is also vital to develop event correlations approaches by adopting

correlations algorithms. The development of learning knowledge base is useful when it comes to understand well-known attacks signatures. Predictive analytics is also amongst the suggested improvements due to its capabilities in predicting whether an attack will take place or not.

This can be implemented through the adoption of ML and AI. When dealing with large amount of data, tools that support big data are highly recommended. Especially in the event of supporting distributed event correlation. Data normalisation and unification of alerts are introduced as future improvements as well. Researchers added that a number of events normalisation approaches have been launched and used by business-related communities (Kotenko et al., 2022).

In contrast, these methods that includes might not be effective enough to distinguish the relationships amongst alerts due to limitation in fields numbers. To evaluate correlation approaches, the development of up-to-date dataset is needed. This can be achieved via the publication of experimental data. For instance, some information and data cannot be shared due to confidentiality, but authors can disclose it upon request for research and improvements purposes. Having the opportunity to assess the methods on current dataset and new ones is an effective approach. It helps in evaluating the efficiency of such an approach for event correlations by considering various types of threats (Kotenko et al., 2022).

There are various inefficiencies factors that prevent SOC from being effective. The lack of monitoring; a good number of organisations are believed to use SOC for monitoring only a small portion of their systems. Onwubiko and Ouazzane (2019) argued that in some firms SOC only monitor 5% of the systems. The quality aspect seems to be absent where organisations are recommended to implement custom efficient use cases instead of relying on general basic monitoring. Some processes such as; events playbooks are meant to be added to SOC. In some cases, they might not exist or if they do exist, they are not updated accordingly. As well, the lack of SOC capacity and standardisation are associated with skills shortages in cyber security and organisations who have different understanding of SOC perceptions.

In a lot of scenarios organisations ignore end-users when implementing security measures. Traditional security frameworks are usually developed to defend systems. Firewalls, IDS/IPS and other prevention systems are example of these traditional security measures. Such security approaches

are part of SOC that have limitations. For instance, correctly configuring firewall can be difficult task to achieve. Users might also face obstacles in performing internet-based activities until a firewall is set up efficiently. Systems can also face service slow down due to implemented security policies. SOC elements are required to continuously be managed and controlled for any upcoming updates. Services including data analysis via SOC aim to analyse network traffic to catch and prevent malicious activities as early as possible. Also, SOC introduce information security management systems to conduct risk assessments. Hence, these types of services must be applied correctly without impacting on the other sides of the business (Nalanagula and Roy, 2022).

Implementing the correct services is essential when constructing SOC. Bikov et al. (2021) added that organisations are facing failure when inaccurate services are being applied. The lack of having a clear strategy is one of the main challenges that occur with SOC implementation. Threat monitoring, threat hunting and threat investigation are the suggested areas of focus. Covering these aspects helps in triggering meaningful alerts so analysts are able to understand and identify the required data. Establishing a strong architecture begin from the first stages where SOC team is suggested to gather and grasp the requirements effectively.

SOC is a protection central that aim to handle security incidents due to its capabilities in monitoring and preventing threats. It is one of the complicated defensive systems and only limited numbers of researchers highlight the problems associated with SOC. A literature was conducted by Danquah (2020) contained various concerns that might arise for justifying SOC budget. For instance, how a compromise will be detected and the severity of such an incident. The impact plus the responsibility for threats detection and the reaction to events are also amongst these questions. Once an incident occurs then more concerns arise of who will be dealing with it and if the triage is required to be transmitted internally or externally.

To overcome the mentioned concerns and challenges, Danquah (2020) suggested a technique called "OODA" that was founded for military purposes. The methodology stands for Observe, Orient, Detect and Adapt. It was implemented to justify budgets for SOC. From a cyber security aspect, the first phase of the OODA is observe. It is to monitor systems and collect data from network end points. The orient step is valuable to analyse incoming and stored data via appropriate tools to spot any anomalies across

network. Based on the gathered information and analysis results, the decide phase helps in determining required actions to be taken. Acting upon previous phases is the last step to execute the required decided action.

For future statistics analysis by SOC, data associated with logged events and alerts that have been generated from various network appliances and tools are usually stored in a log management repository. Therefore, log management exposes SOC to different challenges such as categorising, filtration and parsing logs. Security devices are usually generating logs in various format, .csv and .xml are examples of these logs. A server that plays a role of collection server is required to transfer these logs into. Communication protocols can be used to transfer logs from instruments to the collection server. Being able to provide an effective and successful communication amongst units and systems is achieved via simple parameter. The main challenge here is transferring these data and not the structure of a protocol. Identifying a unique format is suggested for log management production and correlation input. Categorising logged events is a huge challenge that SOC users are facing. Madani et al. (2011) compared logged events into three different types. Anti-virus software, IPS/IDS, firewalls, routers, switches and servers are amongst the security appliances categories.

They provide details of an event id or rule id that can be useful for correlation purposes. Accordingly, operating systems category include specific types of operating systems such Linux and windows. These logs can be correlated with each other unlike application logs category that are required to be correlated separately. SOC use stored logs for analysing and auditing purposes via applying forensic standard methods. There are legal concerns that might occur in the event of detecting such an event if a prosecution is required (Madani et al., 2011).

Determining if an alert is genuine to highlight if an attack could be discovered or not depends on the quality of such an alert. System audit policies can be configured on log sources to ensure the high-level quality of the produced alerts. Triggering an alert in the case of log file deletion or even if tempted to do so is an example of a system policy set up. It is also recommended to define policies that trigger alerts in the occurrence of the following events: deleting password, copy password, set up of a new account, deletion of an existing account, privileges escalation to admin and root levels (Onwubiko, 2015).

Kokulu et al. (2019) conducted a qualitative study by interviewing various SOC analysts and founded the following challenges. The visibility of network endpoints and infrastructure can be low which impact on the effectiveness of SOC processes. It is one of the most common problems that analysts are facing. Phishing attacks are also major concerns where employees are required to be trained efficiently to prevent such attacks. A major phishing attack occurred during the 30 days just after providing phishing training to employees. This indicates that training is not as efficient as expected in practical. 18 interviews are conducted to retrieve findings and based on the research; participants did not consider false positives as severe issue in SOC. Nonetheless, in academia these alerts can be fatal in automatic detection, and 5 of participants have raised some worries about unfiltered and uncorrelated alerts data.

The challenges findings cannot be generalised as agreed by authors and results are limited due to the interviews number. Different issues are identified as well and based on findings, managers are advised to communicate more with their analysts to increase the efficacy of automation and tools functionalities. Also, unique metrics can be in place for analysts to use, but they must be justified to understand the reason behind using them. Kokulu et al. (2019) added that by explaining metrics to analysts, managers will be able to gather useful insights feedback and SOC analysts will feel more confident and comfortable.

The possibility of security threats has increased significantly due to the improvement of digital environment, where SOC is being implemented. Alharbi (2020) conducted qualitative study on SOC at several organisations. Participants have highlighted numerous challenges such as high false positives, the insufficient quality of threat intelligence and low quality of automation level. Studies are aiming to enhance SOC by exploring these challenges that organisations are facing. Investigating high false positives more in-depth to propose an effective solution is recommended for future research (Hall, 2025).

Mutemwa et al. (2018) stated that integrating SOC into an organisation expose various challenges in terms of people, process and technologies. People integration means analysts must work and integrate smoothly with other employees. Communications skills are the main key element when working with people from several department and roles. When introducing SOC, a gap can occur where the stakeholders of technologies and processes

in an organisation might not understand the roles of cyber security team. Secondly, a variety of technologies can be found in an organisation but not all of them might be up to date. Some of them might be new or legacy. In this scenario SOC technology can be the latest versions of hardware or software and integrating it with an existing old technology can be challenging. Several enterprises accept the risk of running existing legacy systems due to the cost of implementing new technologies. The integration of processes includes steps that will be followed by SOC to deal with an event. There might be a current procedure that an organisation follows but this must also integrate with SOC processes to provide efficient reporting and understanding of events.

It is vital for at least one member of a SOC to be part of Change Advisory Cab (CAB) when integrating SOC technologies with current organisations' IT assists. CAB is associated with IT Service Management (ITSM) that includes International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) 20000 standard. Evaluating the risks and mitigation methods for specific change is one of the CAB roles to alert organisations of the potential threats and how they could impact on business. In other words, stakeholders of CAB are responsible of assessing risks that could occur due to a change in an IT environment. Emergency Change Advisory Board (ECAB) is also a subset of CAB, but its main role only associated with urgent events where delays are not accepted. SOC is recommended to be part of the ECAB, which helps in mitigating risks and prevent potential breaches that could occur with urgent changes in an IT facility. SOC playbook that include guidelines to be followed when investigating incidents is highly recommended. It assists in seeing previous reports of responding to security events. A playbook can be referred to an error database and it should be updated occasionally. Reporting on incidents must be done via regular SOC reports depending on organisations requirements. Statistics and analysed events that are conducted by analysts must be included in reports. The location of events occurrences on various assets alongside the procedure of security event investigation must be added to reports as well (Mutemwa et al., 2018).

Ban et al. (2021) stated, a huge number of organisations have tools that generate false positives according to a survey conducted by cloud security alliance. Cloud access security is one of these tools that produces alerts alongside other security monitoring devices. Up to 31.9% of security analysts do not look into alarms due to the high amount of false positives.

Authors presented a framework to implement solution of how to mitigate false positives. The solution consists of ML and data visualisations methods that can investigate alerts that are produced from several security devices. The solution has 4 modules.

The first module is "Alert Generation", Ban et al. (2021) investigated 133.77 million logs and believed that various network instruction detection systems are working together to identify irregularities on network. "Feature Processing" module is added to convert alert messages format into a standard one, as different devices produce different types of alert formats. An example: formatting alert logs into a standard JavaScript object makes it easier to retrieve an enhanced picture of the security situation of a company. "Machine Learning" module apply several algorithms to differ between high critical alerts and less critical ones. The data can be visualised and investigated at last in the "Investigation" module to decrease the investigation complexity. Figure 2.11.63 is the overall picture of the solution.

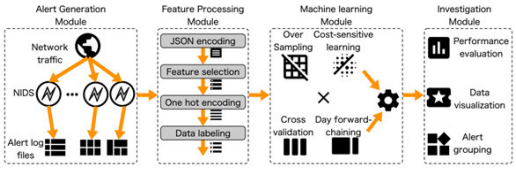


Figure 2.11.63: Solution Framework (Ban et al., 2021)

As a result of the proposed technique by Ban et al. (2021) research, it reduced the number of false positives but did not eliminate it completely. A small number of alerts have been left for security analysts to investigate. The study was conducted on multiple security tools, but researchers added that for future research the proposed technique can be conducted on specific security device to get better outcome. There are few questions to address in regards of the proposed solution. Security threats are increasing highly where exploiters are developing their methods and techniques. Therefore, the proposed technique might've reduced false positives but did not completely eliminate them. Also, it has been conducted on one organisation across several security appliances but for future research according to authors customising the recommended method on one security tool to achieve the full mitigation of false positives can be followed.

Figure 2.11.64 below depicts a model developed by Majid and Ariffi

(2019) based on reviewing previous studies and analyse their findings from surveys with SOC specialists. The concept of the model of a successful SOC is to present humans, processes and technologies as main factors. Although, continuous improvement is a vital factor for success to ensure quality stability. Executing all these factors cannot be done without the most essential aspect which is the financial factor. Therefore, the implementation of a SOC is often linked with organisations financial capabilities.

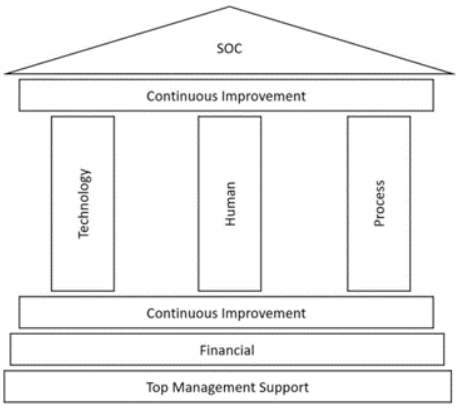


Figure 2.11.64: Model for SOC Development (Majid and Ariffi, 2019)

The model symbolises a visual picture of a successful SOC structure. SOC aims to eradicate threats and make sure that vital services are being implemented to protect organisations critical systems. Starting from the bottom, top management support and finances are external influences that can affect precisely on successful implementation of a SOC. Their role is to support the main components of SOC which are human/analysts, processes and technologies. Top management usually authorise financial approvals for SOC development and continuous improvements. Hence, the model visualisation represents top management at the beginning starting from the bottom. The human or analysts' factor is located in the middle between processes and technology due to the reason if it is absent. Other technology and process factors can always replace human element by applying ML and AI methods. New threat will always occur and SOC services are recommended to be on up to date to deal with these challenges. The ongoing improvements element is added in the visual model twice above and under SOC components to emphasise on the necessity of continuous developments in facing potential and sophisticated attacks (Majid and Ariffi, 2019).

Shah et al. (2019) explained that in some cases SOC usually deliver its services by obeying into a SLA with clients whose traffic is monitored via sensors. These endpoints generate data in the form of alerts via various automated tools comprises of IPS/IDS. The produced logs are required to be investigated by analysts based on their severity and triaged using the tier system of low - medium - high priority. An alert with highest priority is firstly triaged using the process of queue priority. Even though, some challenges can occur in an unexpected scenario where the estimated high priority alerts are produced massively form a specific sensor.

If a new type of event is occurred, then analysts might not have the required time to analyse other alerts as the new one requires more time and effort to investigate. As a result, the priority queuing approach can be exposed to major difficulties. Firstly, various endpoint with regular degree of logs generation is being examined with less time than high prioritised alerts. This exposes low and medium priority alerts to the lack of effective alert analysis. Secondly, breaches of SLA elements can occur due to the preference of investigating high triaged alerts over the low-medium ones. Hence, Shah et al. (2019) suggested the implementation of enforcement approach that guarantee the balance between SLA and the services delivered by SOC.

Based on Dun et al. (2021) findings, there is a gap in SOC sector and additional studies are recommended into the topic. Human, processes and technology components are all recognised in most of the literature that reviewed by authors, but operations and configuration were differently implemented in each investigated SOC model. Studies showed that there are disadvantages and lack of sufficient documentation for developing a SOC as literature revealed that the focus was mainly on technical elements.

There are various questions remain unanswered in findings, and Dun et al. (2021) suggested future research on SOC as there are still no proper guidelines that organisations can follow to secure data and architect operations. It is also recommended to implement unique correlations rules for SIEM to model real time threats detection. Overall, the implementation of a productive SOC is determined by the correct integration amongst its components (Anomali, 2024).

2.12 Case Study I

Clinical research is conducted by Kotsias et al. (2023) on financial firm which they called "Greenback" anonymously for confidentiality reasons. The study revealed the organisation experiences up to 20 billion data of cyber security events in a 24-hour period. These events are produced from various technology assets as the corporation operate in up to 34 countries with capital value of up to 50 billion American dollars. As part of cyber security strategy, the company employs a dedicated SOC to threats detection. Researchers realised that there are still some problems even with applying dedicated SOC. APTs are highly targeting the firm due to its market position where large number of financial services are carried out. Reflecting on that, the sophistication of attacks and expansion of threats landscape might be able to overcome defensive measures that are set by Greenback. Another realisation is related to the militarisation of cyber security threats landscape. This led to the need of cyber defence system that is able to respond similar to a military style. Hence, the adoption of CTI was highlighted in terms of the dedicated SOC. Accordingly, Greenback is not used to operate in a military style where the company is more focused on clients and competitors whilst abandoning cyber opponents. As a result of these problems, CTI was proposed as a new model for cyber protection in order to integrate it with the culture which in turn will help in changing managing behaviours towards the reality of cyber threats landscape.

Intrusion detection systems and sophisticated firewalls are implemented in Greenback using market leading vendors such as Microsoft and FireEye. This helped in preventing some of the attacks. In terms of monitoring traffic, SOC is deployed on 24 hours 7 days a week to diagnose and investigate threats in coordination with IT operations crew. SOC is divided into 3 different layers for analysis purposes. Gathering raw data and triage incidents are part of the roles of level 1 analysts alongside recording them in tickets management platform. Assessing criticality of such an event is also part of their role to whether escalate it to a higher level or not. level 2 analysts are more involved with management loads and providing extra guidance on particular alert if it's false positive or not. When critical incidents are identified then it's level 3 analysts' responsibility to assess the situation via using more sophisticated analytics tools to investigate and operate alongside other teams such as IT operations (Kotsias et al., 2023).

Even though, with the implementation of a dedicated SOC the threats

response was inactive. This means that responding to cyber threats was not based on knowledge from other firms' insights that have faced similar threats before. SOC team had the ability to answer the questions of what attacks have conducted and how they occurred. Strategic questions such as why such an attack happened, who conducted it and when the next attack will be carried out were unable to be answered by team. Therefore, practitioners echoed on the need of implementing CTI function that is able to adapt with sophisticated threats actors (Kotsias et al., 2023).

A diverse number of heterogeneous technologies is retained by Greenback across north, south America, Asia and Europe. Protecting these technologies from threats is heavily relied on SOC logs that are generated by appliances and assets. Identifying meaningful patterns is completed via the adoption of SIEM that helps in logs correlations, storage and analysis. As shown in Figure 2.12.65 an advanced cyber analytics platform is responsible of collecting data related to staff activities. These logs are grouped and correlated then security events are produced based on pre-defined algorithms. A group between 4-6 specialists are employed to adopt CTI functionalities. They are responsible of gathering data from variety of local and international sources including security and law agencies, threat intelligence suppliers and other intelligence experts in financial area. CTI team is able to collect information from valuable sources that are useful in providing accurate advice to analysts and cyber security leadership to apply protective frameworks in advance (Kotsias et al., 2023).

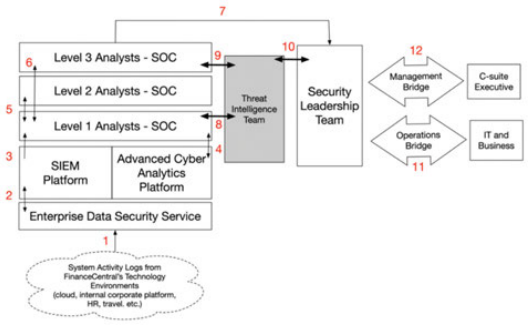


Figure 2.12.65: Cyber Analytics Platform (Kotsias et al., 2023)

Suitably, embedded threat intelligence tools are purchased and applied into SOC to specify threat patterns and their priorities. Strategic and tactical levels information are fed to stakeholders as well throughout the team.

For instance, operation level team is constantly monitoring threat landscape and sending information to analysts for actions to be taken such as blocking anomalies IP addresses and providing suggestions of investigations. When it comes to tactical level, the team is able to predict future threat activities by validating them versus level 3 analysts' observations. Detecting recent threats actors' behaviours, their methods and procedures became under the strategic level umbrella to highlight and fulfill any cyber gaps that could expose the firm to high risk of attacks. The adoption of CTI enhanced the cyber security aspects of Greenback by highlighting the alignment amongst cyber defence and cyber-attack actions. It is also decreased the achievement of such attacks by stopping them on early basis. Improvements in efficiency and moving toward the focus on cyber defence across cyber-attacks are amongst the advantages as well. Researchers performed the clinical study to elaborate on how military intelligence can be applied and adopted effectively in commercial sector. They believe that CTI as a service can be transferred and implemented into any similar commercial managerial framework. Most essentially, the research emphasised on the move from reactive reactions to transit into detailed defensive actions operated by threat intelligence (Kotsias et al., 2023).

2.13 Case Study II

Vaarandi and Mäses (2022) highlighted some of the gaps associated with SOC building. Cost, limited budget and SOC creation scalability are the issues raised. Those gaps are addressed to recommend the reliance on open-source and free solutions. The study is conducted on Tallinn University of Technology which is based in Estonia. The university include up to 12000 users with 10000 staff and 2000 of students. The university's SOC operates since 2019. Managing network infrastructure and other critical systems is mainly done by IT support department. On the other side various assets are controlled by academic staff where required such as academic department sub networks. Tier 1 analysts' roles are fulfilled by up to 3 students volunteers. Other roles are linked with staff. Employing students helped in reducing the cost of SOC personnel and also provided students with an opportunity to have hands on experience. Some key challenges are identified in terms of sharing information amongst SOC staff and burnout aspect. To tackle these difficulties, students are chosen from the master course of cyber security where they have already gained some technical skills that can help them in analysing events. The selected students are changed each semester to prevent exhaustion.

Addressing knowledge share issue is dealt by providing 3 weeks of training to new students by previous semester ones. This helped in a smooth and efficient handover. Knowledge base repository is also created. It consists of playbooks, documentation and information about past events plus how to triage incidents. Maintaining an efficient communication amongst analysts is organised via MS team's platform where details are shared quickly and smoothly. There are other different implications when it comes to deal with sensitive information. Hence, privacy and confidentiality regulations are required in SOC systems. As a result, new employed analysts are required to take security awareness training to understand the rules of managing sensitive data (Vaarandi and Mäses, 2022).

The usage of personal devices or transferring information from SOC environment to an external media drive is strictly forbidden. Therefore, maintaining accountability and confidentiality is done by the signing of compulsory non-disclosure forms. Overall, built in networks are assigned to SOC to make sure it is separated from other networks for privacy concerns and having physical access to the SOC space is limited to trusted employees (Vaarandi and Mäses, 2022).

Figure 2.13.66 below depicts the architecture of the university SOC alongside the monitored assets and tiered levels.

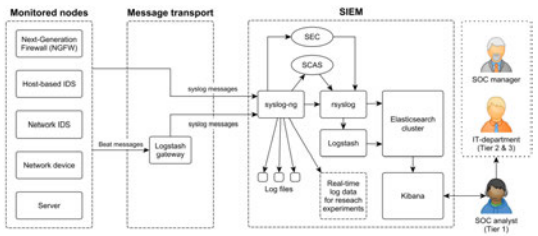


Figure 2.13.66: Tallinn University SOC (Vaarandi and Mäses, 2022)

Handling alerts is the most essential part of SOC operations. Thus, the university's SOC events are triaged according to their severity. High priority incidents are examined first by tier 1 analysts. In the case of an incident high impact tier 1 will send alerts for further investigation where needed to tier 2 and 3 analysts. The outcome of the investigations is then sent to be stored in knowledge base as support documentation for future events. Reports that are generated on daily basis from different tiers are also

retained in repository. This highlights the importance of documenting as much as investigating alerts. Tallinn university is amongst the organisations that struggle to implement sophisticated automation processes when dealing with alerts. Vaarandi and Mäses (2022) emphasised on the need of AI in SOC where absence of automation could cause alerts overload which in turns can lead to analysts' frustration. At the university environment, there are up to 200000 generated events from IDS sources on daily basis.

Dealing with this number is a huge challenge for SOC team. As a result, an open-source approach is developed to implement unsupervised algorithm method. The tool is defined as SCAS as shown in Figure 2.13.66. It helps in grouping alerts in a real time stream. Each of the groups illustrates events that are identified from the same source but only within a short time scope. Then, cluster approach is used in alerts groups. The clusters are matched against regular appearance of IDS alerts. This helps identifying similar paradigms that represent low risk threats. For unfamiliar activities and events, their alerts groups are represented as outliers. They are scored as -1. The calculation for alert groups that are linked with cluster is considered between the range of $0 - 1$. The unusual events that are identified as outliers are the ones that require more in-depth investigation according to SCAS tool process. One of the benefits of SCAS that it does not need any physical interaction with as it is able to process large volume of IDS events precisely low risk alerts. In 2022 between January and February, the tool managed to decrease the number of IDS/IPS events from 11484738 to 71033. This allowed analysts to have more time and focusing on high important alerts. Simple Event Correlator (SEC) is also applied as shown in Figure 2.13.66 to automate alerts that identify an attacker's behaviours and generated within short period of time (Vaarandi and Mäses, 2022).

2.14 Case Study III

A study is carried out by Basyurt et al. (2022) to gather valuable knowledge on how to improve SOC processes. The research is conducted by interviewing up to 9 individuals from Germany who are experienced in the field and work with various types of SOC on daily basis. For example, integrated SOC units, governmental sector and private enterprises. The individual's roles are varied which included: incidents responders, team leaders and cyber threats answering points. The method used is semi-structured approach where the interview guide comprised of six sections alongside their related questions. Below are the sections and their allocated questions.

- ***Descriptive information:*** *What does your normal day-to-day work usually look like?*
- ***Reporting of organisational cyber incidents:*** *What data do you need or transmit in order to deal with cyber threats?*
- ***Collection of data on cybersecurity:*** *What data sources are you analyzing to identify these threats and security vulnerabilities?*
- ***Situation picture for the cyber threat situation:*** *To what extent is a situation picture of a cyber threat and security gaps created?*
- ***Communication of cyber threats:*** *To what extent do you adapt cyber alerts to different communication channels and affected actors?*
- ***Ethical, organisational, and legal aspects:*** *What are organisational and legal requirements for data processing or stakeholder communication?*

Figure 2.14.67 illustrates an overview of the IT SOC system of German state. Different elements are added together to complete the full picture of the German SOC process. At the beginning, events are generated by clients reports via phone/email or alerts that are automatically produced by systems such as IDS/IPS. To respond to an incident, the reported event is stored in a ticketing management system to investigate it further and collect appropriate information. Once evidence is collected, awareness channels such as social media are used for further analysis. After a full investigation is completed, a report is created to inform stakeholders of any potential risks and to distribute warning messages about a particular threat (Basyurt et al., 2022).

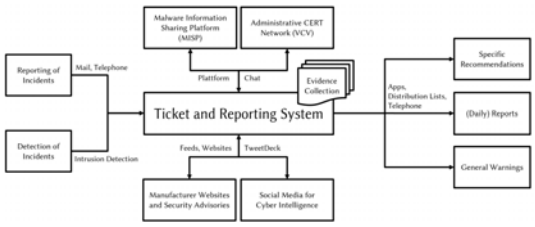


Figure 2.14.67: German State IT SOC (Basyurt et al., 2022)

Various difficulties and gaps are raised by participants in terms of SOC elements. Legal implications on data collection where extracting data from

open sources can face legal restrictions as 6 interviewees added. Application Programming Interfaces (APIs) are also amongst the challenges that analysts face when collecting data. The absence of effective API prevents SOC users from gathering the data needed as it will be limited. More importantly, lack of automation is highlighted which could help in data filtering. Any occurrence of redundant data can be eliminated via the adoption of automatic processes which in turn can decrease workload on analysts. Dashboards are suggested as well to read open-source data more easily and help making quicker decisions. From a communication perspective, some participants elaborated on the lack of communication when dealing with threats (Basyurt et al., 2022).

Targeting a particular group with certain warning messages about a threat can be difficult to achieve. When analysts are required to spread a message about a threat, the targeted individual might not hold enough technical skills to assess and read the situation. Therefore, analysts could spend more time with specific groups trying to further explain the situation. Alongside delivering a warning message, following the recommendations often lack of 100% implementation. To clarify it more, one of the individuals added that the targeted persons might not read the situation as risky as SOC analysts and ignore the given instructions. Distributing warning messages is a huge challenge in the cases where manual processes are required. Various events can generate information with different formats such as Hypertext Markup Language (HTML). In this context, an individual mentioned that this code will have to be imported manually into a system called TYPO3. After this process, additional manual effort and re-ajustments are needed due to errors and unexpected results (Basyurt et al., 2022).

The mentioned challenges are distributed into key areas of development. 5 difficulties are linked with communication. 4 obstacles are acknowledged for open-source data collection and analysing the cyber situation. The imposed challenges require adoption of technological tools to support analysts in their tasks. This include: data collection, data analysis and cyber communication. A conceptual visualisation of such a tool is introduced in Figure 2.14.68 below by Basyurt et al. (2022) based on their findings.

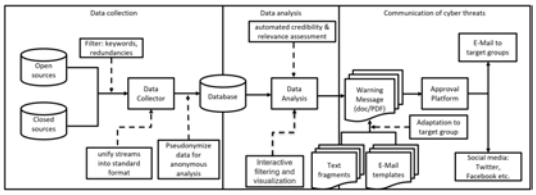


Figure 2.14.68: Conceptual Visualisation Tool (Basyurt et al., 2022)

Addressing the issue with collecting various format of input data is solved by implementing a standard process and format of events reporting. In this scenario unforeseen challenges have raised in terms of motivating data sources to adopt the same data format standard. The suggested solution for this is to extract information with their primary format then use AI methods to change their format into the predefined standard form. Assessing their credibility can be achieved via automated process that is configured in advance to only extract information based on predefined keywords or rules. Regular reviewed sources can be predefined based on certain parameters to help obtaining only relevant information that help in reducing false information. For example, correlation approaches can be useful in decreasing the amount of incorrect information by checking its validity and compare it with other various trusted sources. Providing solutions of legal implications are neglected as authors described the situation to be in-hand of legal authorities and institutions. Legal concerns could be overcoming by anonymising users' information before analysing and storing them (Basyurt et al., 2022).

As described previously, the issue with cyber threats communication is to target particular groups. Each group require various set of formulations that identify their IT skills. Implementing an application that can be modified is recommended to address communication challenges. The application can help in fulfilling this gap by publishing warning messages based on predefined texts and segments that only associated with certain groups. The disseminate of such customisable messages is an effective solution by making sure that only understandable communications are received. To enhance the efficiency of threats messages awareness, emotional effects could be included. The proposed application solution not only help in addressing the challenge of spreading threats messages but also it is an effective tool to solve the problem of manual efforts of producing warning messages. The process of selecting keywords and automatically spell checking the message prior to publish helps in reducing manual attempts. The targeted groups can be contacted after to acquire details about the adopted technologies by targets

and the efficacy of the messages. Authors added another challenge which is obtaining an alert approval for warning messages. This can be solved via tool where both parties can approve such an alert by making correction where required on the implemented tool. This helps in reducing time and efforts instead of keep sending alerts for further amendments and approvals (Basyurt et al., 2022).

Even with the mentioned solutions, researchers believe that having a full automation of communication is not possible at the meantime due to the requirements of approvals from different parties. Information to create threat warning messages might not be obtainable straightaway. The results of such a threat can harm systems badly where it requires more in-depth investigation prior to communication. However, once an approval is obtained then a message can be spread amongst channels that are recognised in advance. Basyurt et al. (2022) contributed to the field by producing this empirical research. Challenges and gaps are identified amongst suggested solutions and key areas of developments. The suggested applications and tools are gained from interviewees opinions where all of them are expertise in SOC. Figure 2.14.68 showed the conceptual tool that is developed to help in overcoming the mentioned difficulties. Researchers added that further studies are needed on these challenges to gain more information about new approaches implementation or to enhance the existing ones.

Chapter Three

Methodology

3 Methodology

3.1 Introduction

This section justifies our chosen research methodologies and methods. The validation of SOC challenges, more precisely automation in detecting events and logs is performed within a detailed literature and variety of experiments. There are few questions that should be asked at first, how to carry out such a research and how to resolve a certain problem? These questions are referred to methodologies and methods as well as the reason of why this investigation is conducted. The difference between methodologies and methods are clarified according to the research problem that the researcher tends to explore (Faryadi, 2019).

Figure 3.1.69 is the life-cycle of the research.

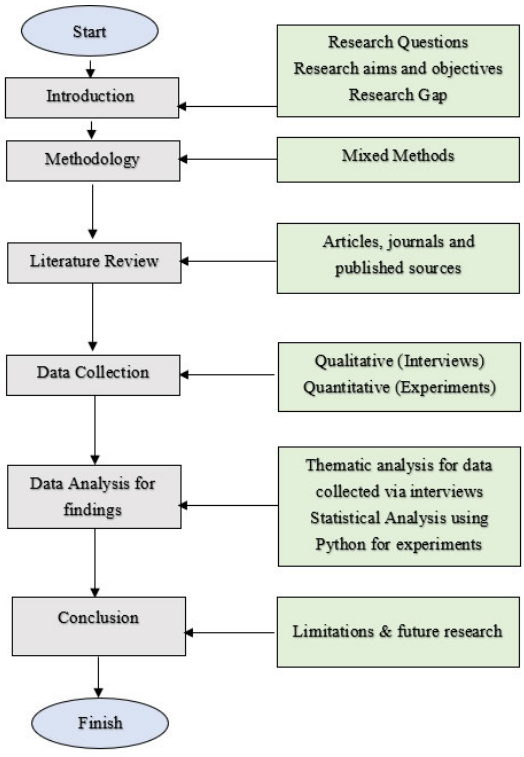


Figure 3.1.69: Methodology Flow Chart

The researcher chose a mixed approach of qualitative and quantitative

to conduct this study. Both approaches involve data gathered from interviews and experiments. The research includes primary data collected from interviews alongside secondary data from trusted published sources (Mkandawire, 2019).

Conducting a literature review based on SOC was the first step by adopting a comprehensive literature approach. The literature data are collected from various trusted sources including google scholar, IEEE and other academic resources. Searching for different keywords such as SOC challenges or SOC Automation and other keywords related to the research to extract the only linked information is the filter that have been taken. Another filtering criteria is applied on publication date where articles must be published at least within the last 5 years of the start of the research to gather up-to-date information. This thesis adopts an approach which highlights relevant sections including the chosen research design, data collection and data analysis techniques. It contextualises the preferred design and the implementation of several research methods based on the selected research. Again, emphasising on the research problem and questions indicate how the chosen methods are set to analyse and discuss research findings.

It is essential to select a methodology based on research objectives. It must be compatible with the research to achieve the research aim. The chosen data collection techniques are part of the overall methodology to interpret and analyse findings. The chosen research is associated with cyber security and SOC.

There are essential steps that must be taken before conducting the research. An updated literature review is investigated where the architecture of SOC and threat detection using ML techniques are highlighted. How to gather and collect the required data is outlined in methods. The main aim of this section is to explain the selected adopted methods to complete the research. The preferred design and adoption of methods are contextualised based on the researcher choice. Therefore, methods such as interviews and experiments are mentioned alongside their strengths and weaknesses to justify the choice. Ethical concerns are required to be identified to decrease the risk level and to be prepared for any potential threats. They are highlighted as well as unexpected risks can always occur. Therefore, the researcher is aware of the most important aspect which is to ensure the privacy and confidentiality of the collected data.

3.2 Time Horisons

According to Saunders et al. (2019) setting time margins is part of the research. Cross-sectional and longitudinal are types of time horisons that can be chosen. For this research, the researcher selects cross-sectional type due to the allocated time frame of the research which is within 4 years. Therefore, if the research will take longer than 10 years then longitudinal time horison is the preferable one as Melnikovas (2018) added as well.

3.3 Data Collection

Data collection methods are divided into two elements: qualitative and quantitative. Observations, interviews and focus groups are qualitative data collection methods where the gathered information are known as primary data. Collected data using quantitative method are often numerical data or secondary data that have already been published by different researchers (Saunders et al., 2019; Mkandawire, 2019).

3.3.1 Interviews

The author collected both primary and secondary data. Organisations and individuals who experienced challenges related to the chosen area are interviewed to gather the primary data. Secondary data are collected by investigating previous studies. The preferred selected format for this study is an online based interview, but also with the option of having face-to-face if a participant was unable to attend online. Also, sending the set of questions via emails or post to individuals if they request to.

The usage of different methods administration ensured the delivery of good sampling coverage by decreasing errors related to coverage issues. The individuals who are expertise in the chosen field and who are experienced working with SOC are targeted. Unstructured interviews are carried out with up to 5 participants to gain insights of the challenges that are being faced in SOC environment. All interviews were conducted online via Microsoft Teams to overcome barriers such as geographical ones.

Only 5 interviewees in UK are interviewed due to various reasons. First, it is hard to get in touch with SOC specialists who are happy to be interviewed or share data in regards of SOC challenges. This is due to confidentiality and data protection concerns. Also, the chosen number of participants help in narrowing the research focus on specific challenges and gain more

details on them instead of having broad wide of information with limited depth. The role of participants can be found in Table 3.3.1 below.

Table 3.3.1: Participants Information

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

Accordingly, data analysis is conducted using thematic analysis and statistical analysis of summary of key challenges that are raised by interviewees. A discussion is carried out to find any relationship between findings and previous conducted literature. Interviews were recorded and transcripts are retrieved. Coding approach A-E is used to refer to each participant. As interviews were reviewed, specific challenges or issues were highlighted and coded. These codes were designed to capture particular aspects of the responses that were relevant to the research questions. For example, when participants discussed issues related to "overwhelming volume of logs" or "false positives," these became initial codes that could later be grouped into broader themes.

The initial codes then examined to detect overarching themes. These themes were related codes that represented the broader challenges facing SOC. For instance: The number of logs emerged as a theme based on codes such as "huge number of logs" that were mentioned by different participants. Lack of Skilled Staff was identified as another theme, arising from discussions about the shortage of analysts. False positives were another theme based on interviews that highlighted the high frequency of incorrect alerts. Thematic patterns such as these were categorised to provide insight into the key challenges faced by SOC teams.

After determining the initial themes, they were refined to ensure that they reflect correctly on the data. This process included re-reviewing the transcripts to ensure that the themes highlighted the participants' experiences. Some themes were adjusted or merged for consistency and clarity. For example, lack of communication and automation were identified as in-

terrelated themes, as poor communication often lead to inefficiencies that could be enhanced via automation.

Once the themes were refined, each theme was defined clearly. For instance, Automation: a theme that highlighted the lack of automation in SOC, leading to inefficiencies in handling and responding to alerts. Lack of skilled staff: this theme was defined around the challenge of the lack of qualified personnel, which negatively impacts on the ability to handle security incidents efficiently. Threat Intelligence: this theme identified the gap of threat intelligence integration automation, leading to the reliance on manual actions by analysts.

The final step involved compiling the results of the thematic analysis into a report. In this stage, the themes were connected to existing literature on SOC, allowing for a deeper understanding of the challenges and offering possible solutions. For example, literature suggests that implementing more automation can reduce the burden on SOC teams, particularly in dealing with log management and false positives. Additionally, cross-training staff and improving communication tools were suggested as ways to address staffing and communication gaps.

This research identified key challenges faced by SOC, including the high volume of alerts and false positives alongside gaps in automation, communication and staffing via applying thematic analysis. The identified themes are aligned and consistent with the challenges mentioned in previous literature, highlighting the need for automation, better communication practices, and more skilled staff. The insights gained from the thematic analysis can serve as a foundation for addressing these challenges through SOC improvements.

Additionally, the developed automation model is presented to 10 participants from cyber security to software development fields. The reason behind that is to gain feedback and to evaluate the model based on specialists' opinions. Their evaluation is included in automation experiments chapter. Table 3.3.2 below presents the roles and interviews methods used to evaluate the model where coding approach of P1-P10 is applied. However, there was no overlap between participants in the first and second interviews in which the developed model was presented to different interviewees.

Table 3.3.2: Participants of Model Feedback

Participant ID	Role	Interview Method
P1	Cyber Security Consultant	MS Teams
P2	Cyber Security Consultant	MS Teams
P3	Software Developer	Google Meet
P4	Software Sales	Google Meet
P5	Software Product Leader	Google Meet
P6	Cyber Security Consultant	MS Teams
P7	Penetration Tester	MS Teams
P8	Information Security Analyst	MS Teams
P9	Software Engineer Analyst	MS Teams
P10	IT Analyst	In Person

3.3.1.1 Strengths

The reason behind choosing data collection for interviews is that it allows access to people's experiences and reality by asking more questions to follow up questions that were not considered prior to the interview (Zhang and Wildemuth, 2009). Questions such as What is your role in SOC? and how long you have been doing it for? are asked but the nature of interviews was informal conversation using unstructured approach. Hence, participants had the chance to add any extra information that are not highlighted in questions where needed. These questions are also important, so that the collected data can be analysed from different dimensions or demographers. The nature of this research is associated with SOC which raise confidentiality and data protection issues. Hence, observations, experiments on organisations SOC or collecting numerical data from organisations SOC tools was not possible due to these ethical concerns.

As stated, the researcher used interviews to gather the required data. These techniques consist of open-ended questions or ones with multiple-choice options. Open-ended questionnaires questions were the preference by the researcher to make the interview more appealing and give participants wider space to share their answers and opinions.

There are more advantages of using online interviews which include the short period of time and effective low cost. The researcher can start the in-

terview, stop and restart it at any time as preferred. The time horison of the research is cross-sectional. Therefore, interviews are compatible and suitable for either cross-sectional or longitudinal studies in-case the researcher requires to contact participants again (Nayak and Narayan, 2019).

3.3.1.2 Limitations

Andrade (2020) added that the popularity of collecting data using online approach is growing rapidly due to several reasons such as the cheap collection of data. On the other hand, it is exposed to methodological weaknesses and limitations. The type of participants population alongside their biases towards the sample can decrease the value of findings from the sample. The selected method target participants who are involved in SOC and have experience in cyber security plus interviewees who work in software to evaluate our model. Therefore, the findings of the sample will only be applied to security individuals who are involved in the chosen study.

The targeted population are based in UK. Thus, findings might not be generalised which can limit the scientific value. The limitation of findings generalisation can be resolved with implementing two conditions. The first important aspect is to define the population that the study is conducted on, which is in our case is cyber security population. The other method is to make sure that the method is targeting a sample of population that is overrepresented in a specific area and is not possible to characterise the population (Andrade, 2020).

Hence, the population is cyber security analysts and the specific area is SOC. There are other limitations that can be highlighted. For example, the education level of participants. In this case, only experts who are suitably associated with cyber security fields are contacted.

3.3.1.3 Ethics

The researcher makes sure direct identifiers of respondents are removed from any saved files on personal devices to protect individuals in case a breach occurs. As any method of gathering and collecting data, interviews are exposed to different ethical concerns that the researcher must be aware of. The most essential ethical aspect when conducting the selected research is to protect respondents' confidentiality. In the occurrence of confidentiality

breach, there are unwanted consequences that can impact on participants themselves as the researcher as well. Reputation damage, employability loss or even criminal liability can be the result of such a disclosure of information that respondents can be affected by. Also, participants were able to stop responding to questions if they had privacy and confidentiality concerns (Singer and Couper, 2018). MS Teams is used to record interviews. Participants were given the choice to turn their camera on/off. The recordings were saved and only accessed by the researcher using password protected one drive account.

There is also other two aspects to comply with confidentiality which are informing participants about the elements of the research and obtaining their consent to participate. Statements that include an explanation of the research purpose, the voluntary participation and identifying any foreseeable risks are sent to participants. Thus, biases might occur in responses when it comes to the purpose of the research. Hence, a general research purpose statement is provided where an immediate purpose is avoided to prevent any possible biases.

3.3.2 Experiments

Some experiments took a place and below flowchart shows the expected life-cycle phases of the experiment design by the researcher. The first step is to define the state of knowledge which might be modified at the end of an experiment according to the results findings. Therefore, designing an experiment is followed by performing it which in turn can lead to interpret and understand the results.

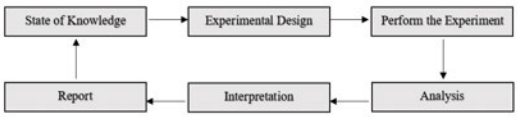


Figure 3.3.70: Experiments Flow Chart

Accordingly, a system block diagram is also created to clarify the system model. Figure 3.3.71 presents the system steps that are taken to develop the model.

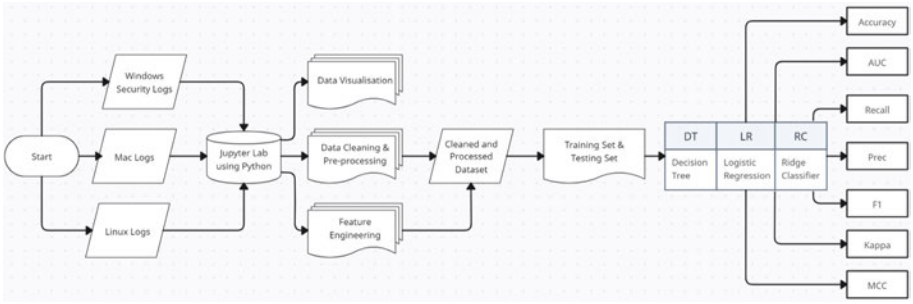


Figure 3.3.71: System Block Diagram

The experiments involved creating a ML model to predict or detect a log number based on task features. This type of problem typically falls under the category of supervised learning, as the model is training to predict a specific target (the log number) based on input features such as the task feature. Since training the model using labeled data (task features with corresponding log numbers), this is a supervised learning problem. The model is trained and tested with 3 types of logs including Windows security logs, Mac logs and Linux logs. Each training 3 different algorithms are used including DT, LR and RC. The experiments took place on windows operating system using Jupyter notebook and Python language. Since the model predicts the log number based on its features such as task, this can be described as predictive modeling. To evaluate the efficiency of the model different stats are produced such as Accuracy, AUC (Area Under the Curve), Recall (Sensitivity), Precision, F1-Score, Kappa (Cohen's Kappa), MCC (Matthews Correlation Coefficient). The results for each experiment and algorithm are provided in the automation experiments section.

3.3.2.1 Strengths

In cyber security research, there are various difficulties that can prevent the experimenter from resolving problems. This is due to the definition scale and unexpected variables that can impact on the results. In fact, the researcher needs to be realistic when conducting experiments as the investigated variables might not be the only ones that the results are relying on. There could be other uncontrollable variables which might influence the outcome. Conducting experiments help in producing results to understand whether the problem can be resolved sufficiently or not. Hence, this can only be determined via experimental process where the research problem usually

requires repetitions and in this case alerts/logs. The aim is to explore and understand phenomenology of alerts to examine the problem on a larger scale (Tardiff et al., 2016).

Having a control over facts that can impact on the overall outcome of the research study is one of the advantages that experiments offer to the researcher. The experimenter could remove or neglect any variables that could impact on the results. The focus then can move towards one or more variables that can help in producing sufficient results. The nature of experimental design help in understanding SOC environment. Also. the relationship between genuine alerts and false ones to build a comprehensive knowledge about the phenomena. As mentioned, experimental studies are flexible as they can be repeated which is useful to validate results or examine other variables.

3.3.2.2 Limitations

There are several limitations associated with the selected research. Experiments are conducted in cyber security field where ethical implications might occur and could prevent experiments from taking place. More precisely, in experiments there will be variables that must be controlled but they can be irrelevant. This can produce circumstances where the situation is provided as artificial and not realistic. The research study results are also exposed to errors committed by the researcher or the machine, which can lead to influence the outcome. In this case, there are other challenges that might occur, such as unreliable samples and personal biases. Some of the experiments also take time and the expected results might not occur as expected and might lead to disappointment. Hence, the assumptions can always be updated according to the outcome of each experiment. Hypotheses are an essential key in science as they can help in improving the design of experiments. Achieving meaningful results that can be repeated is a challenge that the researcher is also aware of. Research problems can be huge and complicated. Performing experiments directly on them is not recommended and might be impossible. The experiments are conducted on subproblems and then integrated them with each other to generate an understanding about the big picture (Tardiff et al., 2016).

For example, various alerts related to different cyber security events are tested separately. Small and repeatable experiments are expected to

highlight and understand the nature of the SOC-reported alerts.

3.3.2.3 Ethics

There are various ethical issues when dealing with cyber security experiments. These ethical concerns related to SOC can be avoided if experiments aspects are highlighted and designed consciously. Hence, the experimenter is required to be aware of controllability when carrying out experiments. This means any effects must've been known in advance to make sure they do not impact on other services. Thus, the researcher is decided to conduct ethical hacking experiments using virtual labs to ensure the privacy and security of real-time services. Also, testing is carried out as part of the security-by-design process to review tools and software that will be used (Pieters et al., 2014).

As machines and software are required for experiments, there are regulations and laws that must be obeyed. Computer Misuse Act 1990 ensure the researcher only use programs or computers for experiments purposes and not for malicious reasons (Legislation.gov, 1990). For example, when conducting ethical hacking it must be on either virtual machine or local host and not on live systems or websites. There is various testing that can be conducted on real live environment. In these cases, it must be authorised by stakeholders such as; penetrating testing. There are other aspects where General Data Protection Regulation (GDPR) is required to be adhered to. This is important to avoid any unwanted consequences and potential breaches (ICO, 2018). It is essential to build some knowledge about specific risks and ethics of potential hazards in advance to decrease the level of their occurrence.

Chapter Four

Interviews Findings

4 Interviews Findings

4.1 Introduction

Participants in UK from several cyber security organisations are interviewed to identify key challenges they face when working with SOC. The interviewed individuals are referred to as letters instead of revealing their real names to avoid any potential confidentially implications and data protection regulations. Unstructured interviews are conducted with various questions to gather insights. The researcher had minimal guidance, which allowed the conversation to evolve naturally. The approach characteristics are conversational and open-ended which focused on qualitative insights and personal perspectives. Also, highly flexible and adaptive to the interviewee's responses. The advantages of the unstructured interviews include deeper exploration and more detailed responses as well as building rapport with the interviewee. It is ideal for discovering new ideas or insights. On the other hand, it is time-consuming and harder to analyse where responses can vary widely, making comparison difficult. Also, prone to interviewer bias. Accordingly, each interview lasted between 30 - 45 minutes and the following are the questions asked during the interviews:

1. *What is your role in SOC ?*
2. *How long you have been doing it for ?*
3. *How long do you interact with SOC on daily basis ?*
4. *What are the main challenges do you face when using SOC ?*
5. *Do your team members agree on the same challenges ?*
6. *Are there any planned solutions for the challenges mentioned ? If there are, is your team in the process of delivering these solutions ?*
7. *What about false positive rates ? How do you deal with them ? Is there any procedure do you use to mitigate them ?*
8. *In your opinion, what are the best measures that can be implemented to overcome the mentioned challenges ?*
9. *Can we develop python code to mitigate some of the false postive alerts ?*

4.2 Interview I

Participant A is a cyber security engineer who works for a security organisation. A worked in the industry of cyber security for the last 5 years and interacts with SOC of up to 9 hours on daily basis. According to participant, the massive amount of data logs is a key challenge the industry face. For example, a small medium size company with up to 10000 computers could collect windows security logs, domain logs and other logs from domain controller. The size of each log is a couple of megabytes. Therefore, the overall size would then be them megabytes multiplied by 10000. The interviewee mentioned about the importance of having an advanced infrastructure and automation to be able to deal with logs. Other challenges are mentioned in terms of analysts. If an experienced staff leaves then a new analyst joins. It will take a lot of time for them to gain the required skills for the job. This issue might occur continually where it puts the employer back to the first step. Hence, a rigid training regime is required.

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

When proposed with the idea of developing scripts using programming languages such as python for automation purposes. Participant added that they can integrate it with tools like Splunk. A python code can be developed to collect data from an index such as windows security logs. Then integrate it with Splunk to quickly detect false positives that are associated with logs such as windows security logs. Overall, the main key challenge is the number of generated logs where it is nearly impossible to investigate all of them. That leaves organisations under potential threats constantly.

4.3 Interview II

Participant B is a cyber security consultant and building environments is part of the role B carries out. For instance, putting a product together based on client request. That could be building a SOC or vulnerability management. Another responsibility is transition support where parts of security are taken from client environment and transits it to their organisation products. There is also a run team that is responsible on running

a product like SOC building. Participant B has dealt with SOC for over 3 years. The role was being an analyst looking at various logs and alerts using logarithm SIEM which is similar to Splunk. This before moving into being a consultant in cyber security area. Participant mentioned that Splunk is the Rolls Royce version comparing to logarithm meaning that Splunk is more sophisticated.

Communication amongst analysts is one of the biggest soft challenges SOC users face. For example, analysts spent 12 hours a day working in SOC where they get burnt out at the end of the shift. There is no time to speak about things. Also, some of the analysts are new to SOC. From a security point of view, the biggest challenge is phishing attacks. It is quite hard to detect them when they occur. It is very difficult to try and stop these types of attacks apart from reporting them when they are detected. When it comes to phishing attacks, team members agree on this challenge. Not only within SOC, also within the whole cyber security sector. Following on from that, sometimes users who have less technical skills and do not work in a SOC do not admit they clicked on a phishing link. This is because they are not sure about the consequences and they prefer to be quiet. Participant B added when asked about challenges.

When asked about any planned solutions to overcome these challenges. B mentioned that in Microsoft office 365 there is a report phishing function. But when it comes to looking at logs and try to report these logs in a certain process, there is still a lot of work that needs to be done. However, there is no 100% solution where it says that this is definitely how we are going to stop phishing attacks. However, cyber security industry is constantly moving forward and it is still quite difficult to stop phishing. There are also false positives but with better communication amongst team members finding out false positives can be detected a lot easier. Accordingly, when the participant is asked about if developing a code to mitigate false positives can be achievable, B added the below:

"Yes, and I think this can be really good idea, but we need to take big dataset in order to achieve that and this where SOC is struggling at the moment. Clients might be with them for auditing purposes only and they do not care about security and IT until something serious has happened. However, as they only be working with SOC for audits so they might not be available for very long time. Thus, being able to take dataset for over a long period of time is hard".

They also added when a SIEM tool comes into a place, learning and mastering it can take a long time. Overall, implementing a product or a technology that can integrate all these tools into one place can be very effective so analysts can use it more efficiently.

4.4 Interview III

Participant C is a cyber security architect who works for policing digital services. Including developing and designing for national policing. The participant also has an extensive experience from previous roles in leading technical teams and projects. Accordingly, participant interacts with SOC on daily basis where the system is a centralised national management SOC. When asked about difficulties and challenges, a stuck between two various solutions are the technical challenges they face. For instance, some police forces use specific tools and some use different ones. Therefore, combing both solutions into one main is a challenge for them. Analysing the output of both solutions into one main base like having a coherent repository that store data for analysis can be a solution. Geographic challenges are also added in terms of communication. Analysts are often working remotely where they occasionally go to the office. Therefore, communications amongst analysts can cause a challenge more specifically when also trying to speak to the national cyber security and national crime agency as they added.

The high number of events and alerts pose a major challenge. Also, trying to pull data from external sources using threat intelligence. An example is provided by the interviewee, where an event occurred such as false positive and a good number of analysts started investigating the issue. Then, the event turned out to be badly scaled and misunderstood where it was a one-person job. However, it could‘ve been dealt with easily. As stated, if a genuine threat has occurred at the same time where other people were investigating the fake event, the risks could‘ve been high. The participant added that having measures in place to overcome the mentioned challenges are essential more than ever. As added previously, dealing with data in one main container or type of storage area is needed. Thus, they can observe all threats and trends in one dashboard system instead of looking into different places. This would lead to better engaging amongst analysts, leaders and partners. For instance, having automation in place to reduce workload can be an effective solution. As well, having a shared address book where SOC members can pick up the phone and dial a person from a specific organisa-

tion would be a bonus. More precisely, automation of data sharing solutions. As a researcher, a Splunk SIEM tool is mentioned to the interviewee, and they answered with the following:

"We don't use Splunk. Currently we know that there's a couple of national systems. They're currently managed by third parties or monitored by third parties that use Splunk, but we're going to bring them in house and put them into Sentinel".

Participant also added events correlations are required. Plus having automation to pull data from external sources and partners for threat intelligence using particular algorithms. The interviewee emphasised on the need of a shared data centre across partners and organisations. This is for data aggregations, data sharing or data summary. Overall, threat intelligence is heavily relied on manual actions. There are up to 6 individuals who are based in office searching for information to keep track of trends. For instance, windows services threats related information are pulled out manually. Having 20-30% of automation or even more is useful to pull these types of data where workers can focus on dealing with other tasks. Threat intelligence is a massive gap at the moment in terms of what information or threats to look for and automation can reduce manual work. Mapping the monitored systems and spotting gaps can enhance our work effectively and efficiently as participant C concluded.

4.5 Interview IV

Another individual was interviewed, referred to as an Id of "D". An extensive experience of over 18 years in the industry of cyber security including military/governmental sector and private sector roles D has. The official title of the interviewee is the head of cyber defence within large firm where the role is mainly related to managing operations team. Including incident responders, threat intelligence, vulnerability management and offensive security team. All of the lead aspect of cyber security at the organisation participant D is responsible for. They have distributed operations centre around the world including India, Chicago, UK and Singapore. The teams and the head of defence interact with SOC elements for around 13-14 hours on daily basis. When asked about the main challenges the team and head are currently facing, participant broke them down into different levels of complications.

First of all, the top end level includes board level issues. Stakeholders and individuals who are part of the board do not necessary recognise the risks associated with cyber security. For example, it can be quite challenging for them to realise and understand the real impact of such a cyber-attack. Unless they experience a genuine attack. This might be due to the lack of education and awareness of cyber security as D added. On the other hand, investments can reach into an end road. This means money is put towards solving of such a gap but when it is resolved the funds stop where new threats might occur. Various organisations and boards are still under the belief that they can win when a solution is achieved, then they move on. The real environment of cyber security is about continuity and improvements. It's not about solving an issue and move on participant stated. Currently, a good number of board members understand and realise the need of ongoing investments. But there are still a lot of facts to be shared with them to appreciate the changing culture of cyber security.

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

In fact, there is still a group of users who do not appreciate the risks they encounter on daily basis. Not only for them but also for the company as a whole. These highlighted difficulties usually occur due to analysts‘ inability to influence on users directly. They just deal with the consequences because of the lack of investment from the top or wrong direction that come from the top-level board as well. A lot of repetitive is happening when user community goes around all the controls. For instance, behaviours that are prohibited consist of actions such as using personal devices on the network or travelling into a location that is not supposed to be travelling to whilst using work devices. These types of basic aspects results can take a large percentage

of analysts' time. Participant D added that most of team members and cyber analysts agree on the mentioned challenges. More precisely with the user behaviour side as they have direct interactions with them on frequent occasions. Issues like password security and length can cause the team time and effort instead of focusing on other essential elements. Clicking emails that are clearly include malicious and pirated software, browsing sites that are inappropriate for work environment are also the type of behaviours that analysts would agree on because people are not following security processes. To try and reduce the impact of users' behaviours, "D" stated that cyber awareness module training is required to be taken by all company users. But they spend up to 20 minutes working on it and they just forget about it. The following also stated:

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

Adding to above, technical difficulties are mentioned in terms of high alerts volume. False positives seem to be some of the main key technical challenges aspects. The previous role of "D" revealed that 95% of the defined incidents were ultimately false positives as participant stated. In current role environment, the ratio is reduced to be 50% of false positives. It is a big challenge as analysts are unable to go far beyond that without having in depth machine learning tools. A risk can be run where true positives could be lost whilst investigating false positive ones. It is a disturbing situation where analysts are required to spend time in the right places. Losing a true positive can lead to a disaster the head of cyber defence emphasised.

On reflection in terms of probability this may result in a lot of false positives, or an alerting logic may result in a lot of false positives. Thus, if it's 95% at the time it's false positive then there are few essential questions that need to be raised. Would the company just take the risk of giving 12 hours' worth of analyst time back to SOC? and who could be looking at other threats?. It is vital for business to identify whether an alert is true or false. As D added in current workplace it's balanced with 50/50 ratio but they are trying to reduce it as much as possible. They rely on experienced analysts when dealing with false positives. The experienced ones can get into

a conclusion once a ticket is open. This is due to their in-depth knowledge and familiarity working experience with network and its behaviours. But this can also lead to a triage biasing. It is a tricky situation to reduce the number when relying on manual investigations.

When asked about the role of machine learning and implementing automation techniques to try and mitigate false positives where analysts can have more focus on real true ones. Interviewee added the following:

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

Taking all the generated false positives and allow a machine learning method to work through the pattern. An analyst would be able to pick out outliers that they do not fit with false positive patterns. Therefore, they are more likely to pick up true positives and other critical alerts. Having such an approach in place is like the saying of two birds one stone. An overall picture of false positives alerts is valuable to provide mask that machine learning can use to detect true positives. As well via the adoption of techniques such as long tail analysis. There is usually a benefit to have plus even if it does not always get correct. It is an incredible useful solution for analysts where they can still search for these patterns in future if an identical behaviour is occurred.

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

It is crucial for analysts to gain knowledge and encounter variety of techniques and even challenge as well. One useful approach can be applied is similar to quality assurance. For instance, a series of alerts can be picked

each month then allow analysts to work through them step by step. Conclusions can be drawn on whether an analyst is required to change the behaviour of investigating such an alert or suggesting better techniques can be added to playbooks as well. Analysts can work collectively at teams but sometimes that teamwork might not exist. This is because they are not directly working together by checking or reviewing to gather more knowledge from their alerts.

Lastly, for the head of cyber defence the biggest struggle across organisations is the vast amount of data. They always need more data where there is too much potential to deal with them. There are also difficulties associated with data. Cost implications of working with data and also what to do with them? How long they will be stored for?. Accordingly, the future of instant triage is around ML and AI to complement analysts and assist them. Whether it is about collecting information that analysts may require for a successful triage, they need to spend less time on searching. It is vital for them to use their time for easier alerts that are faced before so they can close them automatically. This means an analyst can also have enough time to deal with a new occurrence of an alert. To summarise this interview, the industry is lacking enough experienced analysts. Thus, it's about using their time the best they can. Interviewee summed up that someone is required to write the ML code and it might comprise engineers, operators, or instant responders.

4.6 Interview V

To conclude the interviews, a fifth interview is conducted. The interviewee is acknowledged as participant E. A cyber security consultant at a large firm who is responsible for level 3 or tier 3 analysts in SOC environment is the role of the interviewee. Any event or incident that is escalated from level 1 and 2 will be directed to level 3 for indepth investigation. As part of the job, participant E interacts with SOC on up to 8 hours on daily basis. It is divided to interactions with level 1 and 2 analysts twice a day and the rest with level 3. When asked about the main challenges they currently face, the consultant added that one of the most significant issues is the quality of events.

This means when an event is being triaged to level 3, they require to look into it in a detailed investigation. Thus, it consumes time and effort. The quality of it is needed to be as high as possible to reduce workload

on tier 3 analysts. The biggest gap at the meantime is the skill difference from level 2 to level 3. There is another challenge which is the rotating door at tiers 1 and 2 analysts. Building a relationship with the company who is responsible of that is difficult due to the rotating of analysts. They can be at specific level then they might be moved around into different projects. Hence, it can get harder to start again with new analysts. As a result, communications gaps can be clearly noticed and recognised. As part of the services participant E company offers is outsourced SOC products. Their current client level 1 and 2 analysts are provided by external partner. Sometimes E can be on the opposite side while their firm is the one that provide tier 1 and 2 services. Almost every member of the team agree on the same issue of communication amongst each other. Partners and analysts rotation expose challenges to communication layer.

Building up those friendships and understanding the network is a massive matter to recognise the overall picture of the network. Otherwise, participant added that they can find themselves dealing with the same false positives over again. It is vital to reduce and cut down the noise to be able to communicate effectively and smoothly with partners. It will save everyone time and effort, but they are unable to do that at the moment due to the rotating door of analysts. The planned solutions by the organisation to overcome this type of obstacles is to try retaining talents and to accordingly communicate with their partners. There is a big skill shortage gap in general. Analysts are leaving due to variety of reasons such as getting better jobs with better benefits and privileges. Offering effective training, benefits pay plus the opportunity to be promoted and transfer into tier 3 SOC layer is required to improve retention as interviewee E mentioned.

In terms of managing huge set of data including false positives, the company use Sentinel SIEM tool for their current client. They currently face huge number of false positives. To deal with it, they use what is called a continuous service improvement plan. They look into fine tune and slim down the number of noisy alerts to try and pick the most valuable alert out of all these logs. The team could be dealing with up to 8 million alerts. Therefore, they make sure they work together following continuous service improvement (CSI) process to reduce the noise. When asked about any planned solutions or suggestions to overcome this difficulty the participant provided the following example:

They had a client that use Splunk as SIEM. They also used Splunk

phantom playbooks on top of it which helped massively in decreasing the number of false positives. It works by being able to whitelist an IP and to automatically filter through the whole scene tool. Then it would be automated out. As an analyst, it will not be required to try and triage that particular incident anymore. All it takes is to just whitelist it and be added to the system. Hence, this level of automation can reduce the noise. The interviewee insisted on the automation as it is the future of a SOC to reduce the number of manual efforts. When presented with the researcher idea about developing a code that is able to be fed with specific dataset including various logs to identify specific logs, the participant added the following:

"I feel there is an opportunity to take in the alerts as in a wider to ingest all the alerts into a Python program and do some form of analysis then filter everything out. Then, take only key alerts out of that. There is a lot of opportunity there. I don't know any tools that currently do it. I'm sure there might be something, but I've heard rumours of one guy looking into it. But yeah, there's a lot of opportunity there to slim down the number of false positives into something more".

Implementing such a code could be also added as a plugin into a SIEM tool depending on the type of the tool. Accordingly, the team often find that one rule normally triggers most of the noise. Unfortunately, it cannot be disabled due to its important features. Thus, implementing a process that can slim down a particular rule's noisiness can be an effective idea to be completed. Dealing with a lot of false logs can impact on other events where a true incident could be lost in all that false noise. Back to the beginning of the interview, the quality of triaged alerts is an essential issue to overcome where Tier 3 analysts do not need to look at the same alert everyday all day long leaving behind more vital aspects.

Additionally, the number of analysts currently manage SOC is between $10 - 20$ as overall based on the size of the client. Nonetheless, even it depends on the size of a client, but the team always feel they need more analysts as a last challenge mentioned by the consultant.

4.7 Findings

Based on the overall interviews' outcome, the researcher divided findings into various separate challenges for better understanding as follow:

- **Lack of Automation**
  Participants C, D and E agree on the automation challenge. SOC still lack the required automation to deal with events and logs. Applying more automation methods is required today more than ever due to the nature of technology plus the increasing amount of work when analysing events. The complexity of threats is risen and manual processes limitations are indications for the need of automation in moderinising SOC. Orgnisations must prioritise automation technologies to improve threats detection response time and operations deficiencies. Participants emphasised this need, reinforcing that automation is important for the future of SOC in managing security events effectively.

- **Number of logs**
  The huge number of logs is one of the challenges findings mentioned by both participants A and E. Both of them insisted on the need of an approach that is able to decrease the high number of alerts.

- **False Positives**
  C, D and E interviews revealed the challenge of false positives high numbers. A lack of effective automation approach is one of the reasons of not overcoming this problem.

- **Lack of Communication**
  The absence of effective communication amongst SOC analysts is another challenge per findings. Interviewees B, C and D emphasised on the need of improving communication within SOC. It can help in dealing with events more efficiently and smoothly.

- **Lack of Skilled Staff**
  A big gap is noticed in SOC in regards of skilled analysts. A, B and E highlighted the dilemma of not having enough analysts with the expected set of skills. Hence, lack of skilled staff is amongst the findings.

- **Unexpected Users Behaviours**
  The interviews outcome with B and D uncovered the challenge SOC analysts face when it comes to their organisation users. For example, a mistake from one user can expose the whole company into unwanted consequences.

- **Variety of Solutions**
  This finding includes the technical solutions that are implemented by an organisation. Interviewee C mentioned about merging various tools into one main solution. Using more than one tool exposes the team into variety of solutions usage challenges as C included.

- **Gap in Threat Intelligence and Manual Actions**
  In terms of lack of automation and relying on manual activities, participant C addressed this gap in threat intelligence. As a result, they are overwhelmed with the high amount of required search for information. Hence, automation is mentioned as a solution to reduce this impact.

- **Board Level Issues**
  Challenges in regards of board level are also amongst the gathered findings as participant D added. They are associated with stakeholders' body and individuals who have direct impact on decision making within an organisation.

Overall, the findings of these interviews validated the approach that is taken by the researcher. Expectations are confirmed in terms of the challenges as previous literature highlighted similar ones as well. Participants' responses aligned well with the objectives of investigating key challenges within SOC by literature and interviews. Thus, the insights gained reinforced our existing strategy. This validation provided a confidence in continuing with the same path with minor refinements. Hence, the approach that is selected for this research is carried out accordingly.

4.8 Theoretical Model

Are there any suggested solutions for the mentioned challenges?

Based on findings from interviews and literature review we created a theoretical model with essential developments on SOC elements - refer to below Figure 4.8.72.

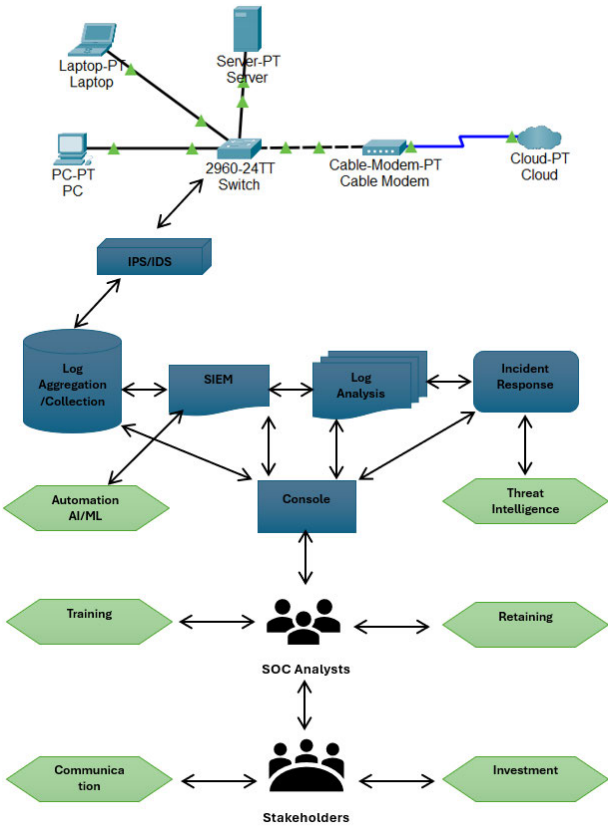


Figure 4.8.72: Proposed Theoretical Model

Accordingly, the roles of the stakeholders is an essential part of SOC building and improvements. They are required to invest and communicate clearly with SOC users as shown in the proposed theoretical model. On the other hand, analysts are required to be trained and retained to tackle the lack of skilled personnel challenge. Automation and threat intelligence are required to be added into SIEM and incident response to decrease the reliance on manual processes and to increase threats detection time and response. Interacting with SOC assets is required to be done via console that help analysts in accomplishing their tasks efficiently. The following subsections explain more about the essential required developments within SOC that are added to the theoretical model and presented in green colour.

4.8.1 Automation

To begin with automation, it includes AI and ML scripts that could be developed using programming languages such as python. They can integrate with SIEM tools like Splunk or added as plugins. A python code can be developed to collect data from an index such as windows security logs. Then integrate it with SIEM to quickly detect false positives that are associated with logs. The main key challenge is the number of generated logs. It is nearly impossible to investigate all of them which leaves organisations under potential threats constantly.

Dealing with a lot of false logs can impact on other events where a true incident could be lost. The quality of triaged alerts is an essential issue to overcome. Events correlations are required amongst having automation to pull data from external sources and partners using variety of algorithms.

4.8.2 Threat Intelligence

As this study is a UK based research, the solution for threat intelligence is retrieved from NCSC (2022) guidance. Depending on the organisation the value of Threat Intelligence (TI) will differ. For instance, if commercial tools are being used then TI is expected to be performed by the vendor. Whilst, if an organisation is looking to implement their own use cases, then they must be ahead of their game by looking into more TI. No matter what approach the organisation is implementing, it is essential to continuously be updated with threat environment. NCSC provides a service called Cyber Security Information Sharing Partnership (CISP) which can be effective for UK organisations to securely share cyber threat information. There are variety of TI platforms available but choosing the right threat intelligence platform based on organisation needs is important as it will be configured and linked with thier SIEM tool. One of the tools that can be considered is called MISP threat sharing. It is an open-source threat intelligence platform that can feed SOC with valuable TI information.

4.8.3 Retaining

To overcome skills shortages, organisations must retain talents and communicate with their partners. There is a big skill shortage gap in general where analysts are quitting. Salaries play a key role when deciding to leave but according to our findings other factors can impact on analysts' decision.

For example, being able to progress and learn more advanced skills is essential to make them feel trusted and looking forward for future promotions. The work environment is required to be healthy and occasionally conducting activities outside work is highly suggested. It helps in building good relationship amongst team members. It is important to highlight the retaining element so organisations can work on it. Offering effective training, benefits pay plus the opportunity to be promoted and transfer into different tiers in SOC layer is required to improve retention. Also, organisations can improve their retaining policies by retrieving insights from their current analysts for any enhancements that can be done.

4.8.4 Training

It is crucial for analysts to gain knowledge and encounter variety of techniques and even challenges as well. One useful approach can be applied is similar to quality assurance. For instance, a series of alerts can be picked each month then allow analysts to work through them step by step. Conclusions can be drawn on whether an analyst is required to change the behaviour of investigating such an alert or suggesting better techniques to be added to playbooks as well. Analysts can work collectively at teams to gather more knowledge from their alerts. Analysts are required to take constant training and update their information according to the evolving cyber threat landscape. To add to the above, all security measures can be under the risk of an internal users who might fall under phishing/scam attack. It is essential to make sure all employees are continuously undertaking essential cyber security awareness training.

4.8.5 Communication

There are two aspects that needs to be considered in terms of communications. First of all, communication amongst analysts. SOC managers need to make sure effective communications are carried out in terms of alerting triage and any further information that are required to be discussed. For example, if an analyst found out information about an upcoming/new threat, it is essential to spread the information amongst others. Not only by chat tools like Microsoft Teams but also to have maybe quick 5-10 minutes meetings to highlight any urgent details. On the other hand, effective communication between SOC manager and stakeholders is highly recommended. This help in developing and enhancing the current SOC to tackle future difficulties. In fact, SOC managers need to highlight the importance of such a develop-

ment and how it can impact positively on the organisation. They also need to understand the business as overall in order to satisfy stakeholders and explain the cyber security landscape in an easy and understanding way. From previous literature and our findings, communication is an essential matter that is required to be improved constantly. Hence, it is added as part of the recommended solutions.

4.8.6 Investments

Overall, without the required investments and understanding from above levels including stakeholders all measures would not take a place in such an organisation. It is essential for stakeholders to understand the need of SOC ongoing developments. SOC managers need to simplify the improvements ideas by understanding their stakeholders and explaining to them of why and how such an improvement in SOC will improve the business. An effective and clear strategy for SOC can be achieved by direct, strong and honest relationship amongst stakeholders and SOC mangers. Hence, without investments ongoing improvements and ideas cannot be implemented.

4.9 Discussion and Analysis

This section highlights the findings of the study conducted to discuss the connection between the gathered data and the literature review associated with the challenges of SOC. Below table 4.9.3 illustrates the key challenges that have been highlighted by interviewees. The first column contains these challenges whilst letters A-E refer to participants IDs. The author added "X" next to any challenge that have been identified by specific individual. Consequently, our data analysis is conducted using descriptive analysis and a summary of the key challenges that the interviewees raised.

A discussion is carried out to find any relationship between findings and previous literature conducted. In fact, interviews were recorded and transcripts were retrieved. The coding approach is used to refer to each participant. Each one of them mentioned specific challenges according to their role and organisation ‘s size. Role specification and organisations size played a key role when it comes to challenges. For example, board level issues are only mentioned by participant D due to the role specification of participant where a point of contact with stakeholders is part of the role.

Table 4.9.3: Challenges Faced By SOC

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

Accordingly, the identified challenges are 9. Therefore, table 4.9.3 provides calculation of each identified one. For instance, lack of automation, false positives, lack of communication and skilled analysts are mentioned 3 times amongst participants. Hence, they are the most common amongst the gathered insights. Figure 4.9.73 is an illustration of the number of the mentioned challenges as it depicts the highest and lowest challenges mentioned by participants.

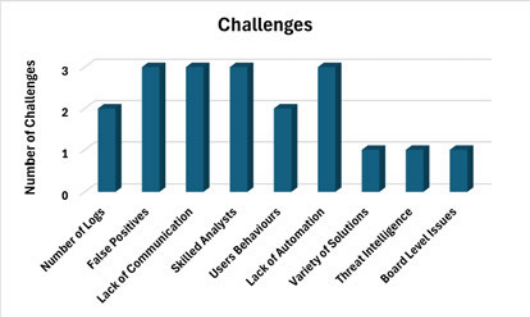


Figure 4.9.73: Challenges Faced by SOC Analysts

Onwubiko and Ouazzane (2019) study highlighted the lack of standardisation and understanding of SOC due to skills shortages in SOC. Participants A, B and E also emphasised on the big gap when it comes to skilled analysts' shortages. Another concern raised is with SOC services or policies that can impact service efficiencies by slowing down the speed as mentioned by Nalanagula and Roy (2022). This can be related to the variety of solutions implication that is mentioned by participant C, where combining various

tools and services into a main one could be beneficial.

Also, implementing the correct services is essential as added by Bikov et al. (2021) but this could lead to conflict decision between SOC manager and stakeholders which is part of the board level issues identified challenge by participant D. Ban et al. (2021) mentioned that a lot of tools could generate false positives but turning off one of these services could expose systems to major risks which is an implication added by participants A and E in terms of the number of generated logs. Alharbi (2020) raised a concern in terms of the quality of automation and false positives. Lack of automation and the number of false positives seem to be an issue amongst most of organisations. Participant D added that automation and machine learning can help in working through specific patterns where an analyst would be able to pick out outliers that they do not fit with false positive patterns.

Accordingly, users' behaviours challenge is also raised by Kokulu et al. (2019) in terms of having efficient training to prevent attacks such as phishing ones which can cause overwhelming job on SOC analysts. To try and reduce the impact of users' behaviours, "D" mentioned that cyber awareness module training is required to be taken by all company users, but they spend up to 20 minutes working on it and they just forget about it. Additionally, Mutemwa et al. (2018) stated that communications skills is the main key when working with people from different departments such as cyber security team and internal IT team. Most of participants mentioned the importance of communication amongst analysts where it can be challenging due to the amount of time they need to spend on investigation and analysis of security events.

Taqafi et al. (2023) agree on the pressure that SOC users are facing to ensure the safety of their organisations. Any weaknesses could cause and lead to security breaches which put SOC in difficult situations. Authors highlighted variety of challenges including the number of alerts, technology differentiation, people and budgets. The growing volume of logs is increasing constantly due to the usage of systems plus new added devices. Following up on every log and carrying out the required analysis can be very difficult task to achieve. Hence, the following question is raised, are SOC analysts focusing on genuine alerts?. On the other hand, SOC include huge duties and each one of them require unique systems and tools to be used. Therefore, challenges are exposed in terms of the variety of tools. Skills shortages and

lack of educated analysts is another challenge raised and agreed by authors which put SOC in an ongoing demand for skilled labour. This could take long periods of training and experience to be tackled. Accordingly, budgets have always been a concern for organisations. Questions are added by authors of how much is an organisation is willing to spend on SOC and how much risks are they willing to take as achieving 100% secure environment is not possible.

In terms of the mentioned and faced challenges there are differences between participants due to various aspects such as the size of the organisation and roles of individuals. Figure 4.9.74 depicts the number of challenges faced by each participant. One of the observations when it comes to the number of challenges mentioned by each participant. There seems to be a relationship between the role of participant and the number of challenges. For example, the role of participant D is head of cyber defence which is higher than other roles. Thus, the number of challenges mentioned by D is 5. In contrast, participant A is a cyber security engineer which has less responsibilities than head of defence. Hence, the challenges raised are only 2. As a result, the higher the position is the more challenges are being faced.

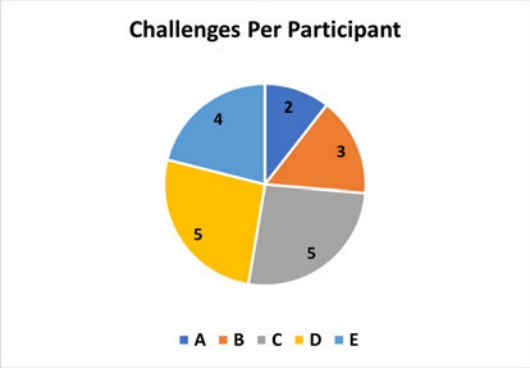


Figure 4.9.74: Participants Chart

Another key finding is the under-estimation of Threat Intelligence (TI) where it is mentioned only once by one participant, which could be due to a lack of awareness. This is a gap that must be bridged even between experts, as the rest of the participants miss it. As only five participants are interviewed to gather challenges, TI is not mentioned as it deserves. The absence of TI and the small number of interviews could have a relationship that limits the study. A bias could occur where the direction of these findings

led to a focus on automation. Thus, these findings are linked with previous literature to support the need for automation arguments.

To continue on the limitations, cyber security experts are interviewed from the user side of SOC. Therefore, vendors and manufacturers are required to be aware of the challenges, as well as to amend and modify tools in alignment with users requirements. Hence, vendors' views and opinions are essential to be considered.

Chapter Five

Automation Experiments

5 Automation Experiments

5.1 Introduction

In this chapter experiments are carried out by the researcher to implement an automation solution that identify logs and alerts based on particular pattern. As this research is about implementing a solution to tackle false positives/negatives, creating such a code will help in picking alerts based on their patterns. The used programming language is Python and it can be used by itself or integrated as plugin to SOC tools. The experiments took place on windows operating system using Jupyter notebook. Variety of dataset samples are used. Synthetic data was used in experiments I - III for testing purposes. However, for automation models Windows security logs are retrieved from a personal computer while Mac and Linux logs are extracted from github. Accordingly, the date of acquisition for these datasets was in 2023.

5.2 Experiment I

Listing 5.2.1 illustrates the beginning of experiments. The 4th line of code is written to define an alert criterion that matches logs that contain words error. Case sensitivity is ignored using regular expression method. Accordingly, a loop through a list of logs is added to check each log against the defined pattern. If an alert/log matches the pattern, an alert message is printed on the console. If not, information about specific service is also printed as added into the code.

Listing 5.2.1: Logs Auto Code

```
1  import re
2
3  # Define an alert criteria
4  alert_pattern = re.compile(r'error|warning', re.IGNORECASE)
5
6  # Define list of logs (this could come from a log file, database, etc.)
7  list_of_logs = [
8
9      "ERROR: Unsupported action or something is incorrect",
10     "WARNING: Need more investigation",
11     "INFO: Details about specific service"
12 ]
13
14 # Looping through each log and check if it matches the alert criteria
15 for log in list_of_logs:
16     if alert_pattern.search(log):
17         print("ALERT: {}".format(log))
18     else:
```

```
19          print("INFO: {}".format(log))
```

Running the above code provides the outcome on the console as shown in below Figure 5.2.75.

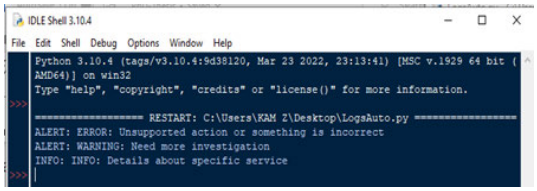


Figure 5.2.75: Logs Auto Running

This experiment was the first step towards developing an enhanced code to detect specific alerts. Logs are added directly into the code inside the "list_of_logs". However, the code can be improved to read errors from files, databases and any other services. For instance, sending logs and alerts to a monitoring system or email will require the implementation of more advanced criteria to identify specific alerts.

5.3 Experiment II

In this experiment the code is modified to read logs from a file instead of hard-coded list. Sample list of various errors codes is added into logs file as shown in Figure 5.3.76 below.

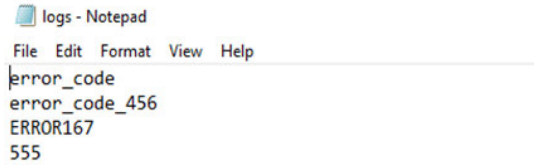


Figure 5.3.76: Logs File

Listing 5.3.2 is the modified code where lines 8-9 are added to read logs from logs.txt file. An alerting criterion is defined supposing the codes of false positives can be either 123 or 456. These codes can be changed depending on false positives codes that are occurring on particular service.

Listing 5.3.2: False Positive Code

```
1  import re
2
3  # Defining alert criteria
4  false_positive_pattern = re.compile(r'error_code_123|error_code_456', re.
       IGNORECASE)
5
6  # Reading logs from a file
7  with open("logs.txt", "r") as file:
8      log_list = file.readlines()
9
10 # Looping through each log in the file to check if it matches the alert criteria
       of false postives
11 for log in log_list:
12     if false_positive_pattern.search(log):
13         print("ALERT: {}".format(log))
14     #else:
15         #print("INFO: {}".format(log))
```

Based on the specified looping criteria running the above code will only print the alerts that include codes 123 & 456. The Else statement is commented for the purpose of testing and to show only false positive pattern. In fact, the list of logs has only one log that is associated with the defined criteria of codes 123/456. Therefore, the expected outcome on the console must include only one alert which is shown in below Figure 5.3.77.

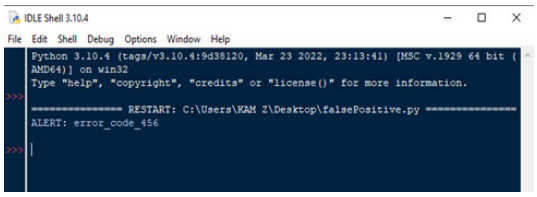


Figure 5.3.77: False Positive Running

To print the rest of logs into the console then Else statement in lines 14 & 15 must be uncommented. By unhighlighting it, the rest of logs will be printed as INFO as showing inside the statement. It can be changed as required. Figure 5.3.78 below is a screenshot of the running outcome on console.

5.4 Experiment III

Accordingly, the code is also modified to send alerts to a monitoring system based on the need and requirements of organisations. A new defined alert criteria is added as shown in listing 5.4.3 based on specific errors and

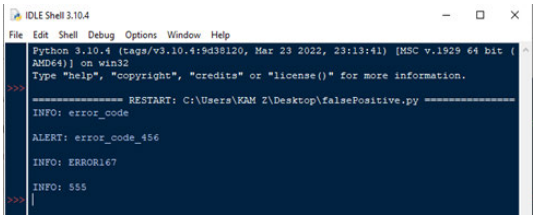


Figure 5.3.78: False Positive 1 Running

warning. A module called request is added in order to send post requests to the monitoring system that is specified by the variable in line 9. In this experiment we used the URL of example.com but it can be changed to the targeted URL of any particular monitoring system. An advanced pattern is implemented to filter out alerts that contain specific error codes that are actually not alerts. These logs are not going to be triggered as the "and not" logical operator is used as shown inside the loop statement.

Listing 5.4.3: Send Alert

```
1  import re
2  import requests
3
4  # Defining alert criteria
5  alert_pattern = re.compile(r'error|warning', re.IGNORECASE)
6  false_positive_pattern = re.compile(r'error_code_123|error_code_456', re.
       IGNORECASE)
7
8  # Defining the URL of the alerting system
9  alert_url = "https://example.com/alert"
10
11 # Reading logs from a file
12 with open("logs.txt", "r") as file:
13     log_list = file.readlines()
14
15 # Looping through each log in the file to check if it matches the alert criteria
         of the alerts and false postives
16 for log in log_list:
17     if alert_pattern.search(log) and not false_positive_pattern.search(log):
18         # Send alerts to the monitoring system
19         requests.post(alert_url, data={'message': log})
20         print("ALERT: {}".format(log))
21     else:
22         print("INFO: {}".format(log))
```

By running the above code, the expected outcome is to print ALERT next to any alert that does not include the codes of 123/456 where these will include INFO word next to them. This can be useful when looking into various logs to discard the false positives ones and distinguish them from

real logs.

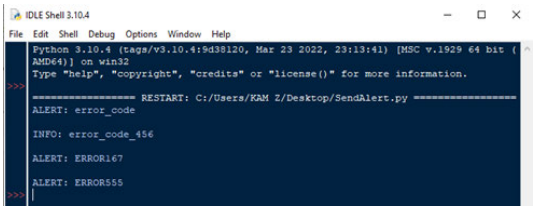


Figure 5.4.79: Send Alert Running

For the above example we used logs.txt file as shown in below Figure 5.4.80 where sample is added to it for testing. In fact, the alert pattern is defined in line 5 to pick any alert that include the word error or warning. Then all the errors apart from error_code_456 will be identified as alerts.

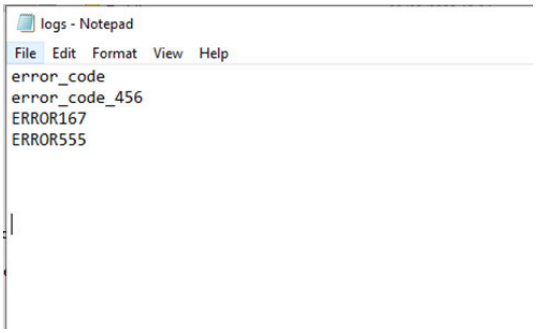


Figure 5.4.80: Logs I

5.5 Experiment IV

In this experiment real windows security logs are exported into excel sheet as shown in Figures 5.5.81 & 5.5.82 below. The events are associated with the researcher‘s personal device. Details such as event ID, date and time are included in these logs.

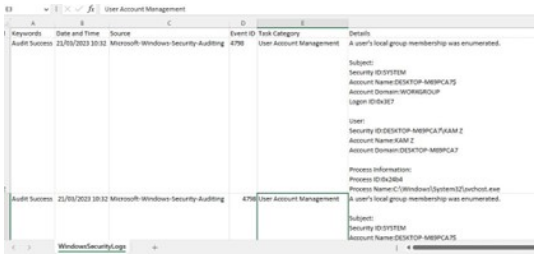


Figure 5.5.81: Windows Security Logs

Figure 5.5.82: Windows Security Logs Cont

A developed code in python is created as shown in listing 5.5.4 to automate events that are associated with specific Event ID. In this example, an event ID of 4798 is only printed to highlight how many logs/alerts are associated with this code. This can be an indicator of a specific behaviour that can be either malicious or genuine.

Listing 5.5.4: Python Code for Security Logs

```
# Importing panadas library
import pandas as pd

# Storing the CSV into file variable
file = 'WindowsSecurityLogs.csv'

# Reading contents of the file using dataframe from pandas
df = pd.read_csv(file)

# To show all columns and rows in console
pd.set_option('display.max_columns', None)
pd.set_option('display.max_rows', None)


# Selecting specific events based on event ID condition
selected_values = df.loc[df['Event ID'] == 4798]

# Printing out the outcome of the specified condition with the event row
    location
```

```
19 print(selected_values['Event ID'])
```

Running the above code will generate only events that are associated with event ID of 4798 as stated in condition at line 16. Therefore, below Figures 5.5.83 & 5.5.84 depict 87 logs associated with 4798 out of the 703 that are exported in the excel sheet.

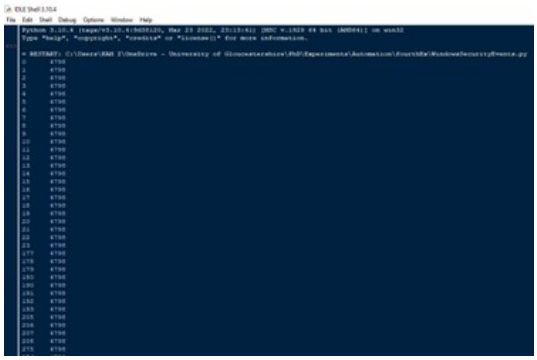


Figure 5.5.83: Compiled Python code for Security Logs I

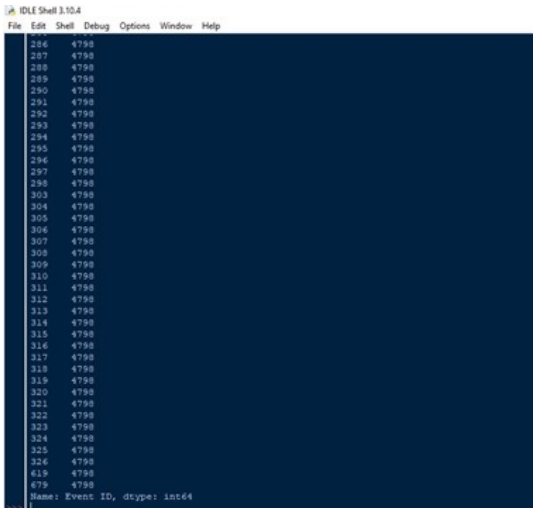


Figure 5.5.84: Compiled Python code for Security Logs II

There are different Event ID codes with different details but the code of 4798 is only chosen for the sake of experiment. However, different code based on different condition can be set to generate specific logs based on

requirements. The process of integrating python to log files including excel sheets or txt files can be helpful. It decrease the time spent by analysts to pick up or check if the file contains important alerts/logs. In fact, running and implementing automation using python code, specific alerts based on specific criteria can be picked up more effectively and smoothly. Thus, analysts can spend the rest of time focusing on other tasks.

5.6 Files Automation

Searching through files to find specific information is part of SOC analysts. In this experiment we propose an automation process to pick files based on specific defined pattern based on the provided code in listing 5.6.5.

Listing 5.6.5: Matched Files

```
import glob
import shutil
import os

# Defining the source and pattern to match files
source = "C:/Users/44739/Downloads/"
pattern = "*.txt" # This pattern can be change based on specific criteria

# Defining the name of the new folder
new_folder = "matched_pattern" # Change this to any name you require

# Creating a destination for the new folder
destination = os.path.join(source, new_folder)
os.makedirs(destination, exist_ok=True) # Creates the directory if it doesn't
    exist

# Use glob to get a list of matched files
matched_files = glob.glob(os.path.join(source, pattern))

# Iterating through the list of matched files
for file in matched_files:
    print("Matched File:", file)

    # Construct the destination path by joining the destination and the file's
        basename
    destination_path = os.path.join(destination, os.path.basename(file))

    # Copy the file to the destination
    shutil.copy(file, destination_path)
    print("File copied to:", destination_path + "\n")
```

The output of the code is shown in Figure 5.6.86 and 5.6.85 below

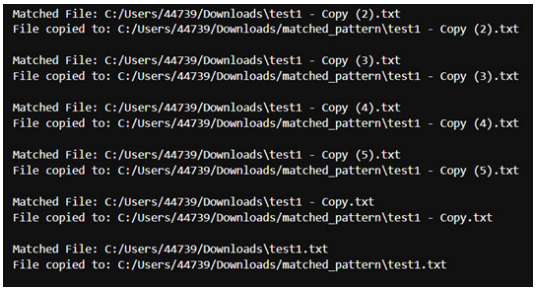


Figure 5.6.85: Matched Files Output

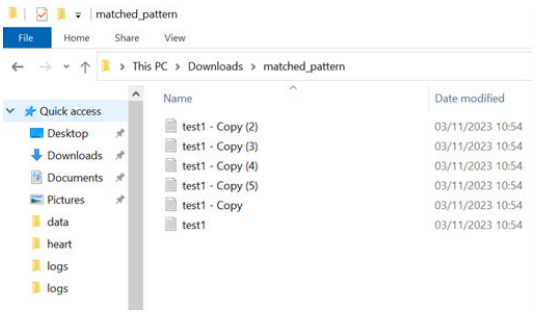


Figure 5.6.86: Matched Files Folder

In this experiment sample, we created a pattern to pick up files that end up with .txt extension from specific path. Then copied these files into a new folder called matched_pattern. Analysts can benefit from using similar approach to decrease their manual time whilst looking for specific files. For instance, files that ends up with .txt extension or any other extension can contain useful information about specific event on the system. Thus, a similar code can be used to identify these files and copy them into a new folder instead of manually checking every folder and subfolder on the system. This can save a lot of work and time where analysts can use their time more efficiently to deal with other critical issues. Few amendments are required in terms of using this specific code where source and destination paths are required to be changed based on the system or criteria a particular organisation is using.

5.7 Web Scraping Automation

Gathering information from external sources is part of SOC tasks. This information help and assist in threat intelligence. Our findings from partic-

ipant C where automation is highlighted to retrieve data instead of relying fully on manual work. In python an automation can be implemented to scrape data from websites. Listing 5.7.6 is an example of a program that is able to scrape data from Wikipedia then save these data into a CSV file as shown in Figure 5.7.87. Based on an organisation requirement the URL can be changed. The type of file whether .csv/.txt and all other elements of the code to achieve what is required.

Listing 5.7.6: Web Scraping

```
# Importing the required libraries

import requests
from bs4 import BeautifulSoup

# The URL of the website you want to scrap
url = "https://www.wikipedia.org/"

# Send HTTP GET request to the URL
reply = requests.get(url)

# HTTP Status code 200 means it is successful
if reply.status_code == 200:
    # Parse HTML content via BeautifulSoup
    soup = BeautifulSoup(reply.text, 'html.parser')

    # Searching the content you want to scrap by checking the HTML of the page
        such as <p> tags
    contents = soup.find_all('p')

    # Create a file to save the scraped content
    with open('contents.csv', 'w', encoding='utf-8') as file:
        for i in contents:
            file.write(i.get_text() + '\n')

    print(f"Scraping is successful. Status Code: {reply.status_code}")
else:
    print(f"Scraping is not successful. Status code: {reply.status_code}")
```

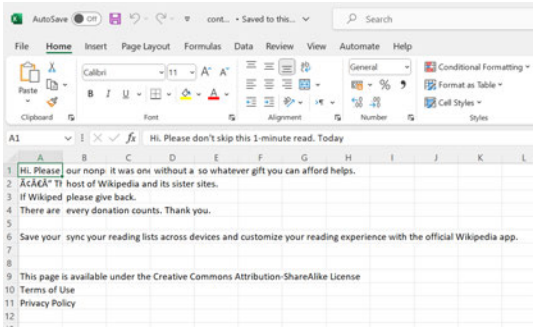


Figure 5.7.87: Contents.csv

Implementing such an automation process is effective to reduce manual search where time can be put on other important aspects. Before scraping any data SOC team must be aware of the legal concerns. Including the terms of websites and any other information of scraping such data. Adding to above, running such a python script can also be automated using time scheduler on windows or any other operating system. By creating task schedule as shown in Figure 5.7.88 depending on requirements the script will be running and data for threat intelligence will be gathered occasionally based on set parameters. Hence, manual work will be reduced and there will be no need to search manually. Refer to below screenshot for how to automate the running of python script in windows.

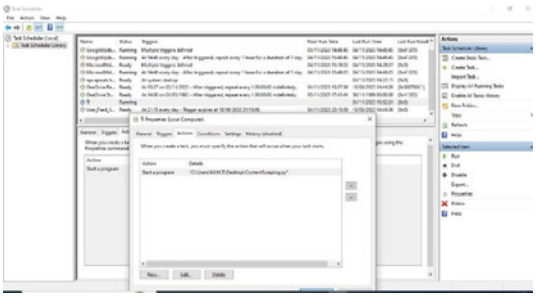


Figure 5.7.88: Task Scheduler

5.8 Automation Models

An automation model solution is divided into different stages including importing, exploring, visualisation and evaluating data results. The data include a sample of windows security logs, sample of MAC logs and sample

of Linux logs that are exported into excel sheet. An effective data visualisation is designed to tell the story of the data sample. This can help organisations and businesses in making data-driven decisions. The models are created using Python programming language and its libraries for the automation purposes. Software tools that used are Anaconda navigator and JupyterLab. The models are established using Python to analyse and predict results based on the trained dataset. The following points provide the steps that have been taken for all different samples. Nonetheless, windows security, Mac and Linux logs samples models are divided into separate subsection for further clarification.

Understanding the Problem

First of all, we predict logs based on their features such as an event ID. The goal is to try and retrieve accurate predictions.

Data collection

The key behind any model is data and without it the model is not able to predict results. The data are windows security logs from the researcher‘s personal computer that have been imported into the CSV file and then loaded into the model. Whilst mac and Linux logs are retrieved from open source platform which is github.

Data Preprocessing

Includes cleaning raw data, handling missed values and convert any categorical variable. For example, if a column is already numerical it does not need any amendments. Where categorical columns are changed to integer data type for better prediction results.

Exploratory Data Analysis (EDA)

This step includes using various methods to discover patterns such as using histograms.

Model Selection

In our example, we have used 3 various algorithms to retrieve results for all three samples models.

Model Training

Models are trained on 80% of the data where the remaining test data are 20% are left for testing.

Models Evaluation

A model performance is also evaluated using different metrics such as confusion matrix and class report.

Model Flow Chart

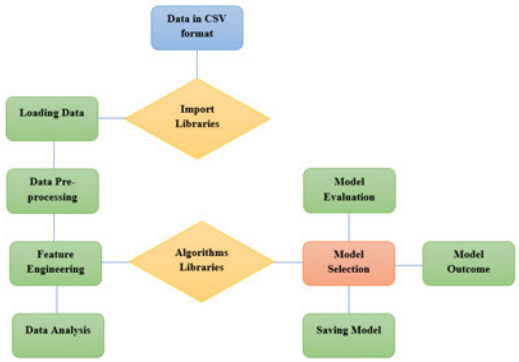


Figure 5.8.89: Flow Chart

5.8.1 Windows Security Logs Model

5.8.1.1 Exploratory Data Analysis (EDA)

For completing such a model first of all we've started by importing the required libraries and the dataset as shown in listing 5.8.7.

Listing 5.8.7: Windows Logs Python Libraries

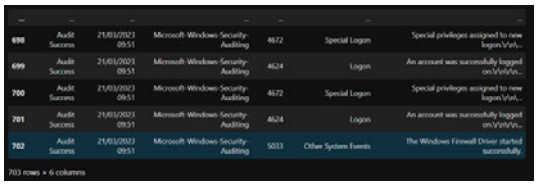
```
1  import numpy as np
2  import pandas as pd
3  import matplotlib.pyplot as plt
4  import seaborn as sns
5  from pycaret.classification import *
6
7  # Loading the CSV file using pandas library
8
```

```
dataFrame = pd.read_csv('logs/WindowsSecurityLogs.csv')

# Printing out the data

dataFrame
```

The dataset is printed out as shown below in Figures 5.8.90 and 5.8.91.

	Keywords	Date and Time	Source	Event ID	Task Category	Details
0	Audit Success	21/01/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
1	Audit Success	21/01/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
2	Audit Success	21/01/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
3	Audit Success	21/01/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
4	Audit Success	21/01/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...

Figure 5.8.90: Windows Dataset I



698	Audit Success	21/01/2023 09:51	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon:\r\n...
699	Audit Success	21/01/2023 09:51	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on:\r\n\r\n...
700	Audit Success	21/01/2023 09:51	Microsoft-Windows-Security-Auditing	4672	Special Logon	Special privileges assigned to new logon:\r\n...
701	Audit Success	21/01/2023 09:51	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on:\r\n\r\n...
702	Audit Success	21/01/2023 09:51	Microsoft-Windows-Security-Auditing	5033	Other System Events	The Windows Firewall Driver started successfully

703 rows × 6 columns

Figure 5.8.91: Windows Dataset II

To decide what columns or rows that most applicable for our scenario, cleaning and exploring the dataset are done using various python built-in functions such as info(), head(), tail(), describe(). In listing 5.8.92 dataFrame.info() shows that there is no missing data.

Listing 5.8.8: Windows Logs Data Preprocessing

```
# Data information

dataFrame.info()

# Checking the data statistics

dataFrame.describe()

# To check if the dataset has null values

dataFrame.isna().sum()


# To check if there is any duplicate rows

dataFrame.duplicated().sum()

```

```
18  dataFrame.duplicated()
19
20
21  # Dropping duplicated rows
22
23  original_data = pd.read_csv('logs/WindowsSecurityLogs.csv')
24
25  data_without_duplicates = original_data.drop_duplicates()
```

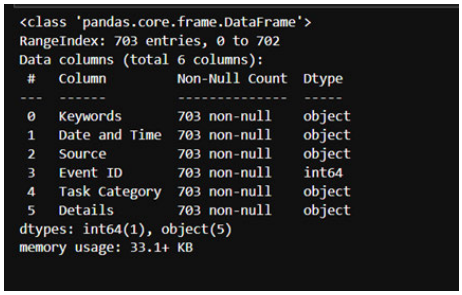
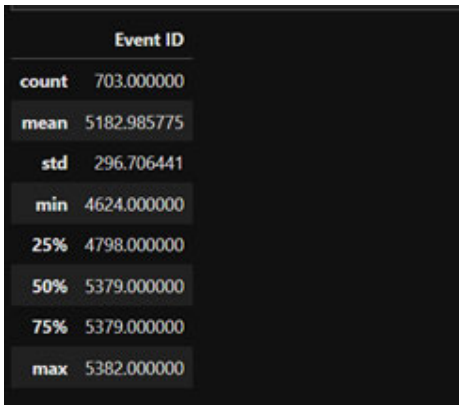


Figure 5.8.92: Windows DataFrame Information

Checking the dataset statistics is done via line 7 and the printed output is shown in Figure 5.8.93.



	Event ID
count	703.000000
mean	5182.985775
std	296.706441
min	4624.000000
25%	4798.000000
50%	5379.000000
75%	5379.000000
max	5382.000000

Figure 5.8.93: Windows Dataset Statistics

Figure 5.8.94 illustrates the output of line 11 to check if there are any null values in dataset which approves that there is 0 so none. We have also checked for duplicated rows and returned 580 duplicated ones.

```
Keywords         0
Date and Time    0
Source           0
Event ID         0
Task Category    0
Details          0
dtype: int64
```

Figure 5.8.94: Windows Dataset Null Values

Therefore, we have dropped them using the code in line 23-25 in listing 5.8.92 to clean the dataset. The results are printed out as shown in Figures 5.8.95 – 5.8.97. We‘ve left with 123 rows as the original dataset was 703 rows.

```
0      False
1      False
2      False
3      False
4      False
       ...
698     True
699     True
700     True
701     True
702    False
Length: 703, dtype: bool
```

Figure 5.8.95: Windows Dataset Duplicates

	Keywords	Date and Time	Source	Event ID	Task Category	Details
0	Audit Success	21/03/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
1	Audit Success	21/03/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
2	Audit Success	21/03/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
3	Audit Success	21/03/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
4	Audit Success	21/03/2023 10:32	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
...	...	...	...	...	...	...

Figure 5.8.96: Windows Dataset Without Duplicates I

678	Audit Success	21/03/2023 09:51	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.\r\n\r\n...
679	Audit Success	21/03/2023 09:51	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated...
680	Audit Success	21/03/2023 09:51	Microsoft-Windows-Security-Auditing	5024	Other System Events	The Windows Firewall service started successfu...
685	Audit Success	21/03/2023 09:51	Microsoft-Windows-Security-Auditing	4799	Security Group Management	A security-enabled local group membership was ...
702	Audit Success	21/03/2023 09:51	Microsoft-Windows-Security-Auditing	5033	Other System Events	The Windows Firewall Driver started successfully.

123 rows × 6 columns

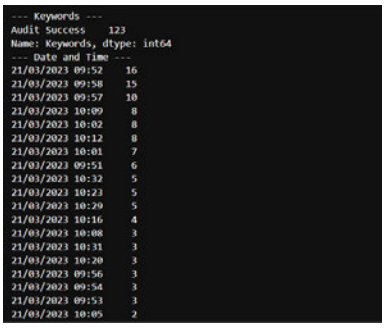
Figure 5.8.97: Windows Dataset Without Duplicates II

As a result, the cleaned data is saved into a new CSV file and named data_without_duplicates for better analysis using the code in listing 5.8.9.

Listing 5.8.9: Windows Dataset Without Duplicates CSV

```
1  # Saving the resulting DataFrame to a new CSV file
2
3  data_without_duplicates.to_csv('logs/data_without_duplicates.csv', index=False)
4
5  # Running a loop of value counts to distinguish unique values
6
7  for c in data_without_duplicates.columns:
8      print ("--- %s ---" % c)
9      print (data_without_duplicates[c].value_counts())
```

Line 7 - 9 code is the loop that it is used to discover noisy data based on unique values. Therefore, the dataset can be further cleaned and more ready for training our model as shown in Figures 5.8.98 - 5.8.103.



```
--- Keywords ---
Audit Success    123
Name: Keywords, dtype: int64
--- Date and Time ---
21/03/2023 09:52    16
21/03/2023 09:58    15
21/03/2023 09:57    10
21/03/2023 10:09     8
21/03/2023 10:02     8
21/03/2023 10:12     8
21/03/2023 10:01     7
21/03/2023 09:51     6
21/03/2023 10:32     5
21/03/2023 10:23     5
21/03/2023 10:29     5
21/03/2023 10:16     4
21/03/2023 10:08     3
21/03/2023 10:31     3
21/03/2023 10:20     3
21/03/2023 09:56     3
21/03/2023 09:54     3
21/03/2023 09:53     3
21/03/2023 10:05     2
```

Figure 5.8.98: Windows Value Counts

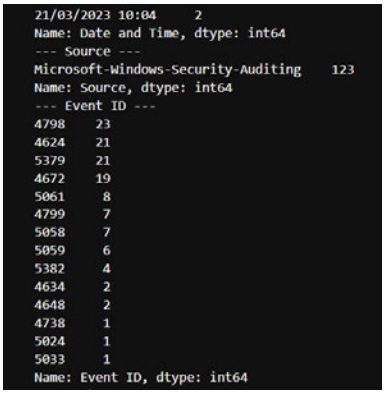


Figure 5.8.99: Windows Value Counts Outcome I

Figure 5.8.100: Windows Value Counts Outcome II

Figure 5.8.101: Windows Value Counts Outcome III

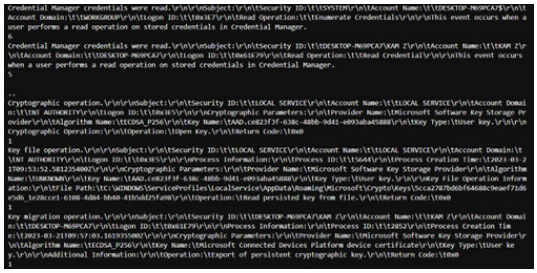


Figure 5.8.102: Windows Value Counts Outcome IV

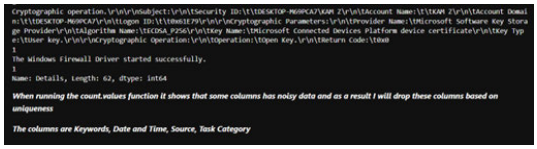
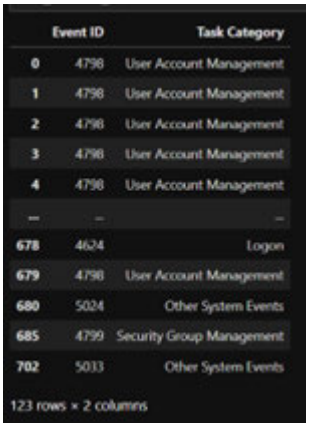


Figure 5.8.103: Windows Value Counts Outcome V

Listing 5.8.10: Windows Noisy Data Drop

```
# Dropping noisy data from the dataset based on uniqueness

data_without_duplicates.drop(['Keywords','Date and Time', 'Source', 'Details'],
     axis=1, inplace=True)

data_without_duplicates.info()
```

Columns such as keywords, date and time, source and details have noisy data so the decision is made to drop them. Hence, event Id and task category column are the only column left as shown in listing 5.8.10 code and output in Figures 5.8.104 and 5.8.105.



	Event ID	Task Category
0	4798	User Account Management
1	4798	User Account Management
2	4798	User Account Management
3	4798	User Account Management
4	4798	User Account Management
...	...	...
678	4624	Logon
679	4798	User Account Management
680	5024	Other System Events
685	4799	Security Group Management
702	5033	Other System Events

123 rows × 2 columns

Figure 5.8.104: Windows Dropped Noisy Data

```
<class 'pandas.core.frame.DataFrame'>
Int64Index: 123 entries, 0 to 702
Data columns (total 2 columns):
 #   Column         Non-Null Count  Dtype
---  ------         --------------  -----
 0   Event ID       123 non-null    int64
 1   Task Category  123 non-null    object
dtypes: int64(1), object(1)
memory usage: 2.9+ KB
```

Figure 5.8.105: Windows Data Without Duplicates Information

Listing 5.8.11 shows that event id is mapped into single numerical values of 0 -13 based on its specific ID. Based on the uniqueness we gathered these values of the event Id column (4798, 4624, 5379, 4672, 5061, 4799, 5058, 5059, 5382, 4634, 4648, 4738, 5024, 5033). Therefore, we have assigned values of 0 - 13 to these events Ids to have better results when developing the model using map function. After converting the Event ID column into 0 -13. Task column also converted into numerical based on the retrieved uniqueness using the map function to have better prediction results as well.

Listing 5.8.11: Windows Mapped Numerical Values

```
1  # mapping the event id into single numerical values based on its specific ID
2
3  # Based on the uniqueness we gathered these values of the event Id column (4798,
       4624, 5379, 4672, 5061, 4799, 5058, 5059, 5382,
4  # 4634, 4648, 4738, 5024, 5033)
5
6  # Therefore I have assigned values of 0 - 13 to these events Ids to have better
       results when developing the model using map function
```

```
7
8
9  data_without_duplicates['Event ID'] = data_without_duplicates['Event ID'].map
       ({4798: 0, 4624: 1, 5379: 2, 4672: 3, 5061: 4, 4799: 5, 5058: 6, 5059: 7,
       5382: 8, 4634: 9, 4648: 10, 4738: 11, 5024: 12, 5033: 13})
10
11 # Task Category column
12
13 data_without_duplicates['Task Category'] = data_without_duplicates['Task
       Category'].map({'User Account Management': 0, 'Logon': 1, 'Special Logon':
       2, 'Other System Events': 3, 'System Integrity': 4, 'Security Group
       Management': 5, 'Logoff': 6})
14
15
16 data_without_duplicates.info()
```

Figures 5.8.106 and 5.8.107 depict the confirmation of the changes.

```
<class 'pandas.core.frame.DataFrame'>
Int64Index: 123 entries, 0 to 702
Data columns (total 2 columns):
 #   Column         Non-Null Count  Dtype
---  ------         --------------  -----
 0   Event ID       123 non-null    int64
 1   Task Category  123 non-null    int64
dtypes: int64(2)
memory usage: 2.9 KB
```

Figure 5.8.106: Windows Mapped Numerical Values Changes Confirmation I

```
: data_without_duplicates
```

	Event ID	Task Category
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
...	...	...
678	1	1
679	0	0
680	12	3
685	5	5
702	13	3

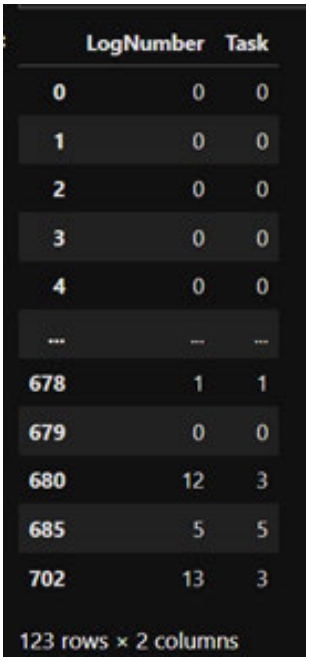
123 rows × 2 columns

Figure 5.8.107: Windows Mapped Numerical Values Changes Confirmation II

To avoid any errors or unnecessary bugs, Event ID and Task Category columns names are changed to remove any spaces or special characters. As a result, Event ID is now LogNumber and Task Category is Task as shown in Figure 5.8.108.

Listing 5.8.12: Windows Columns Names Changes Code

```
#replacing some special character columns names with proper names

data_without_duplicates.rename(columns={'Event ID': 'LogNumber', 'Task Category
    ': 'Task'}, inplace=True)
data_without_duplicates.columns

data_without_duplicates
```



	LogNumber	Task
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
...	...	...
678	1	1
679	0	0
680	12	3
685	5	5
702	13	3

123 rows × 2 columns

Figure 5.8.108: Windows Columns Names Changes

Plotting a bar graph for Event ID(LogNumber) against Task Category(Task) mean to see the co-relation between these columns as illustrated in Figure 5.8.109.

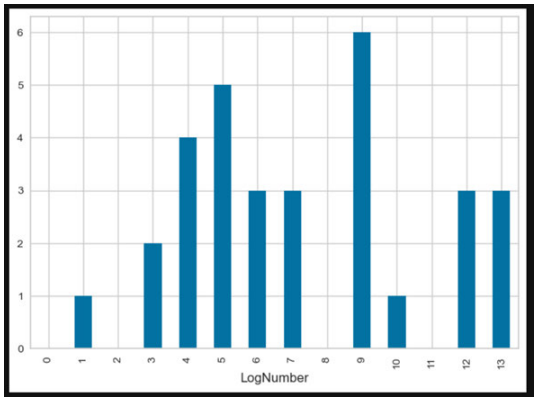


Figure 5.8.109: Windows Log Number and Task Mean Bar Chart

We can see from the data visualisation in Figure 5.8.109 Event 4634 which we refer to it as 9 is likely to be associated with the task of 'Logoff': 6. Whilst event 5 is likely to be linked with task 5 'Security Group Management': 5.

We have also plotted logs numbers and their associated tasks into a scatter plot including a trend-line as shown below in Figure 5.8.110. By hovering on blue dots each log number will disclose its task value.

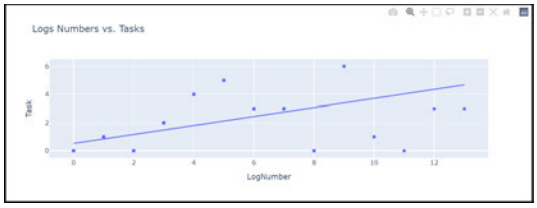


Figure 5.8.110: Windows Log Numbers and Tasks Scatter Plot

Moreover, we can check the categorical values of task column by using world cloud approach as shown in Figure 5.8.111

Figure 5.8.111: Windows Tasks Column Word Counts

A correlation between both columns is also presented in Figure 5.8.112

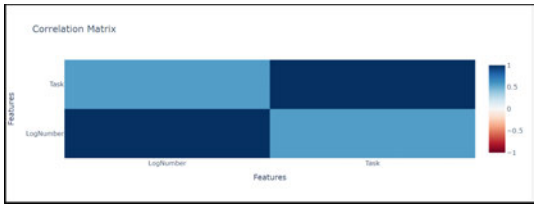


Figure 5.8.112: Windows Log Number and Task Correlation

5.8.1.2 Models Selection

As the data is labeled and the output feature is known a supervised model is the preferred one. Hence, we have chosen supervised model for this classification. Popular classification algorithms include; Logistic Regression, Decision Tree, Random Forest, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Naive Bayes and Neural Networks (Deep Learning).

Listing 5.8.13 shows the chosen algorithm for this model which is Decision Tree Classifier. It also describes that the dataset is split into 80% of training data and 20% of testing. However, this percentage can be changed based on the need.

Listing 5.8.13: Windows Decision Tree Classifier

```
1  # Import scikitlearn module for the model DecisionTreeClassifier
2
3  from sklearn.tree import DecisionTreeClassifier
4  from sklearn.model_selection import train_test_split
5  from sklearn.metrics import accuracy_score
6
7  # Example for classification
8  # X axis is our independent variable LogNumber
9  #Y axis is our dependent variable or the Task of log
```

```
10
11  X = data_without_duplicates.drop('Task', axis=1)
12  y = data_without_duplicates['Task']
13
14
15  # Split the data into 80% training and 20% testing data
16  # We have to split the idependent variables (x) and the target or dependent
        variable (y)
17
18  X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
        random_state=42)
19
20  # Example for classification
21  clf = DecisionTreeClassifier(random_state=42)
22  clf.fit(X_train, y_train)
23
24  y_pred = clf.predict(X_test) # For classification
25
26  accuracy = accuracy_score(y_test, y_pred)
27  print(f'Accuracy: {accuracy}')
```

When running the model with 20% of test data the accuracy score is 1 which is very good as depicted in Figure 5.8.113. Changing the percentage can also change in accuracy score.

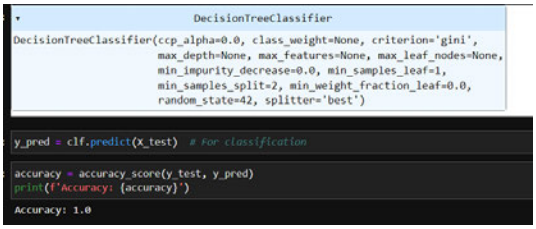


Figure 5.8.113: Windows DT Accuracy

The model is evaluated using confusion matrix and class report. Both plots show a good evaluation result of 100% and 1 for features such as precision and F1 as shown in Figures 5.8.114 – 5.8.115.

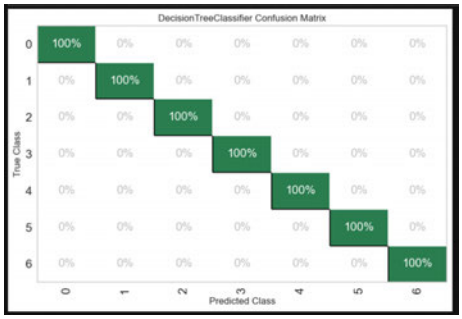


Figure 5.8.114: Windows Confusion Matrix

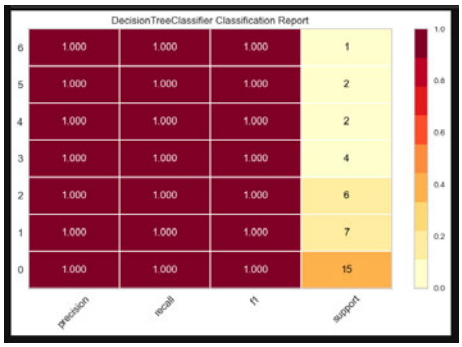


Figure 5.8.115: Windows Class Report

Figure 5.8.116 below shows the prediction result of the Decision Tree classifier.

Figure 5.8.116: Windows DT Prediction

Finally, Figure 5.8.117 depicts the saved model which is called Logs. This can be changed based on requirements.

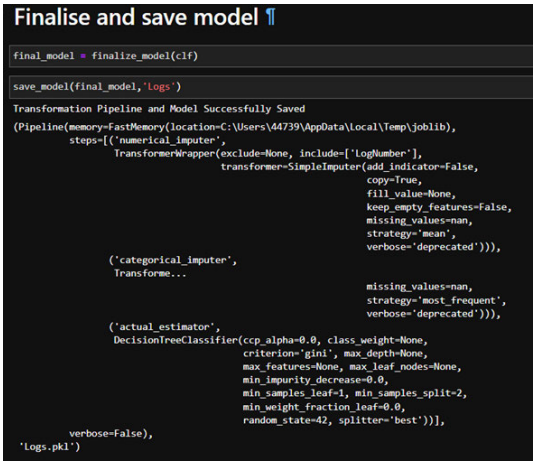


Figure 5.8.117: Windows Model Saved

5.8.1.3 Evaluation

In this dataset the only column that is associated with numbers is Event ID. Its datatype is int64 as we've seen in previous screenshot. Events IDs are normally referred to a specific action or an event that is occurring on the system. For instance, false positives or negatives can be picked up based on their specific event id. From the dataset, we can see that 4624-event id is associated with logon activity whilst 4672 is linked to special logon. As this research is primarily on understanding and creating such an automation solution to deal with logs either false positives or negatives, we have visualised the event ids in different types of figures. Event ids that occurred on a system can be extracted from the dataset which helps in retrieving insights of the logs.

Understanding event types that occur on the system and their number is essential for SOC to make decisions of what is required to be minimised. This can be achieved by using data analysis visualisations and automation techniques. We've seen events that between 5200 – 5400 are the most occurred ones. Therefore, if they are related to a specific service that is not important for the business, then this service can be shut down to reduce the number of these logs. Otherwise, different approach can be taken by ignoring these types of events in the future if they are associated with false positives. Thus, time can be saved so analysts can work on more important

events.

For the model selection, Decision Tree retrieved a score of 1 but when tried linear regression algorithm the score was 0.43 as shown in Figure 5.8.118. Hence, Decision Tree is the preferred one for this model. Additionally, all other algorithms can be used and tested based on the requirements where the model can be monitored based on different predictions outcome.

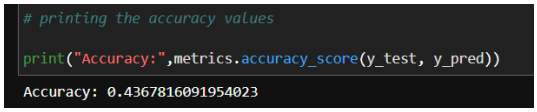


Figure 5.8.118: Windows LR Accuracy

Also the prediction score for Logistic Regression is shown in Figure 5.8.119

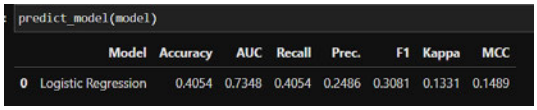


Figure 5.8.119: Windows LR Prediction

Another algorithm is tested against this dataset which is Ridge Classifier. Thus the accuracy was 0.48 whilst the prediction was 0.51 as shown in below Figures 5.8.120 and 5.8.121.

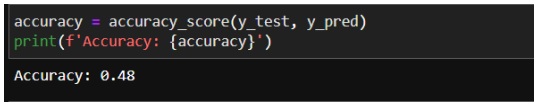


Figure 5.8.120: Windows RC Accuracy

```
predict_model(clf)
```

	Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC
0	Ridge Classifier	0.5135	0	0.5135	0.2765	0.3549	0.2336	0.3529

Figure 5.8.121: Windows RC Prediction

Accordingly, below table 5.8.4 and Figure 5.8.122 are the comparison of the accuracy scores of the three tested algorithms for windows security logs.

Table 5.8.4: Windows Logs Algorithms Accuracy

Algorithm	**Accuracy**
Decision Tree	1
Logistic Regression	0.43
Ridge Classifier	0.48

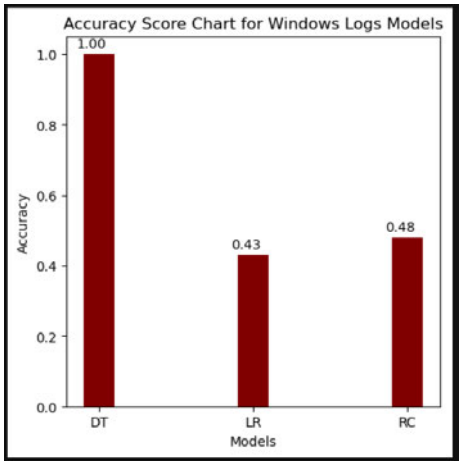


Figure 5.8.122: Windows Logs Models Accuracies

5.8.2 Mac Logs Model

5.8.2.1 Exploratory Data Analysis (EDA)

For Mac Logs EDA we have used the same approach by firstly importing the required libraries and output the dataset as shown in listing 5.8.14

Listing 5.8.14: Mac Logs Python Libraries

```
# Importing the required libraries

import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# reading data from csv file

df = pd.read_csv("logs\Mac_Logs.csv")

df
```

Figure 5.8.123: MacLogs Dataset I

Figure 5.8.124: MacLogs Dataset II

The dataset includes 2000 rows and 11 columns. We have taken the steps of checking data information plus data preprocessing to eliminate any null values or converting categorical columns to numerical format. Listing 5.8.15 shows the code snippet for these steps.

Listing 5.8.15: Mac Logs Data Preprocessing

```
# data information

df.info()

# data stats

df.describe()

# To check if the dataset has null values

df.isna().sum()

# To check if there is any duplicate rows - no duplicates
```

```
14
15 df.duplicated().sum()
16
17 # Running a loop of value counts to distinguish unique values
18
19 for c in df.columns:
20     print ("--- %s ---" % c)
21     print (df[c].value_counts())
```

The output is depicted in Figures 5.8.125 - 5.8.127.

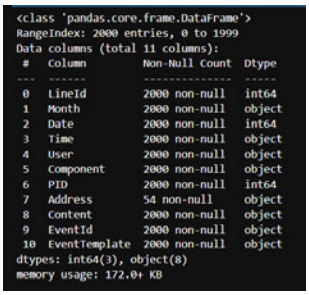


Figure 5.8.125: MacLogs Dataset Information

	LineId	Date	PID
count	2000.000000	2000.000000	2000.000000
mean	1000.500000	4.363500	8128.371500
std	577.494589	2.011813	13672.542824
min	1.000000	1.000000	0.000000
25%	500.750000	3.000000	0.000000
50%	1000.500000	4.000000	94.000000
75%	1500.250000	6.000000	10018.000000
max	2000.000000	8.000000	39203.000000

Figure 5.8.126: MacLogs Dataset Statistics

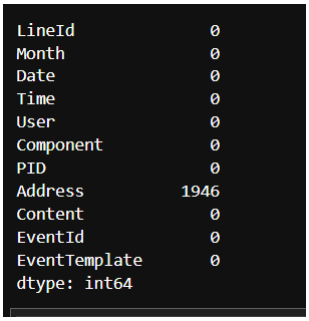


Figure 5.8.127: MacLogs Dataset Null Vlaues

In listing 5.8.16 the code is used to drop noisy data plus to take off the letter "E" of EventId column for the purpose of model training.

Listing 5.8.16: Dropped Mac Logs Noisy Data

```
# Dropping noisy data from the dataset based on uniqueness

new_data = pd.read_csv('logs/Mac_Logs.csv')

df = new_data.drop(['LineId','EventTemplate', 'Date', 'Month', 'Address', '
    Content'], axis=1, inplace=True)

new_data

# As Event Id column has letter E at the start of each cell, I will remove it
    then convert the
# whole column to integer for more analysis and prediction

new_data['EventId'] = new_data['EventId'].str[1:]

new_data['EventId'] = new_data['EventId'].astype(int)

new_data

new_data.to_csv('logs/new_data.csv', index=False)
```

The new dataset is saved into a new variable called new_data as the output showing in Figure 5.8.128.

	Time	User	Component	PID	EventId
0	09:00:55	calvisitor-10-105-160-95	kernel	0	252
1	09:01:05	calvisitor-10-105-160-95	com.apple.CDScheduler	43	323
2	09:01:06	calvisitor-10-105-160-95	QQ	10018	216
3	09:02:26	calvisitor-10-105-160-95	kernel	0	128
4	09:02:26	authorMacBook-Pro	kernel	0	124
...	...	...	...	...	...
1995	07:32:03	calvisitor-10-105-162-124	kernel	0	142
1996	07:43:38	calvisitor-10-105-162-124	kernel	0	331
1997	07:57:11	calvisitor-10-105-162-124	kernel	0	120
1998	08:10:46	calvisitor-10-105-162-124	kernel	0	338
1999	08:10:46	calvisitor-10-105-162-124	kernel	0	121

2000 rows × 5 columns

Figure 5.8.128: MacLogs New Data

We have also saved the data into new dataset after applying the required feature engineering and the preprocessing in previous steps. listing 5.8.17 is the code for providing charts of the processed data. However, we have used EventId and PID columns as they are the numerical data plus of what we will use for training the model and storytelling.

Listing 5.8.17: Mac Logs Charts

```
# Providing Scatter plot for EventId and PID

import plotly.express as px

fig = px.scatter(new_data, x='EventId', y='PID', trendline = 'ols', title='
    EventId vs PID')

fig.show()

# Correlation map

import plotly.graph_objects as go

corr_matrix = new_data.corr(numeric_only=True)

fig = go.Figure(data=go.Heatmap(z=corr_matrix.values,
                            x=corr_matrix.columns,
                            y=corr_matrix.index,
                            colorscale='RdBu',
                            zmin=-1,
                            zmax=1))

fig.update_layout(title='Correlation Matrix',
                xaxis_title='Features',
                yaxis_title='Features')

fig.show()

```

```
# World cloud figure

from wordcloud import WordCloud

tasks = ' '.join(new_data['Component'].astype(str))
wordcloud = WordCloud().generate(tasks)

fig = px.imshow(wordcloud, title='Component Word Cloud')
fig.show()

# Plotting a bar graph for Event ID

# Plotting

fig, ax = plt.subplots()

# Bar width can be adjusted using the width parameter

bar_width = 0.35

# Plot the EventId column

ax.bar(new_data.index, new_data['EventId'], width=bar_width, label='EventId')

# Set labels and title

ax.set_xlabel('Row number')
ax.set_ylabel('Event ID Value')
ax.set_title('Bar Chart of Event ID Column')
ax.legend()

# Show the plot

plt.show()

# Plotting a bar graph for Process ID

# Plotting

fig, ax = plt.subplots()

# Bar width can be adjusted using the width parameter

bar_width = 0.35

# Plot the EventId column

ax.bar(new_data.index, new_data['PID'], width=bar_width, label='PID')

# Set labels and title

ax.set_xlabel('Row number')
ax.set_ylabel('Process ID Value')
ax.set_title('Bar Chart of Process ID Column')
ax.legend()

```

```
84  # Show the plot
85
86  plt.show()
```

The EventId and PID scatter plot is in Figure 5.8.129. Hovering over the dots can provide you with an Event Id and its associated Process ID value.

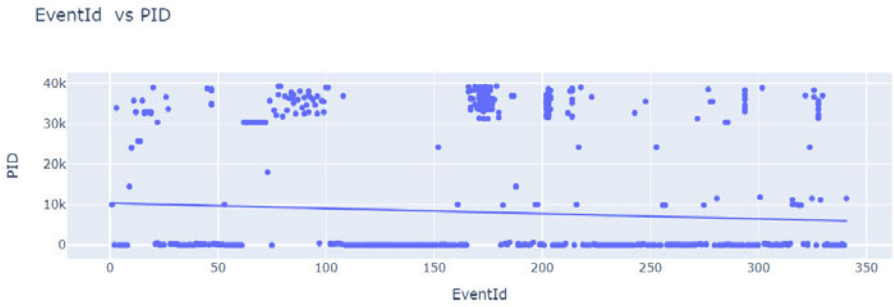


Figure 5.8.129: EventId Vs PID Scatter Plot

A correlation matrix amongst these columns is also provided in Figure 5.8.130. On the other hand we used word cloud to check the words included in component as it is categorical as shown in Figure 5.8.131. However, bar charts of EventId and PID can be seen in Figures 5.8.132 and 5.8.133. Both charts provide an illustration of events and processes values based on row numbers.

Figure 5.8.130: EventId & PID Correlation

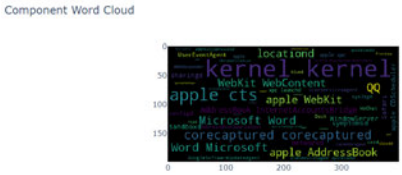


Figure 5.8.131: Component Word Cloud

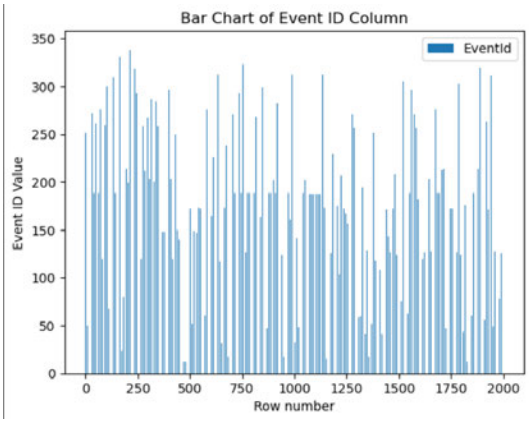


Figure 5.8.132: Event ID Bar Chart

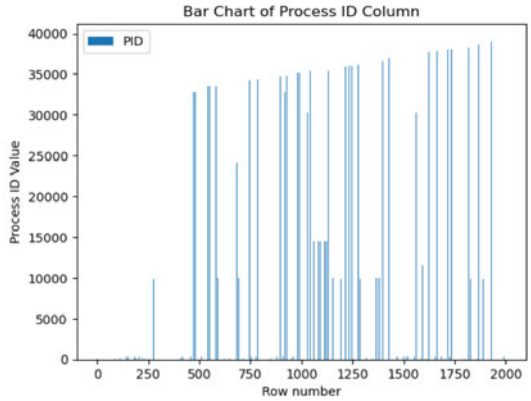


Figure 5.8.133: Process ID Bar Chart

5.8.2.2 Models Selection

For these logs we have used Decision Tree, Logistic Regression and Ridge Classifier models for training, testing and predicting our selected target which is component. Listing 5.8.18 depicts the code used for running the selected algorithms.

Listing 5.8.18: Mac Logs Models Code

```
import numpy as np
import pandas as pd

from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier # Chosen model
from sklearn.metrics import accuracy_score, classification_report # For
     evaluation such as classification report

# Loading dataset

data = pd.read_csv('logs/new_data.csv')

# Handle missing values if any

data = data.dropna()

# Dropping unwanted features columns

data = data.drop('Time', axis=1)
data = data.drop('User', axis=1)

data

# Running a loop of value counts to distinguish unique values

for c in data.columns:
    print("--- %s ---" % c)
    unique_values = data[c].unique()
    for value in unique_values:
        print(value)
    print("\n")

# encoding categorical column

le = LabelEncoder()
data['Component'] = le.fit_transform(data['Component'])

data

# Decision Tree Classifier Section

# Import scikitlearn module for the model DecisionTreeClassifier

from sklearn.tree import DecisionTreeClassifier
from sklearn.model_selection import train_test_split
```

```
46 from sklearn.metrics import accuracy_score
47
48 # Split the dataset into features (X) and target variable (y)
49
50 X = data[['EventId', 'PID']] # Features names
51 y = data['Component'] # Target variable (y)
52
53 # Split the data into training and testing sets
54
55 X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
       random_state=42)
56
57 # Create and train the model
58
59 model = DecisionTreeClassifier() # Chosen model
60 model.fit(X_train, y_train)
61
62 y_pred = model.predict(X_test)
63
64 # Evaluate the model
65
66 accuracy = accuracy_score(y_test, y_pred)
67
68 print(f'Accuracy: {accuracy}')
69
70 # Print the classification report
71
72 class_report = classification_report(y_test, y_pred)
73 print("Classification Report:")
74 print(class_report)
75
76 # Assume X_train has the same columns as your feature names
77
78 feature_columns = X_train.columns
79
80 # Create a DataFrame with the new data and use the same column names
81
82 new_data_df = pd.DataFrame([[252, 0]], columns=feature_columns)
83
84 # Make predictions
85
86 prediction = model.predict(new_data_df)
87
88 print(f'The predicted value for the specific cell is: {prediction}')
89
90 # Logistic Regression Section
91
92 # Import scikitlearn module for the model Linear Regression
93
94 from sklearn.linear_model import LogisticRegression
95
96 # Split the dataset into features (X) and target variable (y)
97
98 X = data[['EventId', 'PID']] # Features names
99 y = data['Component'] # Target variable (y)
100
```

```
# Split the data into training and testing sets

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
    random_state=42)

# Create and train the model

model = LogisticRegression() # Chosen model
model.fit(X_train, y_train)

y_pred = model.predict(X_test)

# Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

print(f'Accuracy: {accuracy}')

# Print the classification report

class_report = classification_report(y_test, y_pred)
print("Classification Report:")
print(class_report)

# Assume X_train has the same columns as your feature names

feature_columns = X_train.columns

# Create a DataFrame with the new data and use the same column names

new_data_df = pd.DataFrame([[323, 43]], columns=feature_columns)

# Make predictions

prediction = model.predict(new_data_df)

print(f'The predicted value for the specific cell is: {prediction}')

# Ridge Classifier Section

from sklearn.linear_model import RidgeClassifier

# Split the dataset into features (X) and target variable (y)

X = data[['EventId', 'PID']] # Features names
y = data['Component'] # Target variable (y)

# Split the data into training and testing sets

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
    random_state=42)

# Create and train the model

model = RidgeClassifier() # Chosen model
model.fit(X_train, y_train)
```

```
155
156 y_pred = model.predict(X_test)
157
158 # Evaluate the model
159
160 accuracy = accuracy_score(y_test, y_pred)
161
162 print(f'Accuracy: {accuracy}')
163
164 # Print the classification report
165
166 class_report = classification_report(y_test, y_pred)
167 print("Classification Report:")
168 print(class_report)
169
170 # Assume X_train has the same columns as your feature names
171
172 feature_columns = X_train.columns
173
174 # Create a DataFrame with the new data and use the same column names
175
176 new_data_df = pd.DataFrame([[323, 43]], columns=feature_columns)
177
178 # Make predictions
179
180 prediction = model.predict(new_data_df)
181
182 print(f'The predicted value for the specific cell is: {prediction}')
```

5.8.2.3 Evaluation

In EDA for Mac Logs we applied feature engineering to the original dataset then saved it into new dataset. Hence, the new_data is used to train our model with. To start with we imported the required libraries for models and dropped the unneeded columns. Figure 5.8.134 is an illustration of these steps.

	Component	PID	EventId
0	kernel	0	252
1	com.apple.CDScheduler	43	323
2	QQ	10018	216
3	kernel	0	128
4	kernel	0	124
...	...	...	...
1995	kernel	0	142
1996	kernel	0	331
1997	kernel	0	120
1998	kernel	0	338
1999	kernel	0	121

2000 rows × 3 columns

Figure 5.8.134: Mac Logs Models Data

Also, our component column is categorical and to convert it to numerical we used encoding approach. For example, Figure 5.8.135 shows the kernel value encoded into 47.

	Component	PID	EventId
0	47	0	252
1	31	43	323
2	16	10018	216
3	47	0	128
4	47	0	124
...	...	...	...
1995	47	0	142
1996	47	0	331
1997	47	0	120
1998	47	0	338
1999	47	0	121

2000 rows × 3 columns

Figure 5.8.135: Encoded Component

For our storytelling, we have chosen component column as our target dependent variable while PID and EventId are the features that are our independent variables. The accuracy and classification report for Decision Tree are shown in Figures 5.8.136 - 5.8.138.

```
y_pred = model.predict(X_test)

# Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

print(f'Accuracy: {accuracy}')
```

```
Accuracy: 0.9825
```

Figure 5.8.136: MacLogs DT Accuracy

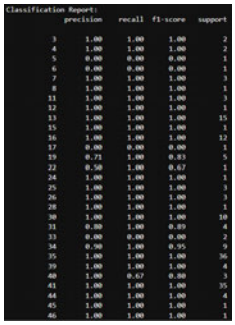


Figure 5.8.137: Mac Logs DT Classification Report I

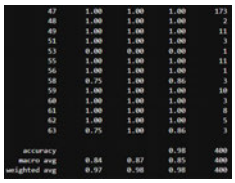


Figure 5.8.138: Mac Logs DT Classification Report II

Figures 5.8.139 and 5.8.140 are the accuracy scores for Logistic Regression and Ridge Classifier.

Figure 5.8.139: MacLogs LR Accuracy

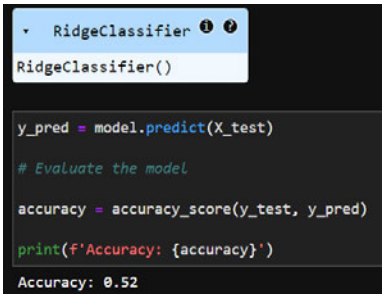


Figure 5.8.140: MacLogs RC Accuracy

As a result, an analyst can distinguish of what processes and events are carried out on a specific component. For instance, predictions can provide details of what activities are likely to be carried out on a component. We split our data into 80% training and 20% testing and achieved an accuracy of 0.98 for Decision Tree whilst both Logistic Regression and Ridge Classifier achieved 0.52 as shown in below table 5.8.5 and Figure 5.8.141.

Table 5.8.5: Mac Logs Algorithms Accuracy

Algorithm	**Accuracy**
Decision Tree	0.98
Logistic Regression	0.52
Ridge Classifier	0.52

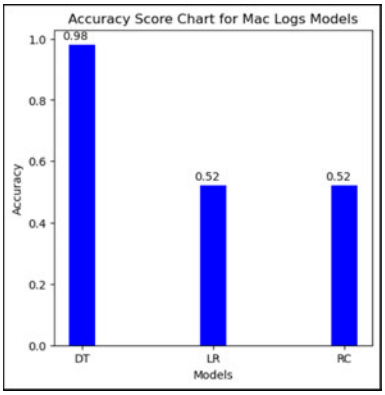


Figure 5.8.141: Mac Logs Models Accuracies

Accordingly, an analyst can also make prediction on specific value where

we have improved our model by adding the following as shown in Figure 5.8.142. For instance, if you pass a value of 252 for eventId feature and 0 to process Id feature then the outcome will be in 47 component value which is related to a kernel based on the encoded labels that we have carried out in new data preprocessing steps.

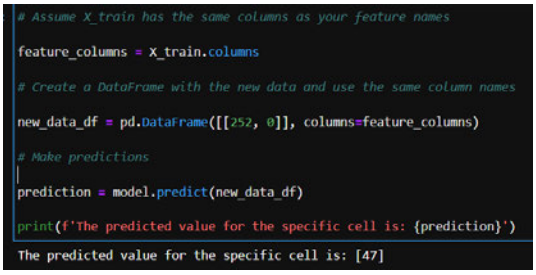


Figure 5.8.142: Mac Logs Value Prediction

5.8.3 Linux Logs Model

5.8.3.1 Exploratory Data Analysis (EDA)

Another testing is carried out on Linux logs sample. Firstly, the required libraries are imported and data preparing is carried out. listing 5.8.19 is the code that is used for analysing the Linux logs dataset.

Listing 5.8.19: Linux Logs Data Analysis

```
# Importing the required libraries

import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# reading data from csv file

dataFrame = pd.read_csv("logs\Linux_Logs.csv")

dataFrame

# data information

dataFrame.info()

# data stats

dataFrame.describe()
```

```
21
22  # To check if the dataset has null values
23
24  dataFrame.isna().sum()
25
26  # To check if there is any duplicate rows
27
28  dataFrame.duplicated().sum()
29
30  # Running a loop of value counts to distinguish unique values
31
32  for c in dataFrame.columns:
33      print ("--- %s ---" % c)
34      print (dataFrame[c].value_counts())
35
36  # Dropping noisy data from the dataset based on uniqueness
37  # PID has missing values. Hence it is dropped
38
39  dataFrame.drop(['PID','EventTemplate'], axis=1, inplace=True)
40  dataFrame
41
42  # As Event Id column has letter E at the start of each cell, I will remove it
        then convert the
43  # whole column to integer for more analysis and prediction
44
45  dataFrame['EventId'] = dataFrame['EventId'].str[1:]
46
47  dataFrame['EventId'] = dataFrame['EventId'].astype(int)
48
49  dataFrame
50
51  # Month Category column is mapped into 0 and 1 values as we only have 2 months
        values (June:6, July:7)
52
53  dataFrame['Month'] = dataFrame['Month'].map({'Jun': 6, 'Jul': 7})
54  dataFrame
55
56  # Level Category column has only one value combo so mapped into 0
57
58  dataFrame['Level'] = dataFrame['Level'].map({'combo': 0})
59  dataFrame
60
61  # Replacing date column name to day as it has the number of days only
62
63  dataFrame.rename(columns={'Date': 'Day'}, inplace=True)
64  dataFrame
```

The following screenshots are the output of the above code. Figure 5.8.143 depicts the linux dataset.

	LineId	Month	Date	Time	Level	Component	PID	Content	EventId	EventTemplate
0	1	Jun	14	15:16:01	combo	sshd(pam_unix)	19939.0	authentication failure; logname= uid=0 euid=0 ...	E16	authentication failure; logname= uid=0 euid=0 ...
1	2	Jun	14	15:16:02	combo	sshd(pam_unix)	19937.0	check pass; user unknown	E27	check pass; user unknown
2	3	Jun	14	15:16:02	combo	sshd(pam_unix)	19937.0	authentication failure; logname= uid=0 euid=0 ...	E16	authentication failure; logname= uid=0 euid=0 ...
3	4	Jun	15	02:04:59	combo	sshd(pam_unix)	20882.0	authentication failure; logname= uid=0 euid=0 ...	E18	authentication failure; logname= uid=0 euid=0 ...
4	5	Jun	15	02:04:59	combo	sshd(pam_unix)	20884.0	authentication failure; logname= uid=0 euid=0 ...	E18	authentication failure; logname= uid=0 euid=0 ...
...	...	...	...	...	...	...	...	...	...	...
1995	1996	Jul	27	14:41:59	combo	kernel	NaN	pci_hotplug: PCI Hot Plug PCI Core version: 0.5	E83	pci_hotplug: PCI Hot Plug PCI Core version: <*>...
1996	1997	Jul	27	14:42:00	combo	kernel	NaN	isapnp: Scanning for PnP cards...	E60	isapnp: Scanning for PnP cards...
1997	1998	Jul	27	14:42:00	combo	kernel	NaN	isapnp: No Plug & Play device found	E59	isapnp: No Plug & Play device found
1998	1999	Jul	27	14:42:00	combo	kernel	NaN	Real Time Clock Driver v1.12	E87	Real Time Clock Driver v<*>.<*>
1999	2000	Jul	27	14:42:00	combo	kernel	NaN	Linux agpgart interface v0.100 (c) Dave Jones	E66	Linux agpgart interface v<*>.<*> (c) Dave Jones

2000 rows × 10 columns

Figure 5.8.143: Linux Logs Dataset

Figures 5.8.144 - 5.8.146 are illustration of the dataset information, numerical columns statistics and if there is any null values.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 2000 entries, 0 to 1999
Data columns (total 10 columns):
 #   Column         Non-Null Count  Dtype  
---  ------         --------------  -----  
 0   LineId         2000 non-null   int64  
 1   Month          2000 non-null   object 
 2   Date           2000 non-null   int64  
 3   Time           2000 non-null   object 
 4   Level          2000 non-null   object 
 5   Component      2000 non-null   object 
 6   PID            1849 non-null   float64
 7   Content        2000 non-null   object 
 8   EventId        2000 non-null   object 
 9   EventTemplate  2000 non-null   object 
dtypes: float64(1), int64(2), object(7)
memory usage: 156.4+ KB
```

Figure 5.8.144: Linux Logs Information

	LineId	Date	PID
count	2000.000000	2000.000000	1849.000000
mean	1000.500000	17.015000	19813.574365
std	577.494589	8.484502	8593.584577
min	1.000000	1.000000	363.000000
25%	500.750000	10.000000	13327.000000
50%	1000.500000	17.000000	22189.000000
75%	1500.250000	25.000000	25548.000000
max	2000.000000	30.000000	32608.000000

Figure 5.8.145: Linux Logs Numerical Columns Statistics

PID and EventTemplate columns are dropped where PID has null values and EventTemplate has a lot of unnecessary noisy data. We have also removed the letter 'E' from the values of event id column then converted it to numerical type for prediction. The month column has only two values Jun and Jul in categorical format. Hence, they are converted to numerical

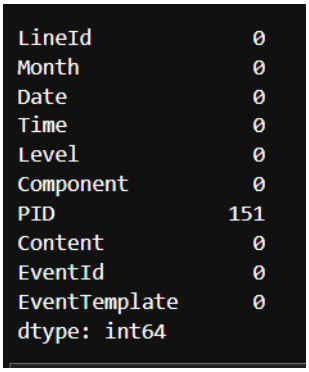
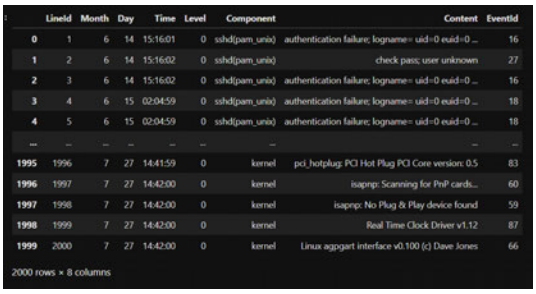


Figure 5.8.146: Linux Logs Null Values

format with new mapped values of 6 and 7. Date column has values of days numbers so the date column name is changed to day instead. Figure 5.8.147 below shows the carried out preparations.



	LineId	Month	Day	Time	Level	Component	Content	EventId
0	1	6	14	15:16:01	0	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	16
1	2	6	14	15:16:02	0	sshd(pam_unix)	check pass; user unknown	27
2	3	6	14	15:16:02	0	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	16
3	4	6	15	02:04:59	0	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	18
4	5	6	15	02:04:59	0	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	18
...	...	...	...	...	...	...	...	...
1995	1996	7	27	14:41:59	0	kernel	pci_hotplug: PCI Hot Plug PCI Core version: 0.5	83
1996	1997	7	27	14:42:00	0	kernel	isapnp: Scanning for PnP cards...	60
1997	1998	7	27	14:42:00	0	kernel	isapnp: No Plug & Play device found	59
1998	1999	7	27	14:42:00	0	kernel	Real Time Clock Driver v1.12	87
1999	2000	7	27	14:42:00	0	kernel	Linux agpgart interface v0.100 (c) Dave Jones	66

2000 rows × 8 columns

Figure 5.8.147: Linux dataset Preparation

Listing 5.8.20 is the code for printing out the word clouds for component and content columns as they have categorical values as shown in Figures 5.8.148 and 5.8.149. A scatter plot is also added to analyse any specific event id with its time, component and content of the selected event id. Lastly, the prepared dataset is saved into a new file to be used for training our model.

Listing 5.8.20: Linux Logs Data Analysis Charts

```
# World cloud figure for component column

import plotly.express as px
from wordcloud import WordCloud

tasks = ' '.join(dataFrame['Component'].astype(str))
```

```
wordcloud = WordCloud().generate(tasks)

fig = px.imshow(wordcloud, title='Component Word Cloud')
fig.show()

# World cloud figure for content column

import plotly.express as px
from wordcloud import WordCloud

tasks = ' '.join(dataFrame['Content'].astype(str))
wordcloud = WordCloud().generate(tasks)

fig = px.imshow(wordcloud, title='Content Word Cloud')
fig.show()

# Scatter plot for events Ids against Month and Day

import plotly.express as px

# Specify the x-value you want to include
specific_x_value = 30

# Filter the DataFrame based on the specific x-value
filtered_dataFrame = dataFrame[dataFrame['EventId'] == specific_x_value]

fig = px.scatter(filtered_dataFrame,x='EventId', y=['Component','Content','Time
    '], title='Event ID vs. Component & Content')

fig.show()

# Save the data into a new dataset after preparing it

dataFrame.to_csv('logs/new_data.csv', index=False)
```

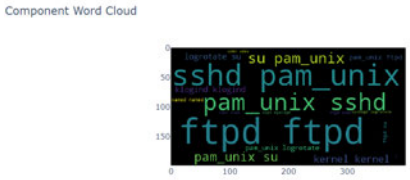


Figure 5.8.148: Linux Component Word Cloud

Figure 5.8.149: Linux Content Word Cloud

Figure 5.8.150 is the scatter plot where we can see that an event id of value of 30 is shown with its time, component and content.

Figure 5.8.150: Linux EventId-Component-Content Scatter

5.8.3.2 Models Selection

For linux logs we tested the prepared data with 3 different algorithms including; Decision Tree, Logistic Regression and Ridge Classifier. Listing 5.8.21 is the code used for these models.

Listing 5.8.21: Linux Logs Models

```
# Importing required libraries

import numpy as np
import pandas as pd
import matplotlib.pyplot as plt

from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score, classification_report # For
    evaluation such as classification report

# Loading dataset

df = pd.read_csv('logs/new_data.csv')
df

# Preparing data by Dropping unwanted features columns

df = df.drop('LineId', axis=1)
df = df.drop('Level', axis=1)
```

```
df = df.drop('Time', axis=1)

df

# encoding categorical column

le = LabelEncoder()
df['Component'] = le.fit_transform(df['Component'])
df['Content'] = le.fit_transform(df['Content'])

df

# Decision Tree (DT) Section

# Import scikitlearn module for the model DecisionTreeClassifier

from sklearn.tree import DecisionTreeClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# Split the dataset into features (X) and target variable (y)

X = df[['Month', 'Day','Component','Content']] # Features names
y = df['EventId'] # Target variable (y)

# Split the data into training and testing sets

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
    random_state=42)

# Create and train the model

# Example for classification
clf = DecisionTreeClassifier(random_state=42)
clf.fit(X_train, y_train)

y_pred = clf.predict(X_test) # For classification

accuracy = accuracy_score(y_test, y_pred)
print(f'Accuracy: {accuracy}')

# Print the classification report

class_report = classification_report(y_test, y_pred, zero_division=1)
print("Classification Report:")
print(class_report)

# Assume X_train has the same columns as features names

feature_columns = X_train.columns

# Creating a DataFrame with the new data and using the same column names

new_data_df = pd.DataFrame([[6, 14, 23, 104]], columns=feature_columns)

# Make predictions
```

```
75
76  prediction = clf.predict(new_data_df)
77
78  print(f'The predicted value for the specific cell is: {prediction}')
79
80  # Logistic Regression (LR) Section
81
82  # Import scikitlearn module for the model Linear Regression
83
84  from sklearn.linear_model import LogisticRegression
85
86  # Split the dataset into features (X) and target variable (y)
87
88  X = df[['Month', 'Day','Component','Content']] # Features names
89  y = df['EventId'] # Target variable (y)
90
91  # Split the data into training and testing sets
92
93  X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
        random_state=42)
94
95  # Create and train the model
96
97  model = LogisticRegression() # Chosen model
98  model.fit(X_train, y_train)
99
100 y_pred = model.predict(X_test)
101
102 # Evaluate the model
103
104 accuracy = accuracy_score(y_test, y_pred)
105
106 print(f'Accuracy: {accuracy}')
107
108 # Print the classification report
109
110 class_report = classification_report(y_test, y_pred, zero_division=1)
111 print("Classification Report:")
112 print(class_report)
113
114 # Assume X_train has the same columns as features names
115
116 feature_columns = X_train.columns
117
118 # Creating a DataFrame with the new data and using the same column names
119
120 new_data_df = pd.DataFrame([[6, 14, 23, 104]], columns=feature_columns)
121
122 # Make predictions
123
124 prediction = model.predict(new_data_df)
125
126 print(f'The predicted value for the specific cell is: {prediction}')
127
128 # Ridge Classifier (RC) Section
129
```

```
from sklearn.linear_model import RidgeClassifier

# Split the dataset into features (X) and target variable (y)

X = df[['Month', 'Day','Component','Content']] # Features names
y = df['EventId'] # Target variable (y)

# Split the data into training and testing sets

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
    random_state=42)

# Create and train the model

model = RidgeClassifier() # Chosen model
model.fit(X_train, y_train)

y_pred = model.predict(X_test)

# Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

print(f'Accuracy: {accuracy}')

# Print the classification report

class_report = classification_report(y_test, y_pred, zero_division=1)
print("Classification Report:")
print(class_report)

# Assume X_train has the same columns as features names

feature_columns = X_train.columns

# Creating a DataFrame with the new data and using the same column names

new_data_df = pd.DataFrame([[6, 14, 23, 104]], columns=feature_columns)

# Make predictions

prediction = model.predict(new_data_df)

print(f'The predicted value for the specific cell is: {prediction}')
```

5.8.3.3 Evaluation

To further prepare our data we dropped lineId, level and time columns as shown in Figure 5.8.151

	Month	Day	Component	Content	EventId
0	6	14	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	16
1	6	14	sshd(pam_unix)	check pass; user unknown	27
2	6	14	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	16
3	6	15	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	18
4	6	15	sshd(pam_unix)	authentication failure; logname= uid=0 euid=0 ...	18
...	...	...	...	...	...
1995	7	27	kernel	pci_hotplug: PCI Hot Plug PCI Core version: 0.5	83
1996	7	27	kernel	isapnp: Scanning for PnP cards...	60
1997	7	27	kernel	isapnp: No Plug & Play device found	59
1998	7	27	kernel	Real Time Clock Driver v1.12	87
1999	7	27	kernel	Linux agpgart interface v0.100 (c) Dave Jones	66

2000 rows × 5 columns

Figure 5.8.151: Linux Dropped Columns for Models

The component and content columns are categorical. Hence, labels encoder approach is used where Figure 5.8.152 shows that the dataset is now ready for training and testing.

	Month	Day	Component	Content	EventId
0	6	14	23	104	16
1	6	14	23	130	27
2	6	14	23	104	16
3	6	15	23	107	18
4	6	15	23	107	18
...	...	...	...	...	...
1995	7	27	9	267	83
1996	7	27	9	260	60
1997	7	27	9	259	59
1998	7	27	9	63	87
1999	7	27	9	47	66

2000 rows × 5 columns

Figure 5.8.152: Finilised linux Dataset for testing and training

For all of the 3 algorithms we split the data into 80% for training and 20% for testing. These values can be changed on the basis of requirements. Comparing to other solutions of windows and mac logs we have used 4 independent variables features in this sample which are 'Month', 'Day','Component','Content' and one dependent variable which is our target 'EventId'.

The highest accuracy achieved is 0.9425 when tested with Decision Tree as shown in Figure 5.8.153.

```
y_pred = clf.predict(X_test)  # For classification

accuracy = accuracy_score(y_test, y_pred)
print(f'Accuracy: {accuracy}')

Accuracy: 0.9425
```

Figure 5.8.153: DT Accuracy

However, Figures 5.8.154 and 5.8.155 are the classification report for Decision Tree.

```
Classification Report:
              precision    recall  f1-score   support

           3       0.00      1.00      0.00         0
           4       1.00      0.00      0.00         1
           8       1.00      1.00      1.00        11
          11       0.00      1.00      0.00         0
          12       1.00      0.00      0.00         1
          13       1.00      1.00      1.00         2
          14       1.00      1.00      1.00         4
          15       0.00      1.00      0.00         0
          16       1.00      1.00      1.00        23
          17       1.00      1.00      1.00         4
          18       1.00      1.00      1.00        63
          20       0.33      1.00      0.50         1
          21       1.00      0.00      0.00         1
          22       1.00      0.00      0.00         1
          23       1.00      0.00      0.00         1
          27       1.00      1.00      1.00        20
          29       1.00      1.00      1.00       187
          31       1.00      0.00      0.00         1
          36       1.00      1.00      1.00         2
          37       1.00      1.00      1.00         1
          38       1.00      1.00      1.00         2
          41       1.00      0.00      0.00         1
          42       0.00      1.00      0.00         0
          43       0.00      1.00      0.00         0
          44       1.00      0.00      0.00         1
          47       1.00      1.00      1.00         1
          49       0.00      1.00      0.00         0
          50       0.00      1.00      0.00         0
          52       1.00      0.00      0.00         1
          54       1.00      0.00      0.00         1
          58       1.00      0.00      0.00         1
          59       0.00      1.00      0.00         0
```

Figure 5.8.154: Linux DT Classification Report I

```
          61       1.00      1.00      1.00         6
          62       1.00      0.00      0.00         1
          67       0.00      1.00      0.00         0
          69       1.00      0.00      0.00         1
          72       0.00      1.00      0.00         0
          75       1.00      1.00      1.00         5
          77       0.00      1.00      0.00         0
          78       1.00      0.00      0.00         1
          81       1.00      0.00      0.00         1
          82       0.00      1.00      0.00         0
          85       1.00      0.00      0.00         1
          89       0.50      1.00      0.67         1
          91       0.00      1.00      0.00         0
          92       1.00      0.00      0.00         1
          94       1.00      0.00      0.00         1
          95       0.00      1.00      0.00         0
         101       1.00      1.00      1.00        24
         102       1.00      1.00      1.00        20
         104       0.00      1.00      0.00         0
         105       0.00      1.00      0.00         0
         108       0.00      1.00      0.00         0
         109       1.00      0.00      0.00         1
         112       1.00      0.00      0.00         1
         113       1.00      0.00      0.00         1
         114       1.00      0.00      0.00         1
         115       0.00      1.00      0.00         0
         116       0.00      1.00      0.00         0
         118       1.00      0.00      0.00         1

    accuracy                           0.94       400
   macro avg       0.66      0.62      0.29       400
weighted avg       1.00      0.94      0.94       400
```

Figure 5.8.155: Linux DT Classification Report II

Logistic Regression achieved 0.7275 as shown in Figure 5.8.156 whilst Ridge Classifier achieved 0.675 as shown in Figure 5.8.157.

```
y_pred = model.predict(X_test)

# Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

print(f'Accuracy: {accuracy}')
```

```
Accuracy: 0.7275
```

Figure 5.8.156: Linux LR Accuracy

```
y_pred = model.predict(X_test)

# Evaluate the model

accuracy = accuracy_score(y_test, y_pred)

print(f'Accuracy: {accuracy}')
```

```
Accuracy: 0.675
```

Figure 5.8.157: Linux RC Accuracy

For further prediction, a testing of a specific cell is carried out. Figure 5.8.158 below shows an accurate prediction for Decision Tree when assigning the features of values [6, 14, 23, 104]. They are associated with value 16 which is an event 16. However, for LR and RC the results were incorrect. Hence, their accuracies were lower than DT.

```
# Assume X_train has the same columns as features names
feature_columns = X_train.columns

# Creating a DataFrame with the new data and using the same column names
new_data_df = pd.DataFrame([[6, 14, 23, 104]], columns=feature_columns)

# Make predictions
prediction = model.predict(new_data_df)

print(f'The predicted value for the specific cell is: {prediction}')
```

```
The predicted value for the specific cell is: [16]
```

Figure 5.8.158: Linux Cell Prediction

Table 5.8.6 and Figure 5.8.159 are illustrations of the comparison between the selected algorithms accuracies.

Table 5.8.6: Linux Logs Algorithms Accuracy

Algorithm	**Accuracy**
Decision Tree	0.9425
Logistic Regression	0.7275
Ridge Classifier	0.675

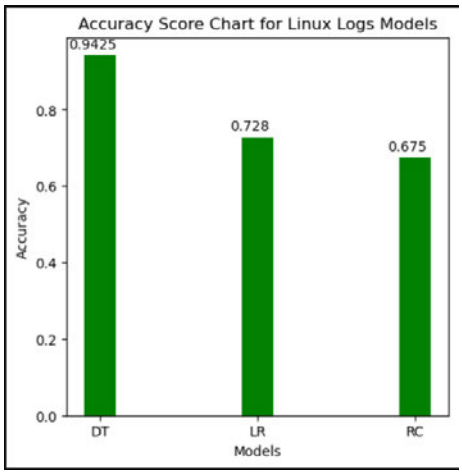


Figure 5.8.159: Linux Logs Models Accuracies

5.9 Feedback and Analysis

Predicting the occurrence of a log based on its specific pattern can be effective. Organisations can minimise the risk of wasting time on false positives and focusing more on essential genuine logs. An automation model can be implemented in any scenario that include dataset. Few changes are required such as the name of the data, target attribute and what organisations are looking to achieve from running the model.

To further evaluate our automation approach, the researcher presented the models to various participants. Insights and feedback are gathered of such an automation model for SOC environment. More interviews are carried out with participants for the feedback which is different from the ones

that are completed to gather the challenges. Hence, participants in this section are referred to as P1, P2, P3 - P10. Various roles within IT and cyber security are the targeted demographic in order to gain wider insights. The dates of these interviews took place between November 2023 & January 2024 and each interview lasted between 30 - 45 minutes.

Table 5.9.7 is mentioned in section 3.3.1 but added again as a duplicated reminder of the second round of interviews.

Table 5.9.7: Participants of Model Feedback

Participant ID	**Role**	**Interview Method**
P1	Cyber Security Consultant	MS Teams
P2	Cyber Security Consultant	MS Teams
P3	Software Developer	Google Meet
P4	Software Sales	Google Meet
P5	Software Product Leader	Google Meet
P6	Cyber Security Consultant	MS Teams
P7	Penetration Tester	MS Teams
P8	Information Security Analyst	MS Teams
P9	Software Engineer Analyst	MS Teams
P10	IT Analyst	In Person

5.9.1 Participants

P1

P1 is a cyber security consultant works for a large size company of up to 750,000 employees. When presented with the model and asked of how can the model deal with logs to improve the efficiency of Security Analysts (Level-1 and 2) job?

The response was as follow:

"I think the most important thing is it reduces time. So, it reduces the time an analyst has to put on a particular event that comes in. It allows them to move on to the next event pretty quickly. I think again it helps out Level 2 analyst as well. What will happen is you get the information from level one in time or the time they've spent on that particular event is speed

up. It means that the vast amount of data they can hand over to level 2 is much clearer. It is able to help them much quicker time period as well".

P1 also stated that the model could be implemented across the whole board not only for windows security logs for example. Which in turn assists in speeding up the time L1 and L2 analysts have to put in. In terms of the impact of such a model on an organisation, there is a massive turnover within SOC where individuals changing places to earn more money. Therefore, participant stated:

"I feel that with this implementation in L1 SOC if you've got a team of five, you could replace one analyst. So, it becomes 4 because the time it speeds everything up. It allows those 4 to then focus on other areas. Companies can save money by not employing as many analysts and they can invest that money into other areas of the business".

A suggestion for such an implementation is to apply it then provide the board management. For instance, the stats of the model including the decreased time spent by analysts and automated activities. This can add a lot of value to the business as P1 concluded.

P2

P2 is a cyber security consultant works for small sized company. The model can be effective for level 1 security analysts in terms of whether an event needs to be escalated to higher level or not participant added. If an analyst is looking for hundreds of logs each day, then he/she will be able to prioritise more efficiently what it needs to go up to level 2 and level 3. The same would work as well for other levels. As a result, such a model assists in speeding processes rather than manually going through and analyse each individual alert. Hence, you can directly jump straight to the point to figure out more in-depth information if needed. P2 also added the following when asked if similar model can be used for other activities other than windows security logs:

"Yeah, definitely it could be used for other stuff. Obviously now cloud is becoming a really big thing. So, there'll be ways to sort of use this with Azure and AWS errors and logs that come up".

Therefore, implementing such a model could be used as plugin for other platforms. In contrast, P2 raised a concern in regards of the impact of such a model on organisations, the following is mentioned:

"I think it may have an impact on the beginning of trying to implement it. How are you going to incorporate it into a new organisation, whether it is a small, medium or large. You might have to scale it differently?"

Businesses could be exposed to difficulties at the beginning in terms of troubleshooting any raised errors by the model. Hence, educating employees is required of any new implemented processes. For example, if an event ID is updated or new ones occurred such as new false positives then employees should be able to adapt to the change by updating the model accordingly. Suggestions are raised by P2 to further enhance the model. For instance, linking events with their severities. By having more graphs to illustrates the risk level of each event. Thus, SOC analysts will be able to distinguish the severity level of such an event at quicker basis.

P3

P3 is a software developer who works for a medium sized company. In terms of applying such a model, it increases the productivity and efficiency of analysts whether they are tier 1 or 2 as P3 added. For instance, unnecessary information is scrapped by using techniques including data preprocessing and feature engineering. As well, it can reduce time spent on non-critical events and focus more on other serious logs. Hence, productivity can be boosted by applying such an automation approach. Exploratory data analysis and using such graphs also support analysts in understanding the nature of events to prepare for an action. When asked if a similar model can be used for analysing other security logs or other activities, P3 added the following:

"We use a software for scrapping web URL. With a similar implemented model, it can be integrated as plugin or used separately to only picking up specific data which reduce a lot of time for us. As well, adding a layer of support for our activities such as analysing page titles, finding broken URLs and metadata".

In contrast, applying such a model can also pose various difficulties in terms of newly implemented service. It requires to be monitored and train

employees on how to maintain it to gather accurate and required results. P3 concluded the interview by highlighting the importance of starting to apply similar automation in their organisation to speed up their daily tasks plus enhancing their productivity. As well, suggestions are added to for the model to be more dynamic and compatible with different types of operating systems.

P4

Software sales representative who works for large sized company is participant 4 who is also interviewed to gather feedback on the automation approach model.

When working with clients, such automation features would be highly valuable, especially in terms of time-saving. The goal would be to allow the user to save a significant amount of time by not getting distracted with wrong data P4 added. By providing analysts with more time back due to the automated process the quality and efficiency of analysts tasks in tiers 1 and 2 is increased. Accordingly, participant added that they would consider the model for their own use. As they often have to deal with duplicated data that can be a distraction. Hence, the automation approach can be applied for different scenarios and processes. In terms of specifying any impact on organisations P4 added the following:

Such a model could definitely have a knock-on effect one the aforementioned stages. It would feed into it, dealing with the root cause issue would eliminate any false data getting into the system.

Suggestions are added in terms of how much time have analysts saved on average by applying the model. Also the different applicable use cases outcome for future amendments.

P5

P5 is an experienced software product leader for 10 years in leading software teams in large sized company. When asked on how the model will be used to improve the effectivity of SOC analyst job whether level 1 or level 3 analysts P5 added the following: once an approach is applied there will be a significant increase in productivity for tier 1 & 2 analysts' jobs. However, the concept is understandable but if a successful implementation of

such a model is achieved then there will be a big achievement in eliminating unnecessary manual tasks.

One of our products is software as a service (SaaS). Therefore, if one of our clients faced any particular problem related to bugs issues then we have to go through a lot of logs manually to discover any anomaly issue. Applying this model can also be used for searching through logs on our platform to discover bugs/issues. As a result, efficiency will increase and client's satisfaction can be achieved as P5 added.

There might be an impact on the organisation services for applying such a model on short term. But on long terms with the correct deployment plus the efficient training, the model can achieve a lot of things such as time and costs reduction. As a suggestion, P5 concluded the interview by adding if there can be a real time prediction. For example, to detect any upcoming or anomaly event based on the current system behaviour. However, this can be achieved by modifying the model and training it with organisation data.

P6

P6 is a cyber security managing consultant who works for large size company. When asked about the effectivity of such a model in improving tier 1 and 2 analysts' job. Participant added the following: when an analyst is at level one or level 2, they fall under the junior to mid part of their career. Therefore, they could be dealing with variety of tools, teams and a lot of types of alerts to distinguish suspicious behaviours and malicious activity. The key problem is no matter what SIEM tool they use, they all produce some degree of false positives. Nonetheless, the effort is not necessarily wasted but it's an effort that isn't contributing to detecting malicious activity and alerts. Hence, false positives take time away from other essential work. False positives can be tuned, not tune them out, but further reduce them. However, it takes additional time and effort and whilst it does optimise SIEM it does distract time away from the actual detection of key events. A model that can predict future events either a moderate or even high degree of accuracy would be really fantastic. It would allow from a training perspective security analyst to understand what a normal behaviour looks like and what a baseline looks like.

For example, if a user log can be seen, then a special login is performed because they're doing it remotely over an RDP session or similar remote

connection. Therefore, through this model an analyst can identify what standard behaviours looks like. In future if they see an event or a series of alarms relating to a user logging in, and a special login occurred. Then they look at that and compare it against the model to see if it's realistic, effectively and if it should be there or not. Over time, the model can be fed with data from that scene to not only help reduce false positives, but also to help train security analysts and specialists of Level 1 & 2 on what good and bad network behaviours look like. It would be interesting to see the opposite where the model can predict the least to be next and subject to some passing to get rid of impossible events. P6 also noted:

"By picking up the events that the model says are very unlikely to occur, but possible you could almost directly use that to detect and fill out alarms. If you detected something like a user logging in from multiple locations or performing multiple logins at different devices or similar. It's absolutely not likely and it wouldn't show up as likely. But if you are not only took the highest predictions from the model, but also took the lowest predictions, you could potentially identify real possible compromises. It is all around. I think it would be a really a massive improvement on what SIEM currently has, especially considering a lot of SIEMs proprietary".

For using such a model approach to detect and analyse other than windows, Linux and mac logs, participant stated that one of the powerful things about this approach that it does not relate to any particular type of product or technology stack. The same approach can be used on any type of logs. For example, I would immediately gravitate to sort of sys logs for full packet capture or something similar. Being able to use something like that to scrape network packets and then identify network packets following or likely protocols or even for your own custom logs within applications if you write them yourselves. It is a definitely a powerful solution because it does not lock you to one particular provider and you'd be able to use similar type of model for any type of logging.

In terms of model budget impact, P6 added that the actual implementation cost would be 0 due to the kind of open code. Thus, that immediately would make it very accessible. Obviously, a dedicated research and development team is required to use the tool, set it up and investigate it. From participant‘s opinion, for medium to large scale organisations, being able to allocate people to do research and development is already costed in. Therefore, a huge impact would not occur on budget in terms of outgoings from

it. In terms of organisational structure, it could significantly impact on roles available in SOC and how it functions. A lot of SOCs have analyst roles, engineer roles, but also instant response. A lot of threat intelligence and SIEM engineers or platform engineering role is specifically to be involved in the patching, deployment and rule set integration of SIEM. Applying such a model can continually improve the effectiveness of SIEM and reduce false positives. An organisation can have a team of dedicated platform engineers using something similar to reduce false positives. P6 also stated:

"In terms of deployment, you're going to encounter the same issues you would in any organisation as they are primarily quite slow and large. It takes time for things to be done, but generally, in terms of technical deployment aspects, you could pipe a large data set from something like logarithm or Splunk. You could always have that on a drive that can access and read from that data. Maybe a scheduled pull overnight or some kind of way of reading the data. I think that would cover deployment integration really into a SOC. I would probably have something like this running in a Demilitarised Zone (DMZ) in a SOC".

In terms of false positives and negatives impact, the overall would reduce false positives. You would be able to identify potential malicious activity and what events are most likely to come next. The model can be compared against what has been seen and validate if they align with the model. If a couple of events are very likely, then checking the model results and seeing if this occurrence has happened before and determining what sort of level of reliability or accuracy the model believes the result that event is likely to follow. While legal and policies impact, there would be no issues as the code itself using offline libraries and is not requesting any sort of web addresses. There's nothing to stop it from running it on air gaps environment and then at that point. It can also run on hardware that's approved for these security accreditations of SOC. In regards of security of infrastructure, the model would help massively to improve security of infrastructure. It could also be applied on tools like firewalls and syslog servers. It could be used for full packet capture as well and not only to predict security logs. You could also predict things alongside security logs and almost evidence that.

Model suggestions are raised in terms of seeing not only the highly probable events but also seeing the ones the model thinks are extremely unlikely. For instance, doing whatever within an environment at given point in time. If you ingest that dataset, you're going to sort of baseline a good normal

standard. A lot of logins at 9:00 o'clock in the morning and lots of log offs between 5-7. Then if a login or a behaviour at 3 in the morning is going to be extremely unlikely according to the model. Logon event at three in the morning followed by another event would be extremely unlikely because it wouldn't fit with the baseline. Identify and predict those types of events could be useful and used for staff training. Potentially, you could say this event is extremely unlikely to follow this event in the vast majority of circumstances. However, if it is occurred, then it can be associated with this type of malicious activity. Overall, P6 concluded by adding the following:

"I think it's a really interesting piece of software and I think it would be really useful inside of SOC and wider organisations".

P7

A cyber security penetration tester agree on the need of automation and is referred to as P7. Such an automation approach can be effective to detect not only malicious activities but also to distinguish between false positives and genuine activities as P7 stated.

Adding more, the model requires training with real dataset in order to retrieve the best out of it. For example, train it with as much logs Ids as possible and if a new event is occurred then it can also be added to the training phase.

The participant emphasised on the need of applying automation in a lot of activities to decrease the manual work and to focus more on other important tasks. However, applying such an automation model requires training, time and continuous revision as P7 concluded.

P8

A senior information security analyst is the role of P8 who works for medium sized company. According to participant, analysts will work more effectively and efficiently if such an automation approach is applied. For instance, data cleaning and pre-processing can help in decreasing duplicated records to focus more on genuine alerts.

P8 agrees on the need of automation in industry to reduce the number of false positives and to decrease the effort spent in manual tasks. Data

cleaning is required more than ever to start working on automation solutions. Predicting events can be more accurate after cleaning the dataset plus decreasing the number of false positives or negatives based on specific features that are identified previously.

However, such a model helps in reducing the time spent on manual analysis but it requires training and monitoring to achieve its goals successfully as concluded by participant.

P9

P9 is a Software Engineer Analyst in large sized company. The output of the model whether (Suspicious, Normal, Unclassified) event would help Security analysts. It would reduce time spent to monitor logs/events by moving from manual method of monitoring events/logs into more automated one based on well-known suspicious events as participant added.

When asked about considering such a model for analysing other security logs P9 added the following:

"I think it is crucial to use more automated tools that can prompts alerts as quickly as possible in case of suspicious events. However, since the model is untested, that would make it hard to recommend it at the moment to be the main source of filtering the events. I would suggest moving into test phase then verify phase then apply".

Participant also added that the impact of such a model on an organisation budget is split into three phases:

1. It will force the firm to dedicate a lot of time/resources to feed the patterns of suspicious events/logs into the model to allow it to discover it in the future.

2. It would be verifying that the pattern is reliable enough to classify the event, so it will be time/resource consuming as well.

3. Third phase would be implementing the model as the main source of detecting the suspicious events. In this phase, there would be noticeable saving in time/resource.

Another impact is mentioned in terms of reducing false positives or detecting false Negatives (classifying normal events as suspicious/Not detecting suspicious event/log) where undetected event could be disastrous since it could lead into money loss or reduce the confidence in an institution.

Overall, P9 stated that the model has a good potential. However, it has not been tested against real dataset that has real suspicious events/logs which is suggested by the participant.

P10

To conclude the overall evaluation, the last feedback is gathered from participant 10 who is an IT analyst works for large sized organisation. Accordingly the model can increase the efficiency of security analysts by allowing them to carry out there tasks in a more coherent manner. This shall give them more flexibility to narrow down searches when analysing for a particular event.

P10 also suggested that a similar model approach can be considered in other departments including different internal department within IT. Including service desk, management and the operational department which can be an extra automation layer to the overall IT within an organisation.

The impact of such a model shall be cost worthy initially. On the long run it would be beneficial as it shall enhance the productivity. This model shall gives more of a clear structure and be a valuable asset to security department. This is because the model does encompass a large security aspect for the running of a particular large organisation. It allows security principles to be set in place and policies giving substantial high-level of security infrastructure as P10 summarised.

5.9.2 Analysis

To further our findings, a statistical analysis is carried out based on the feedback gathered from participants. Figure 5.9.160 below illustrates the efficiency of such a model. For example, the time reduction is mentioned by all participants which is 26% out of the overall mentioned advantages of the model where it reduces time spent by analysts to locate a specific log. Meanwhile, the model also eliminates unnecessary manual tasks which

is 16% out of the overall scale. Thus, Figure 5.9.160 provides the statistics of how many times each efficiency element is mentioned by participants.

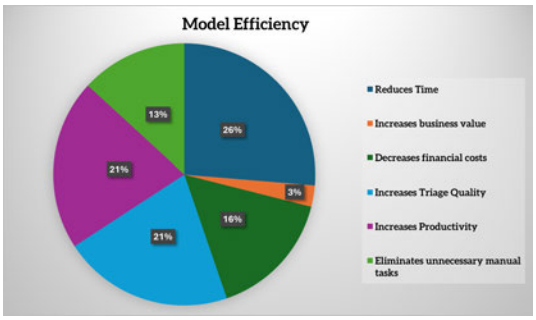


Figure 5.9.160: Model Efficiency

Figure 5.9.161 depicts the limits of the model that are added by participants. Accordingly, 10 participants added that it requires training and one added that it needs troubleshooting. Regular updates and short term negative impact are also mentioned.

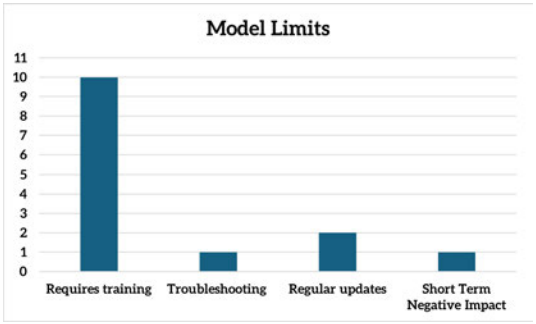


Figure 5.9.161: Model Limits

Also, model suggestions are mentioned by participants as follow:

- To provide stats to management.
- To provide severity level Stats.
- To be more dynamic.
- Operating systems Compatibility.
- Add it as a plugin for other tools.

- Provide stats in terms of average time saving.
- Apply it with different applicable use cases.
- Provide bugs Real Time Prediction.
- To be able to predict less likely events.
- Train it with different events codes.

All participants agreed that such an automation model can be implemented on different types of logs and apply it on different types of activities.

5.10 Grid Martix

Based on findings from evaluating the automation solutions. We have also created a Grid matrix that can be used to evaluate an automation model based on its performance and set parameters. Refer to below Figure 5.10.162 for the Matrix.

Criteria							
Detection Methods	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Signature Based	10						
Anomaly Based	10						
ML Based	10						
Data Sources	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Network Traffic	9						
Endpoints Data	9						
Logs	9						
Users Behaviours	9						
Detection Accuracy	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
TP	8						
FP	8						
TN	8						
FN	8						
Response Time	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Time to Detect	7						
Time to Respond	7						
Scalability	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Dataset Size Handling	6						
Number of Devices Involved	6						
Costs	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Initial Investment	5						
Ongoing Operations	5						
Integration	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Compatibility with Current Systems	4						
Reporting & Alerting	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Reporting Instruments	3						
Alerting Methods	3						
User Friendliness	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Required Training	2						
Ease of Use	2						
Customization	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Particular Threats Applying Ability	1						
Total Score	**Solution I**			**Solution II**		**Solution III**	

Figure 5.10.162: Grid Matrix

Organisations can evaluate the efficiency of threat detection automation based on below set of parameters or adding other features if required:

Detection Methods: either signature based, anomaly based or ML based.

Data Sources: include network traffic, endpoints data, logs or users' behaviours.

Detection Accuracy: such as true/false positive and true/false negative.

Response Time: time to detect and time to respond.

Scalability: dataset size handling and number of devices involved.

Costs: operations and investments costs.

Integration: compatibility with other current systems.

Reporting & alerting: tools and mechanisms for reports and alerts.

User Friendliness: the required training and ease of use.

Customisation: the ability to apply and tailor it to particular threats.

Each parameter or criteria is assigned a specific scale based on its value to the business. For example, detection methods can be assigned 10 as a scale where customisation might be assigned 8. Thus, due to the assigned value we can gather that detection methods criteria is more important than customisation. However, these values can be set based on organisations requirements.

Solutions ratings can be assigned numerical values based on their performance that is aligned with each criterion. For instance, values between 1-10 can be assigned to each solution to discover how well it performed. As well, the scale score for each criterion is calculated by multiplying the scale **(S)** for each criterion by the rating **(R)** of how well a solution is performed based on that specific criterion. Overall, the total score of how well a so-

lution is performed is extracted from adding up all the weighted scores for each criterion.

Accordingly, an equation can be written as follow:

$$\text{Scale Score (SS)} = S \times R \tag{1}$$

$$\text{Total Score (TS)} = \sum_{i=1}^{n} \text{SR}_i \tag{2}$$

Where **SRi** is equal to weighted score for criterion **i**. Refer to below example for more explanation:

For instance, if a response time criterion is given **7** as a scale and a solution is performed **6** for this specific criterion. Then the scale score would **42** as follow:

$$7 \times 6 = 42$$

.

However, the total score of how well a solution is performed would be adding **42** to all other scale scores.

The selection of parameters of the Grid-Matrix is essential for the construction and evaluation of automated solutions to optimise performance and accuracy. This method includes systematically exploring a predefined set of parameter combinations. This allows for comprehensive evaluation across multiple dimensions. Weights are assigned to different parameters to reflect their relative importance based on an organisation needs to influence a model's behavior. By carefully defining these weights, SOC team can prioritise key aspects of an automation solution system. For example speed, precision and robustness ultimately lead to a more effective and tailored automated solution. This approach ensures that the solution is finely tuned to meet specific objectives and operational requirements of a particular organisation.

Chapter Six

Conclusion

6 Conclusion

6.1 Introduction

This section concludes this thesis and contains identified limitations and recommendations for future research. The limitations include the constraints faced during the research whilst recommendations are proposed for future research direction.

6.2 Conclusion

This dissertation aimed to explore and address the challenges that SOC face by focusing more on the high number of logs. The research is carried out through an extensive review of the literature, an effective designed methodology and rigorous data analysis. Our understanding of SOC and its challenges are significantly enhanced due to this research contribution. The findings of this study suggest that organisations that are looking to establish SOC or they already have one need to be aware of the potential challenges that might occur. This will shed lights on the required solutions to overcome these implications that are gathered from our findings. The results also confirm the importance of the main challenges faced by SOC and how they impact on analysts? Plus, how to reduce the number of particular alerts such as false positives.

Accordingly, this study provides various remarkable contributions to the field of SOC:

Contribution 1: findings about the main challenges SOC analysts are currently facing are identified from industrial point of view plus linking them with a literature review from an academic point of view. This is an important factor which help in collaborating amongst industry and academia to share knowledge and develop solutions for any upcoming implications. Hence, one of our papers named assess the challenges faced by SOC is published.

Contribution 2: the theoretical and automation models can be used as a starting point for organisation and benefit from them. They can be developed further and maintained based on the need of each SOC. For example, an automation model shows how automation and machine learning are working towards detecting specific alerts. This can be done via using

Python Programming Language that is an effective solution for data analysis and making decisions. Having control over various variables can be achieved via the implementation of python automation in SOC.

Contribution 3: Based on the automation solution feedback from participants, a grid matrix is also created to assess the effectiveness of such a solution. Nonetheless, with only few amendments such a matrix can be applied for different other solutions.

This thesis helped in developing and improving our understanding of SOC. It also address potential directions that can be taken by researchers and practitioners who are interested in this field for further research and exploration. Limitations are mentioned to shed lights on the implications, but recommendations are also identified to be aware of these limits and overcome them in future research.

To summarise this thesis, it provided in-depth information about SOC. It is supported by an extensive literature in order to explain and highlight the importance of SOC for organisations. Evidence of cyber security threats and technical work are added to support the literature. It gives an in-depth understanding of how analysts perform their daily tasks. The collected data throughout interviews assisted in creating the automation model to overcome the mentioned challenges that are related to automation.

Thus, the focus was more on automation and ML in saving time and reducing the work that can be done on analysing logs. Experiments are carried out using python language to complement the overall work and to provide a taste of technicality for the thesis. In fact, cyber security attacks are growing, and the need of sophisticated tools is required more than ever. SOC plays essential role in mitigating such attacks. Hence, research that target SOC and their challenges is always required to implement, enhance, improve, and develop any existing functions.

6.3 Limitations

The limitations of this study highlight constraints and boundaries that have influenced elements of the research such as findings, methodology and research design. First of all, sample size is one of the limits of this study as we only conducted interviews with small number of participants. This can have an impact on the generalisability of our findings. The collected data

is completed via interviews with various participants, and this can have a bias influence in terms of honesty and accuracy of responses. A bias may be occurred in terms of the sample as we only conducted interviews with SOC specialists in UK only. Hence, external validity of our findings can be limited where regional variation might arise.

Time constraint is also amongst limits as longer term study over an extended period was not possible due to the nature of this research. Accessing to specific data and records such as an excel sheet that contains number of logs was not possible due to privacy and confidentiality concerns which limited the ability to produce comprehensive analysis. Participants ethical concerns were considered which constrained the ability to gather certain data. Accordingly, it is essential to understand that findings of this research may only be applied to a particular group and might not be generalised to other settings or contexts.

The subjective interpretation of qualitative data may propose bias into the analysis despite the effort of maintaining objectivity. Uncontrolled variables might have not been considered of the analysis which can influence the research outcome. Also, the study could be subject to publication bias as studies outcome are more likely to be published. This can cause overestimation of the impact sizes.

Experiments are only conducted to create foundation level of how automation can help in detecting specific logs based on predefined patterns. The number of logs organisations face is only a rough number that has been released during interviews with no given set of data or excel sheet that contain some of the logs due to privacy and regulations concerns. On the other hand, the developed theoretical model provides an overview of the challenges that are mentioned by interviewees and the required solutions to overcome them. However, the research focuses more on logs and the need of ML and automation in detecting specific logs.

Also, technical solutions are based on experiments, and they might only be applied into organisations who are willing to apply them. Thus, technical solutions and codes are limited to the implementation of specific tools. Thus, the structure behind solutions can be employed for different tools such as adding python code as plugin into Splunk SIEM, and code might need to be written in different query languages depending on the applied tool. For example, in Splunk, users use Splunk Processing Language to search for

information and alerts, but it is different for other tools.

It is important to acknowledge these limitations and constraints in order to maintain transparency and accuracy in research. Researchers must attempt to reduce these limitations as much as possible and examine their influence on the research conclusions.

6.4 Recommendations

This study provided valuable insights into the challenges faced by SOC and the need of automation to detect events. Further research is required to delve deeper into other aspects where different results might occur to help improving our understanding. More precisely in automation learning process where technology is being enhanced on daily basis. The findings of this study include valuable implications for SOC users. This can help them in focusing on these challenges and working on solutions to overcome them. Organisations can also benefit from these findings by considering using enhanced technological tools such as Splunk SIEM which has better processes than other SIEMs that organisations are currently using. This helps in increasing efficiency and analysing logs effectively. The effected group by SOC challenges can use these implications to spread awareness amongst SOC specialists plus engaging in their field to promote the desired changes.

The research can be expanded to include interviews with SOC specialist around the globe in order to find any other challenges that did not mentioned by this study‘s interviewees. Also, the code for experiments can be modified and enhanced continuously for more advanced automation. Methodological recommendations are also advised where enhanced data collection techniques are required to improve the validity of results in addressing particular limit. For future researchers, if they are able to retrieve actual data from organisations about specific logs, this would be beneficial to carry out more experiments. However, researchers must be aware of the ethical implications when collecting such data to ensure the integrity of the research process. Accordingly, some implications of the findings might occur over time. Therefore, it is essential to construct a long-term monitoring process that can help in tracking any changes to ensure recommendations are still up-to-date and relevant to the field.

It is also recommended to improve the impact of this research; any future findings are suggested to be published widely in trusted journals and

presenting them in conferences to reach broader audience. Also, engaging in peer review process is effective in seeking advice and feedback from experts. This can help in refining findings and ensure the validity and credibility of the research.

Each of the challenges mentioned in interviews can provide its own research direction. Therefore, scholars can carry out whole research by focusing only on one of these challenges. Collaborative research can also be conducted between researchers and institutions or organisations to address the complexity of SOC. Considering this approach will help researchers in expanding the scope and the influence of future studies. New challenges always occur and SOC is the future of tackling sophisticated security attacks. For professionals in the field of SOC, it is advised that training programs are offered based on this research findings to help in expanding knowledge and enhance practices within the industry. Overall, a non-stop and ongoing research is required in order to keep up with new trends and develop the needed solutions.

6.5 Reflection

Deciding to pursue a doctoral study was a constant ambition that I always had since completing BSc and MSc in computing related fields. My passion for continuous learning and knowledge exploration has led me to consider this route. The chosen topic was cyber security related due to its significance and importance for almost everyone nowadays. The purpose was to continue my studies as well as being an effective individual who could contribute towards the knowledge and community in general.

My eagerness to advance my own knowledge was not only the main purpose but also producing meaningful contribution to the field. As required by the university PhD policy the initial phase of my journey was on developing a solid foundation in research methodologies. Hence, research methodologies modules are completed successfully. This first achievement paved the road for me by providing the necessary tools and techniques that are required to approach my research with clarity and structural organisation.

Alongside the journey a mixture of stress and the feeling that I'm always behind are felt consistently. Retrieving acceptance from the research committee to carry out the research was an important milestone in this journey. As a result, I was able to publish two papers which helped in having more

believe to finalise the research. One of the main challenges I faced is when my first supervisor decided to leave the university but agreed to stay as my supervisor which helped a lot. Also, my second supervisor was always supportive and provided the assistance, guidance and feedback whenever is needed.

Being part of the staff members in my department was also a big challenge. This is due to the feeling that I need to produce a good piece of work. Delivering lectures and leading on outreach activities were part of the work that I had to carry out at the university. Thus, time management skills is improved efficiently to balance between my research and work. Public speaking is also improved as a result of presenting in conferences and delivering contents to audience.

By reflecting back on the whole journey, there are variety of advantages that have been achieved. The key takeaways are divided into different themes including academic, professional and personal. My academic, communication and technical skills are clearly improved as well as my confidence level. Also, my knowledge of cyber security more specifically the topic of SOC is expanded which is vital for career development.

Overall, I believe that I took the right decision by conducting a PhD research. I'm very grateful for all the advice, help, support and guidance by everyone who I met throughout this journey. My key advice to anyone who is willing to pursue a PhD research is to go for it as there is a lot of experience and knowledge to gain from.

7 Bibliography

Afzaliseresht, N., Miao, Y., Michalska, S., Liu, Q., and Wang, H. (2020). From logs to stories: human-centred data mining for cyber threat intelligence. *IEEE Access*, 8:19089–19099.

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2020a). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, 4(3):125–152.

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2020b). 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)*, pages 1–8. IEEE.

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers Security*, 124:102959.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., and Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, 101:102122.

Alharbi, S. A. (2020). A qualitative study on security operations centers in saudi arabia: challenges and research directions. *J. Theor. Appl. Inf. Technol.*, 98(24).

Ananthapadmanabhan, A. and Achuthan, K. (2022). Threat modeling and threat intelligence system for cloud using splunk. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE.

Andrade, C. (2020). The limitations of online surveys. *Indian journal of psychological medicine*, 42(6):575–576.

Anomali (2024). Five ways to improve soc efficiency in 2025.

Aung, W. P., Lwin, H. H., and Lin, K. K. (2020). Developing and analysis of cyber security models for security operation center in myanmar. In *2020 IEEE Conference on Computer Applications(ICCA)*, pages 1–6.

Ban, T., Samuel, N., Takahashi, T., and Inoue, D. (2021). Combat security alert fatigue with ai-assisted techniques. In *Cyber Security Experimentation and Test Workshop*, CSET '21, page 9–16, New York, NY, USA. Association for Computing Machinery.

Basyurt, A. S., Fromm, J., Kuehn, P., Kaufhold, M.-A., and Mirbabaie, M. (2022). Help wanted-challenges in data collection, analysis and communication of cyber threats in security operation centers. 20.

Berlin, K., Slater, D., and Saxe, J. (2015). Malicious behavior detection using windows audit logs. In *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, pages 35–44.

Bienias, P., Kołaczek, G., and Warzyński, A. (2019). Architecture of anomaly detection module for the security operations center. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pages 126–131.

Bikov, T., Radev, D., Iliev, T., and Stankovski, D. (2021). Threat hunting as cyber security baseline in the next-generation security operations center. In *2021 29th Telecommunications Forum (TELFOR)*, pages 1–4.

Calder, A. (2020). *Cyber Security: Essential principles to secure your organisation*. IT Governance Ltd.

Cersosimo, M. and Lara, A. (2022). Detecting malicious domains using the splunk machine learning toolkit. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6. IEEE.

Crowley, C. and Pescatore, J. (2019). Common and best practices for security operations centers: Results of the 2019 soc survey. *SANS, Bethesda, MD, USA, Tech. Rep*, pages 1–24.

Danquah, P. (2020). Security operations center: a framework for automated triage, containment and escalation. *Journal of Information Security*, 11(4):225–240.

de Céspedes, R. and Dimitoglou, G. (2021). Development of a virtualized security operations center. *J. Comput. Sci. Coll.*, 37(3):108–119.

Debar, H. (2019). Security operations & incident management knowledge area issue. *The Cyber Security Body Of Knowledge (CyBOK)*, pages 1–48.

Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S. L., and Iliadis, L. (2018). The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence. *Big data and cognitive computing*, 2(4):35.

Dun, Y. T., Ab Razak, M. F., Zolkiplib, M. F., Bee, T. F., and Firdaus, A. (2021). Grasp on next generation security operation centre (ngsoc): Comparative study. *International Journal of Nonlinear Analysis and Applications*, 12(2):869–895.

Engel, C., Mencke, S., Heumüller, R., Hormann, R., Aedtner, H., and Ortmeier, F. (2021). Customizable operation center for smart security management. *Procedia CIRP*, 104:1930–1935. 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0.

Eskelinen, T. (2022). Development of open-source siem and security operation centre in a company.

Faryadi, Q. (2019). Phd thesis writing process: A systematic approach–how to write your methodology, results and conclusion. *Online Submission*, 10:766–783.

Feng, C., Wu, S., and Liu, N. (2017). A user-centric machine learning framework for cyber security operations center. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 173–175.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., and Aylin, P. (2019). A retrospective impact analysis of the wannacry cyberattack on the nhs. *NPJ digital medicine*, 2(1):98.

Google (2025). Cybersecurity forecast 2025.

Gupta, S. and Gupta, B. B. (2017). Cross-site scripting (xss) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, 8:512–530.

Hall, C. (2025). Top 5 challenges facing modern socs (incorporating additional insights). https://www.cadosecurity.com/blog/top-5-challenges-facing-modern-socs-incorporating-additional-insights. (Accessed: 10/02/2025).

Han, C.-H. (2021). Blockade-detection-response based security operations dashboard design. *Computers in Human Behavior Reports*, 4:100143.

Hristov, M., Nenova, M., Iliev, G., and Avresky, D. (2021). Integration of splunk enterprise siem for ddos attack detection in iot. In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, pages 1–5.

ICO, I. C. O. (2018). General data protection regulation (gdpr). *Intersoft Consulting, Accessed in October*, 24(1).

János, F. D. and Dai, N. H. P. (2018). Security concerns towards security operations centers. In *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, pages 000273–000278. IEEE.

Jurgens, J. and Cin, P. D. (2025). Global cybersecurity outlook 2025.

Kiiveri, K. (2021). Automation in cyber security. *Turku University of Applied Sciences*, pages 1–31.

Kim, J.-y. and Kwon, H.-Y. (2022). Threat classification model for security information event management focusing on model efficiency. *Computers Security*, 120:102789.

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., and Ahn, G.-J. (2019). 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*, CCS '19, page 1955–1970, New York, NY, USA. Association for Computing Machinery.

Kotenko, I., Gaifulina, D., and Zelichenok, I. (2022). Systematic literature review of security event correlation methods. *IEEE Access*, 10:43387–43420.

Kotsias, J., Ahmad, A., and Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, 32(1):35–51.

Lalos, D. (2022). *Analysis on Security Orchestration Automation and Response (SOAR) platforms for Security Operation Centers.* PhD thesis, University of Piraeus (Greece).

Legislation.gov (1990). Computer misuse act 1990. https://www.legislation.gov.uk/ukpga/1990/18/contents. (Accessed: 07/04/2022).

Levshun, D. and Kotenko, I. (2023). A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities. *Artificial Intelligence Review*, pages 1–44.

Madani, A., Rezayi, S., and Gharaee, H. (2011). Log management comprehensive architecture in security operation center (soc). In *2011 International Conference on Computational Aspects of Social Networks (CASoN)*, pages 284–289.

Majid, M. A. and Ariffi, K. A. Z. (2019). Success factors for cyber security operation center (soc) establishment. EAI.

Mathew, A. (2021). Artificial intelligence for offence and defense-the future of cybersecurity. *Educational Research*, 3(3):159–163.

Melnikovas, A. (2018). Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of futures Studies*, 23(2):29–44.

Microsoft (2016). Web server (iis) overview. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831725(v=ws.11). (Accessed: 05/07/2022).

Mihindu, S. and Khosrow-shahi, F. (2020). Collaborative visualisation embedded cost-efficient, virtualised cyber security operations centre. In *2020 24th International Conference Information Visualisation (IV)*, pages 153–159. IEEE.

Mkandawire, S. B. (2019). Selected common methods and tools for data collection in research. pages 143–153. Marvel Publishers.

Mutemwa, M., Mtsweni, J., and Zimba, L. (2018). Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. In *2018 International conference on intelligent and innovative computing applications (ICONIC)*, pages 1–6. IEEE.

Nalanagula, S. and Roy, A. (2022). Cyber security operations centre: A user-cantered machine learning framework.

Nayak, M. and Narayan, K. (2019). Strengths and weaknesses of online surveys. *technology*, 6(7):0837–2405053138.

NCSC (2022). Building a security operations centre (soc). https://www.ncsc.gov.uk/collection/building-a-security-operations-centre. (Accessed: 04/06/2022).

Ndichu, S., Ban, T., Takahashi, T., and Inoue, D. (2021). A machine learning approach to detection of critical alerts from imbalanced multi-appliance threat alert logs. In *2021 IEEE International Conference on Big Data (Big Data)*, pages 2119–2127.

Nguyen, T. H. (2022). Cybersecurity logging & monitoring security program.

Nugraha, I. (2021). A review on the role of modern soc in cybersecurity operations. *Int. J. Current Sci. Res. Rev*, 4(5):408–414.

Oesch, S., Bridges, R., Smith, J., Beaver, J., Goodall, J., Huffer, K., Miles, C., and Scofield, D. (2020). An assessment of the usability of machine learning based tools for the security operations center. In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pages 634–641.

Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *2015 international conference on cyber situational awareness, data analytics and assessment (cybersa)*, pages 1–10. IEEE.

Onwubiko, C. (2018). Cocoa: An ontology for cybersecurity operations centre analysis process. In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–8. IEEE.

Onwubiko, C. (2021). Rethinking security operations centre onboarding. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–9.

Onwubiko, C. and Ouazzane, K. (2019). Challenges towards building an effective cyber security operations centre. *arXiv preprint arXiv:2202.03691*.

Pieters, W., Hadžiosmanović, D., and Dechesne, F. (2014). Cyber security as social experiment. In *Proceedings of the 2014 new security paradigms workshop*, pages 15–24.

Raimondi, M., Longo, G., Merlo, A., Armando, A., and Russo, E. (2022). Training the maritime security operations centre teams. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 388–393. IEEE.

Sadeghian, A., Zamani, M., and Abdullah, S. M. (2013). A taxonomy of sql injection attacks. In *2013 International Conference on Informatics and Creative Multimedia*, pages 269–273.

Saraiva, M. and Mateus-Coelho, N. (2022). Cybersoc framework a systematic review of the state-of-art. *Procedia Computer Science*, 204:961–972. International Conference on Industry Sciences and Computer Science Innovation.

Saunders, M., Lewis, P., and Thornhill, A. (2019). *Research methods for business students*. Pearson education, 8th edition.

Schinagl, S., Schoon, K., and Paans, R. (2015). A framework for designing a security operations centre (soc). In *2015 48th Hawaii International Conference on System Sciences*, pages 2253–2262.

Schlette, D., Vielberth, M., and Pernul, G. (2021). Cti-soc2m2 – the quest for mature, intelligence-driven security operations and incident response capabilities. *Computers Security*, 111:102482.

Seemma, P., Nandhini, S., and Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11):125–128.

Shah, A., Ganesan, R., and Jajodia, S. (2019). A methodology for ensuring fair allocation of csoc effort for alert investigation. *International Journal of Information Security*, 18:199–218.

Shah, S. A. R. and Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to snort system. *Future Generation Computer Systems*, 80:157–170.

Shahjee, D. and Ware, N. (2022a). Designing a framework of an integrated network and security operation center: A convergence approach. In *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, pages 1–4.

Shahjee, D. and Ware, N. (2022b). Integrated network and security operation center: A systematic analysis. *IEEE Access*, 10:27881–27898.

Sharma, K., Zhan, X., Nah, F. F.-H., Siau, K., and Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1):69–91.

Shatnawi, A. S., Al-Duwairi, B., Almazari, M. M., Alshakhatreh, M. S., Khader, A. N., and Abdullah, A. A. (2022). Adaptable plug and play security operations center leveraging a novel programmable plugin-based intrusion detection and prevention system. *arXiv preprint arXiv:2204.04576*.

Sievierinov, O., Ovcharenko, M., and Vlasov, A. (2021). Enterprise security operations center. *COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES*.

Singer, E. and Couper, P. M. (2018). Ethical considerations in internet surveys 1. *Social and Behavioral Research and the Internet*, pages 133–162.

Sopan, A., Berninger, M., Mulakaluri, M., and Katakam, R. (2018). Building a machine learning model for the soc, by the input from the soc, and analyzing it for the soc. In *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pages 1–8.

Stiawan, D., Idris, M., Malik, R. F., Nurmaini, S., Alsharif, N., Budiarto, R., et al. (2019). Investigating brute force attack patterns in iot network. *Journal of Electrical and Computer Engineering*, 2019:1–14.

Taqafi, I., Maleh, Y., and Ouazzane, K. (2023). A maturity capability framework for security operation center. *EDPACS*, 67(3):21–38.

Tardiff, M. F., Bonheyo, G. T., Cort, K. A., Edgar, T. W., Hess, N. J., Hutton, W. J., Miller, E. A., Nowak, K. E., Oehmen, C. S., Purvine, E. A., et al. (2016). Applying the scientific method to cybersecurity research. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pages 1–8. IEEE.

Tureczki, B. and Szenes, K. (2021). Interdisciplinary optimization of security operations centers with digital assistant. In *2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, pages 397–402.

Vaarandi, R. and Mäses, S. (2022). How to build a soc on a budget. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 171–177.

Venherskyi, P. and Karpiuk, R. (2021). Using machine learning (ml) to detect threat anomalies for reducing false-positives on the daily cybersecurity operation centre routine. *The 12th International Scientific Conference ≪ITSec≫*, (29):123–128.

Vielberth, M., Böhm, F., Fichtinger, I., and Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8:227756–227779.

Weissman, D. and Jayasumana, A. (2020). Integrating iot monitoring for security operation center. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE.

Yin, L., Fang, B., Guo, Y., Sun, Z., and Tian, Z. (2020). Hierarchically defining internet of things security: From cia to caca. *International Journal of Distributed Sensor Networks*, 16(1):1550147719899374.

Zhang, X., Knockel, J., and Crandall, J. R. (2015). Original syn: Finding machines hidden behind firewalls. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 720–728.

Zhang, Y. and Wildemuth, B. M. (2009). Unstructured interviews. *Applications of social research methods to questions in information and library science*, 2:222–231.

Zhong, C., Lin, T., Liu, P., Yen, J., and Chen, K. (2018). A cyber security data triage operation retrieval system. *Computers Security*, 76:12–31.

Appendices

A Publication I

- *Assessing the Challenges faced by Security Operations Centres (SOC)*

Publisher Name: Springer, Cham

Date: 17/03/2024

Part of the book series: Lecture Notes in Networks and Systems ((LNNS, volume 920))

Presented at: The Future of Information and Communication Conference (FICC 2024)

B Publication II

- *A Grid-Matrix Based on Industry Needs to Evaluate Automation in Security Operations Centre (SOC)*

Publisher Name: IEEE Xplore

Date: 08/11/2024

Presented at: The 11th International Conference on Future Internet of Things and Cloud (FiCloud 2024)

C Author Consent Form

UNIVERSITY OF GLOUCESTERSHIRE

UNIVERSITY AUTHOR CONSENT FORM FOR A RESEARCH THESIS

This form must be submitted along with the final version of the thesis.

I confirm that I have read and understood the University's regulations and procedures concerning the submission of a thesis (as summarised below) and have submitted the following items in order to fulfil my requirements for graduation from the University of Gloucestershire:

Author's Name: KAMAL ODAN

Title of Thesis: ANALYSIS OF KEY CHALLENGES IN SECURITY OPERATIONS CENTRE (SOC). A NOVEL AUTOMATED SOLUTION TO REDUCE NOISY EVENTS

Degree: DOCTOR OF PHILOSOPHY

University Reference Copy

I understand that requests made by any individual or organisation to the University Library to borrow my thesis will be referred to the University's Research Repository or Electronic Thesis Online Service (ETHOS).

I understand that the library will add the following notice to the final version of my thesis:

© [author name] [date of completion]
This thesis is copyright material and no quotation from it may be published without proper acknowledgement.

Deposit in the University's Research Repository

COVERED WORK
In accordance with current University regulations, the thesis is deposited in the University's Research Repository. Research referred to below as "Thesis" is covered by this agreement and when I deposit my Thesis in the future, whether personally or through an assistant or other agent, I agree to the following:

NON-EXCLUSIVE RIGHTS
Rights granted through this agreement are entirely non-exclusive. I am free to publish the Thesis in its present version or future versions elsewhere and I agree that the University's Research Repository administration may, without changing content, translate the Thesis to any medium or format for the purpose of future preservation and accessibility.

I understand that work deposited in the University's Research Repository and EThOS will be accessible via the World Wide Web. I understand that once the Thesis is deposited, a citation will always remain visible. Removal of the item is usually only possible for legal reasons.

Sept 2021

I understand that as a consequence of depositing the Thesis in the University's Research Repository an electronic copy will be included in EThOS. In doing so I understand that work deposited in EThOS repository will be accessible via the Internet. EThOS, or its agents, may without changing content, translate the Thesis to any medium or format for the purpose of future preservation and accessibility.

FURTHER INFORMATION ON EMBARGOS
Your thesis will normally be included in the University's Research Repository and EThOS unless you impose an **Embargo** (maximum of 2 years from the date of the viva voce examination). During the embargo period, your thesis will be withheld from inclusion in EThOS and no consultation, loan or copying of it will be possible.

Permission to impose an embargo of more than 2 years can only be granted by the Chair of the Research Degrees Committee and is usually applicable only in exceptional circumstances, e.g., when your thesis contains sensitive material.

Please note: Once the embargo period has expired, work will be included in the University's Research Repository and EThOS. If you require an extension to the embargo period please apply to the Chair of the Research Degrees Committee before the current embargo has expired.

I AGREE AS FOLLOWS:

- That I have exercised reasonable care to ensure that the Thesis is original, and does not to the best of my knowledge break any UK law or infringe any third party's copyright or other Intellectual Property Right.
- The administrators of the University's Research Repository do not hold any obligation to take legal action on behalf of the Depositor, or other rights holders, in the event of a breach of intellectual property rights, or any other right, in the material deposited.
- I have consulted with my supervisor, any co-supervisors and any commercial sponsors regarding the requirement for an embargo (please see notes above) and we agree as follows:

☒ No embargo is required

☐ An embargo is required for a period of _____ years (max 2 yrs)

Reason/s for embargo (must comply with one or more exemptions under the Freedom of Information Act 2000 Part II, sections 22-44) https://www.legislation.gov.uk/ukpga/2000/36/pdfs/ukpga_20000036_en.pdf

Please note: If you do not specify one of the above we will assume that you do not require an embargo and will proceed in adding your thesis to the University's Research Repository and make it available for consultation.

Signature..... [redacted]

Name (Block capitals):.....KAMAL ODAN.....

Student number..... [redacted]

Email..... [redacted]

Phone..... [redacted]

Date.....26/05/2025.....

Sept 2021