People's Democratic Republic of Algeria

الجمهورية الجزائرية الديمقراطية الشعبية

Ministry of Higher Education and Scientific Research

وزارة التعليم العالي والبحث العلمي

Saad Dahleb Bida 1 University

Computer Science Faculty

Matster's Thesis

Towards the Master's Degree in Computer Science

Design and Implementation of a SOC Based on Elastic SIEM

Achieved by:

BOUABID Abou El Kacem Amine SSI

ZOUBIRI Abdelmalek SIR

Supervised by:

AROUSSI Sana

KHOUFACHE Azeddine

Defended on 30/06/2024 before the jury consisting of:

President: OUKID Salyha

Examiner: BENYAHIA Mohamed

2023/2024

Acknowledgements

We are writing to express our deepest gratitude for the support and guidance we have received throughout this incredible journey.

First and foremost, we would like to thank Allah for His countless blessings, for providing us with strength, wisdom, and perseverance. Without His divine guidance, none of this would have been possible.

To our family and friends, thank you for your unwavering support and encouragement. Your love and belief in us have been our greatest sources of strength. You have stood by us through every challenge and celebrated each achievement, making this journey all the more meaningful.

We are also profoundly grateful to our teachers at the university. Your dedication and commitment to education have inspired and equipped us with the knowledge and skills necessary for success. Special thanks go to our supervisor, whose guidance and support have been instrumental in our academic growth. Your insights and mentorship have been invaluable.

Lastly, we extend our heartfelt thanks to the host organization for this incredible opportunity. Your support and resources have provided us with a platform to learn, grow, and achieve our goals. Special thanks again to our supervisor at the host organization for their continuous help and encouragement.

Thank you all for being an essential part of this journey. We are forever grateful for your contributions and support.

With sincere gratitude,

The students.

Abstract

As cybersecurity threats continue to evolve in complexity and frequency, companies face growing challenges in safeguarding their assets. Despite the availability of various security solutions, organizations still endure significant losses from these attacks. Moreover, in Algeria, there has been a tightening of regulations concerning the security obligations of companies.

Implementing multiple security measures can be complex and may have drawbacks. Therefore, establishing a centralized facility to oversee these measures is imperative. By deploying a Security Operations Center (SOC), organizations can bolster their security posture, leading to fewer incidents and mitigated losses in the event of cyber-attacks.

Our project aims to establish a SOC for MNA, using Elastic SIEM and the NIST incident response framework. This initiative not only reduces costs for the company but also streamlines security operations, making them more manageable and efficient.

Keywords: SOC, SIEM, Elastic, Incident Response, NIST, Cybersecurity.

Résumé

Alors que les menaces de cybersécurité continuent d'évoluer en complexité et en fréquence, les entreprises sont confrontées à des défis croissants pour protéger leurs actifs. Malgré la disponibilité de diverses solutions de sécurité, les organisations subissent toujours des pertes importantes à cause de ces attaques. Par ailleurs, en Algérie, on constate un durcissement de la réglementation concernant les obligations de sécurité des entreprises.

La mise en œuvre de plusieurs mesures de sécurité peut être complexe et peut présenter des inconvénients. Par conséquent, il est impératif de mettre en place un cadre centralisé pour superviser ces mesures. En déployant un centre d'opérations de sécurité (SOC), les organisations peuvent renforcer leur posture de sécurité, ce qui réduit le nombre d'incidents et atténue les pertes en cas de cyberattaques.

Notre projet vise à établir un SOC pour MNA, en utilisant Elastic SIEM et le cadre de réponse aux incidents du NIST. Cette initiative permet non seulement de réduire les coûts pour l'entreprise, mais aussi de rationaliser les opérations de sécurité, en les rendant plus faciles à gérer et plus efficaces.

Mots Clé : SOC, SIEM, Elastic, Réponse aux Incidents, NIST Cybersécurity.

ملخص

مع استمرار تطور تهديدات الأمن السيبراني من حيث التعقيد والتكرار، تواجه الشركات تحديات متزايدة في حماية أصولها. على الرغم من توفر حلول أمنية مختلفة ، لا تزال المنظمات تعاني من خسائر كبيرة من هذه الهجمات. وعلاوة على ذلك، صارت الدولة الجزائرية تشدد على اللوائح المتعلقة بالالتزامات الأمنية للشركات.

يمكن أن يكون تنفيذ تدابير أمنية متعددة معقدا وقد يكون له عيوب. ولذلك، فإن إنشاء مرفق مركزي للإشراف على هذه التدابير أمر حتمي. من خلال نشر مركز العمليات الأمنية (SOC) ، يمكن للمؤسسات تعزيز وضعها الأمني ، مما يؤدي إلى عدد أقل من الحوادث وتخفيف الخسائر في حالة الهجمات الإلكترونية.

يهدف مشروعنا إلى إنشاء مركز عمليات أمن (SOC)لمجموعة MNA، باستخدام Elastic SIEM واستعمال إطار الاستجابة للحوادث NIST. لا تقلل هذه المبادرة من التكاليف على الشركة فحسب، بل تعمل أيضا على تبسيط العمليات الأمنية، مما يجعلها أكثر قابلية للإدارة والنجاعة.

كلمات المفتاحية: مركز العمليات الأمنية، نظام إدارة المعلومات والأمان، Elastic، الاستجابة للحوادث، NIST، الأمن السيبراني.

Contents

List of Figures

List of Tables

Abbreviation List

ACL Access Control List

API Application Programming Interface

BTHb:SOCTH Blue Team Handbook: SOC, SIEM, and Threat Hunting

CA Certificate Authority

CCNA Cisco Certified Network Associate

CEO Chief Executive Officer

CIA Confidentiality,Integrity, Availability

CLEH Certified Lead Ethical Hacker

COBIT Control Objectives for Information and Related Technology

CM Cybersecurity Manager

CMD Command-Line

CMMI Capability Maturity Model Integration

CPU Central Processing Unit

CSR Certificate Signature Request

DDoS Distributed Denial of Service

DNS Domain Name Service

DoS Denial of Service

ECS Elastic Common Scheme

EDR Endpoint Detection and Response

EQL Event Query Language

ESQL Elasticsearch Query Language

GPO Group Policy Object

HR Human Resources

HTTP Hypertext Transport Protocol

IDS Intrusion Detection System

IP Internet Protocol

IR Incident Response

ISO International Organisation of Standarisation

ISP Internet Service Provider

IT Information Technology

JSON JavaScript Object Notation

KQL Kibana Query Language

LA Lead Auditor

LI Lead Implementer

MNA Mare Nostrum Advising

NAS Network Attached Storage

NFS Network File System

NIC Network Interface Card

NIST National Institute of Standards and Technology

NSM Network Security Monitoring

NTP Network Time Protocol

OS Operating System

PDCA Plan Do Check Act

PDF Portable Document Format

P2P Point to Point

RAM Random Access Memory

RBAC Role Based Access Control

RM Risk Management

SAN Storage Area Network

SIEM System Information and Event Management

SLA Service level agreement

SOC Security Operations Center

SQL Structured Query Language

SSH Secure Shell Protocol

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

UI User Interface

URL Uniform Resource Locator

VA Vulnerability Assessments

VLAN Virtual Local Area Network

VM Vulnerability Management

VPN Vritual Private Network

General Introduction

Enterprise security involves a wide array of strategies, plans, policies, and technologies aimed at protecting an organization's information, assets, employees, and operations. This protection extends to data as it travels across networks. As the digital landscape evolves and organizations increasingly adopt cloud computing and digital infrastructure, the demand for strong enterprise security measures continues to rise. Enterprise security ensures the confidentiality of sensitive data, maintains the integrity of information, and guarantees system availability, thereby bolstering the resilience and reliability of the organization's operations.

Security attacks are becoming increasingly complex and exhibiting increasingly sophisticated capabilities. So, addressing the complexity and sophistication of such attacks must include not only investing in preventive measures, but also the development of intelligent and integrated monitoring capabilities incorporated into an incident response program.

Arguably, getting compromised at some point is inevitable. As the previous CEO of Cisco Systems, John Chambers, said, *"There are two types of companies: those who have been hacked and those who don't yet know they have been hacked"*. So, the organisations need to be warned: A security breach is not an *if* but a *when*. The good news is that a breach does not necessarily mean that the business will immediately experience negative impact, because attackers usually need time to accomplish their objectives beyond gaining unauthorized access to the network. Discovering and preventing this type of behavior is just one of the many reasons organizations develop a security operations center (SOC) [1].

MNA group is an enterprise that specializes in cyber-Security which aims to solidify its security to ensure its clients personal data safety. This project aims to collect all the security measures of MNA group in one solution, monitoring all employees activities and improve the security incidents detection and response by setting up a SOC using a SIEM solution, creating processes for incident response, log retention and new detection rule creation.

In the first chapter, we will introduce key aspects of information security. We will then delve into the concepts of a Security Operations Center (SOC), covering its core elements, the main services it provides to a company, and the methodology used to set up a SOC within an organization. Additionally, we will explain what Security Information and Event Management (SIEM) is, discuss its components, review the solutions available in the market, and highlight why Elastic is the best choice for our needs.

In the second chapter, we will use the methodology outlined in the first chapter, along with Elastic SIEM and the NIST framework, to set up a SOC for the MNA group. This

will begin with studying the organization's structure and network diagram and analyzing its security needs. We will then design the SIEM architecture, assign the SOC team, and create the SOC processes and incident response documents. A list of necessary detection rules for the organization will also be prepared.

In the final chapter, we will implement the SIEM architecture using the Elastic Stack, configure and secure its components, and set up security measures such as the reverse proxy, host firewall. Following this, we will configure Rsyslog and create policies to integrate the source devices. We will then implement the detection rules. Finally, we will explain some of the attacks and showcase some of the detection rules we created for them .

In the conclusion, we will comprehensively summarize the work we have undertaken throughout this project, encapsulate the achievements of this project and outline potential steps for sustaining and enhancing the SOC to ensure long-term security and resilience for the MNA group.

Chapter 1

Introduction on Security Operation Center

1.1 Introduction

In an increasingly digital world, information security has become a crucial concern for businesses and organizations. Sensitive data, computer systems and networks are exposed to risks such as cyber-attacks, data loss and breaches of confidentiality. To address these challenges, it is important to examine the various aspects of information security and understand the measures taken to manage them.

In the first chapter, we will explore the various aspects of information security. Additionally, we will delve into the Security Operations Center (SOC) and its components and services. Then, we will focus on Security Information and Event Management (SIEM) and its anatomy, then take a look at some of the most popular SIEM solutions available in the market. After that, we will define the incident response and cover its timeline. Finally, we will dive into the SOC's set up process.

1.2 Information Security

The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [2]. Information security stand on three main pillars, referred to as the CIA triad [3]:

- **Confidentiality:** refers to protecting information from being accessed by unauthorized parties.
- **Integrity:** refers to the consistency, accuracy, and trustworthiness of data over its entire life-cycle.
- **Availability:** of data is that the business or authorized user can access it when needed, the data should be readily available to authorized users.

1.2.1 Concepts

There are several concepts that pertain to information security:

- **Threat:** any circumstance or event with the potential to cause the security of the system to be compromised [4].

- **Vulnerability:** A bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability [5].
- **Risk:** is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence [6].
- **Asset:** the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes [7].
- **Risk Assessment:** the probability that a particular security threat will exploit a system vulnerability [8].
- **Log:** A record of the events occurring within an organization's systems and networks.[9]

1.2.2 Risks

Some of the common types of information security risks are:

- **Malware:** a program that is written intentionally to carry out annoying or harmful actions, which includes viruses, Trojan horses and worms [10].
  - **Virus:** a program that replicates itself by attaching to other programs or files, where it hides until activated [11].
  - **Trojan Horse:** a useful or seemingly useful program that contains hidden code of a malicious nature that executes when the program is invoked [12].
  - **Worms:** a self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself [13].
- **Denial of Service (DOS):** is the prevention of authorized access to a system resource or the delaying of system operations and functions, distributed denial of service (DDoS) is a denial of service technique that uses numerous hosts to perform the attack [14] [15].
- **Social Engineering:** is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks [16].

1.2.3 Essential Measures

Information security measures are a set of practices and procedures including non-technical (teams) and technical measures that aim to protect information from unauthorized access, use, disclosure, disruption, modification, or destruction.

1.2.3.1 Teams

The responsibilities of individuals in the field of cyber-security are categorized into two distinct teams:

- **Red Team:** a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cyber-security by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment [17].

- **Blue Team:** the group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks, one over a significant period of time, two in a representative operational context (e.g., as part of an operational exercise), and three according to rules established and monitored [18].

1.2.3.2 Technical

There are several strategies that exists in order to enhance security in the domain of cybersecurity:

- **Encryption:** cryptographic transformation of data (called "plain-text") into a form (called "cipher-text") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state [19].
- **Firewall:** an inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall) [20]. auth access
- **Authentication:** security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [21]
- **Access Control:** procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space.[22].

1.3 Security Operation Center (SOC)

It means different things to different people, but the definition for a SOC used in BTHb:SOCTH [18] is:
"A centralized team in a single organization that monitors the information technology environment for vulnerabilities, unauthorized activity, acceptable use/policy/procedure violations, intrusions into and out of the network, and provides direct support of the cyber incident response process."

1.3.1 Services

Security operations center can provide numerous services to the business, the implementation of these services based on business type, funding, and other things [23].

1.3.1.1 Reactive Services

The services in response to incidents are mainly:

- **Monitor Security Posture(Alerts):** this is the primary role of SOC: monitoring the environment for security conditions, alarms, health of the security platform, and responding through the organizations various technical solution(s).

- **Command Function(IR/Analysis):** this may be a recurring activity, incident command means that the SOC will identify incidents, work with incident handler, coordinate containment operations, assist in eradication efforts, take information from the incident and use it to better implement internal systems based on newly found intelligence and may also support pushing out updates or other fixes.
- **Initiate & Manage Incident Response(identification and remediation support):** a significant portion of the activities of a SOC focuses on finding and validating security incident based in alarm and NSM work.
- **Vulnerability Management:** the SOC can assist and run the vulnerability management program (take on consideration of tasking that may not able to handle), effective VA/VM program needs to be executed within the business context and concept layer.
- **Forensics/eDiscovery:** depending the size of SOC, forensic support may be conducted in-house or with a third party, the difference between forensics and eDiscovery is that eDiscovery is focused on collecting search information from live, in use data and information repositories that is generated and used by people, Forensic goes deeper, examining system artifacts from the file system that show intent for users to interact files and data.
- **Reporting:** run reports to support compliance requirements and IT General Controls monitoring.
- **Malware Analysis:** tools allow to upload a suspect binary and then advise if it is known bad and provide varying levels of activity analysis, if the analysis reveals something suspicious, operational intelligence task taking, best practices is running samples through a local malware analysis engine built on Sandbox to prevent informing the attacker, who is likely monitoring online services, that the malware was found.
- **Intrusion Detection:** detection systems can be deployed on the network and host, and all require care and feeding in order to make sure they are operating properly.
- **Notification Refinement:** alarm conditions that are deemed valid create notifications with sufficient supporting information for the recipient(s).

1.3.1.2 Proactive Services

These services are counter-measures for incidents.

- **Network Security Monitoring:** NSM is the collection, detection, analysis, and escalation of indications and warnings based on network level data that indicate an intrusion.
- **Threat Hunting:** is a proactive process that inherently assumes that there is some form of intrusion or breach, it sees to detect security threats, intrusions, misuse, and breaches by data mining, it start by hypothesis of compromise and then tests that hypothesis.
- **Platform Health Monitoring:** monitoring the SIEM dashboards and alert stream, reviewing and acting on alerts following a priority basis, and the SIEM platform and

other supporting data sources in order to detect issues and work with data custodians to ensure data survivability (making sure that events are parsed and creating new or refined alarms).

- **Threat Intelligence:** according to Gartner *"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."*

1.3.1.3 Other Services

Theses services are extra measures to take to strengthen security:

- **Policy and Procedure Support:** all monitoring controls and capabilities should tie directly to established policy and procedure.
- **Internal Training and support:** ensuring that as the SOC changes the line staff must be trained and updated. (blue team).

1.3.2 The Core Elements

An effective SOC need to have a good mix of these three areas (figure 1.1), People, Process and Technology [1].

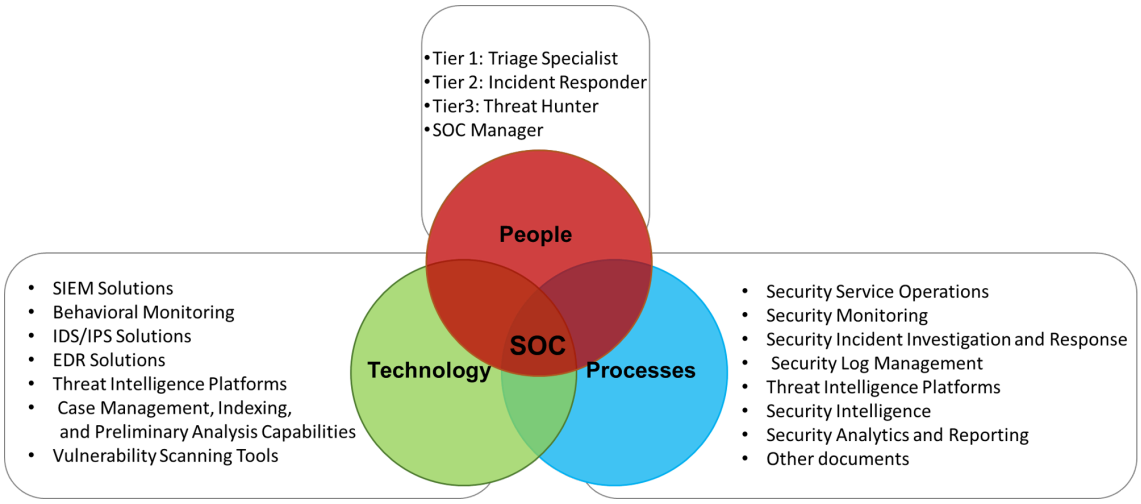

Figure 1.1: The pillars of SOC

1.3.2.1 People

Are the core of any successful SOC, when evaluating people-related capabilities, areas that pertain to governance, structure, experience, and training and certifications should be considered.[1]

The responsibilities of these individuals are primarily segmented into four distinct roles:

- **Tier 1 — Triage Specialist:** are mainly responsible for collecting raw data, reviewing alarms and alerts and identifying other high-risk events and potential incidents. For every alert, the triage specialist has to identify whether it's justified or a false positive, as alert fatigue is a real issue. If problems occurring cannot be solved at

this level, they have to be escalated to tier 2 analysts. Furthermore, triage specialists are often managing and configuring the monitoring tools.

- **Tier 2 — Incident Responder:** review the higher-priority security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence (indicators of compromise, updated rules, etc.). Incident responders are responsible for designing and implementing strategies to contain and recover from an incident. If a tier 2 analyst faces major issues with identifying or mitigating an attack, additional tier 2 analysts are consulted, or the incident is escalated to tier 3.
- **Tier 3 — Threat Hunter:** are the most experienced workforce in a SOC. They handle major incidents escalated to them by the incident responders. They also perform or at least supervise vulnerability assessments and penetration tests to identify possible attack vectors. Their most important responsibility is to proactively identify possible threats, security gaps and vulnerabilities that might be unknown. Additionally, any critical security alerts, threat intelligence, and other security data provided by tier 1 and tier 2 analysts need to be reviewed at this tier.
- **SOC Manager:** supervises the security operations team and provides technical guidance if needed. This includes training and evaluating team members, creating processes, assessing incident reports and developing and implementing necessary crisis communication plans. He also oversees the financial aspects of a SOC, support security audits and reports to the respective top-level management position.

In addition to the tiered roles, multiple other technical and specialty roles can exist.

1.3.2.2 Processes

Are the enablers between people and technology, the security operations processes that assess how security incidents and vulnerabilities are handled, understanding and documenting the current state of SOC processes are important to the development of a suitable and realistic SOC road-map [1]. The two words process and procedure are so often spoken together in this industry, there seems to be little to distinguish between them:

- **Processes:** used to describe a set of proscribed actions that are taken to perform a particular set of activities under a service.
- **Procedures:** describe a specific step-by-step way that an individual performing an activity must perform that activity.

The number of processes and procedures types in a SOC is based on the policies and requirements of the company, the services offered, and the technologies used:[1],

- **Security Service Operations:** processes and procedures under security service operations address approved methods to maintain SOC systems and content.
- **Security Monitoring:** processes and procedures under security monitoring address how commonly occurring events and incident reports should be examined, assessed, and escalated if necessary.
- **Security Incident Investigation and Response:** processes and procedures for security incident investigation and response address how to perform investigations and handle incidents in highly consistent and rigorously defined ways where appropriate.

- **Security Log Management:** processes and procedures for security log management are focused on how to manage the entire log management life-cycle consistently and according to enterprise-wide policies and procedures. Although this might be provided through a common log management solution, it is also common for the SOC to be responsible for security log management specifically.
- **Security Intelligence**: processes and procedures for security intelligence, including threat and vulnerability intelligence provided by human intelligence analysts, are focused on how to provide human-readable intelligence based on current threats and vulnerabilities within the environment and on external intelligence relevant to the organization.
- **Security Analytics and Reporting:** processes and procedures for security analytics and reporting cover how raw security and SOC services data/outputs will be analyzed and reported. This includes both scheduled and ad hoc reporting for a wide variety of potential consumers.

There also exists other types of processes and procedures in the SOC like **Security Service Management** and **Security Vulnerability Management**.

1.3.2.3 Technology

Using the right technology is also critical to the success SOC, technology is related to infrastructure readiness, log collection and processing, system monitoring, security control positioning, and vulnerability management [1].

The components of a SOC focus primarily on tools and technologies that assist security experts in monitoring, analyzing, investigating, and responding to security incidents, such as:

- **Security Information and Event Management (SIEM) Solution:** provides real-time event monitoring, analysis, and alerts.
- **Behavioral Monitoring:** assists security experts in creating a baseline when using machine learning or behavior modeling to identify security concerns.
- **Intrusion Detection System (IDS):** helps security experts detect an attack in the initial phases.
- **Endpoint Detection and Response (EDR):** provides visibility and containment options.
- **Threat Intelligence Platforms:** collects and aggregates internal and external sources of information for investigation.
- **Case Management, Indexing, and Preliminary Analysis Capabilities:** captures case-related data and tracking information, performs analysis, and gathers results for investigation.
- **Vulnerability Scanning Tools:** those tools with vulnerability assessments help detect these weaknesses and take the necessary actions to correct them and enhance security.

1.4 SOC Set-Up Methodology

The deployment of a SOC can be a complex process, involving the selection of appropriate technologies and tools, the establishment of operational processes, staff training and the validation of SOC effectiveness. However, a well-designed and well-managed SOC can help organizations improve their security posture and protect their IT assets.

In this section, we will explore the processes for building an effective SOC, using best practices recommended in the book *'Security Operations Center: Building, Operating, and Maintaining Your SOC'* by Joseph Muniz, Gary McIntyre, and Nadhem AlFardan. We will examine the different stages of SOC deployment (figure 1.2), including planning, design, construction, operation, and maintenance [1].

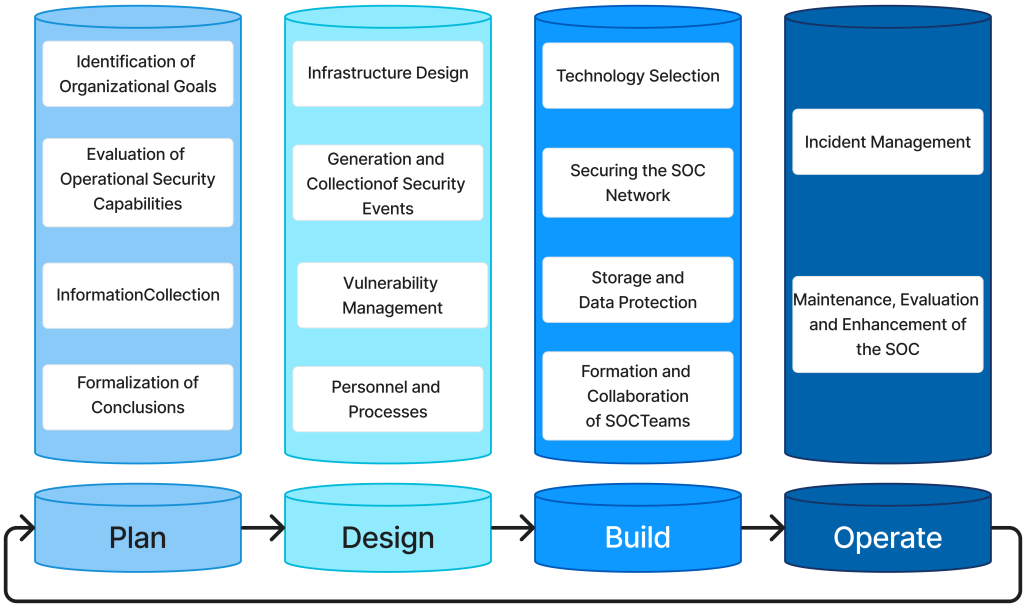

Figure 1.2: SOC Set-Up Methodology. [1]

1.4.1 Planning Phase

This phase is essential for planning the implementation of an effective SOC, ensuring that the SOC is designed to meet the organization's needs and maximize its impact on business activities.

1.4.1.1 Identification of Organizational Goals

It is necessary to clearly establish the business and IT objectives of the organization to enable the SOC to be structured accordingly. The business objectives are the desired results the organization aims for in terms of performance, profitability, and customer satisfaction. The IT objectives are the organization's desired results in terms of security, availability, and reliability of its IT infrastructure.

By defining both the business and IT objectives clearly, the SOC can be customized to address the organization's requirements and enhance its influence on the business.

1.4.1.2 Evaluation of Operational Security Capabilities

The evaluation of operational security capabilities allows for the collection of information and analysis of existing security processes within the organization. This assessment helps determine the maturity level of information security within the organization. The evaluation can be handled by using a maturity assessment methodology, such as CMMI (Capability Maturity Model Integration) or COBIT (Control Objectives for Information and Related Technology).

This process helps point out the areas where improvements are needed and defines investment priorities for the SOC.

1.4.1.3 Information Collection

Once the business and IT goals and the operational security capabilities of the organization have been identified, it is important to collect all relevant information about the organization, its IT processes, systems, and applications. This may include details about critical systems and applications, potential threats, known vulnerabilities, past security incidents, and current security management practices.

1.4.1.4 Formalization of Conclusions

After running a thorough analysis of operational security capabilities and maturity levels, the conclusions must be normalized in the form of reports. These reports are used to justify investment in SOC construction and to inform organizational decision-makers about security priorities.

The planning phase is critical for the success of SOC construction because it ensures that resources are allocated appropriately and that investments in information security are aligned with the organization's strategic objectives.

1.4.2 Design Phase

The design of a SOC is a crucial step in ensuring the security of an organization. During this phase, the SOC plans the necessary infrastructure to effectively collect security events and manage vulnerabilities. The SOC is also responsible for monitoring, analyzing and responding to security incidents. To ensure the success of this mission, the SOC must have a robust infrastructure, qualified personnel, and well-defined processes.

1.4.2.1 Infrastructure Design

During the design of a SOC, several key elements must be considered to guarantee its smooth operation. This includes the work environment for SOC analysts, which means they need access to tools and technologies that allow them to efficiently collect and analyze security data. Additionally, they should have access to communication tools such as instant messaging, video conferencing systems and file-sharing tools to ease collaboration and communication among themselves.

- **Internal Arrangement of The SOC**
  - **The Operations Room:** is the area where SOC analysts carry out their daily tasks. This includes monitoring SOC dashboards, handling incidents, analyzing and investigating security incidents, conducting research, and performing administrative duties. The layout of the operations room should provide all

SOC analysts with direct visibility to the SOC video wall used to project or display various dashboards.

- **The Crisis Room:** typically equipped with conference and video conferencing facilities, allows remote participants to engage. The SOC team uses this room for managing major or severe security incidents, but it is also utilized for regular meetings.
- **The SOC Manager's Office:** manages the SOC's operations. It is recommended that their office are within the SOC ground and separated by glass windows, allowing visibility into the operations room and the SOC's video wall.
- **The Computer Room (Optional):** It may be necessary to set up a computer room to host SOC equipment when it cannot be securely hosted in other locations such as data centers. If a SOC computer room is required, environmental controls for the computer room must be considered to assure that heating, electrical power, air conditioning, and other requirements comply with the organization's standards.

The video wall must be positioned sufficiently high so that all screens are easily visible to SOC analysts from their seated positions.

- **Workspace for SOC Analysts** SOC analysts need to be able to work effectively in a highly stressful environment. Security incidents can be extremely stressful and SOC analysts need to perform under pressure to swiftly resolve security incidents. To achieve this, it is important to provide a comfortable and ergonomic work environment for SOC analysts.

  The analysts should also have access to a standard corporate workstation for routine tasks such as email and web browsing. It is also important for analysts to have access to a telephony service for internal, local, and, if necessary, international calls. Incoming and outgoing calls can be recorded if needed for security purposes.

- **SOC Network Design** The design of a SOC explains how to organize and access the various components of the SOC network. For this purpose, network segmentation (either virtual or physical) is required. Here's a common SOC network design:

  - **SOC Tools:** These tools should be hosted in a dedicated and isolated network segment, accessible only from the analysts' workstations.
  - **Analyst Workstations:** A specific network segment should be dedicated to SOC analyst workstations.
  - **Standard Enterprise Services:** A separate network segment, not connected to the SOC network, should be reserved for standard enterprise services such as email and internet traffic.
  - **Malware-Related Tasks:** Many SOCs also require an additional segment for malware-related tasks, such as reverse engineering, Sand-boxing, or hosting systems used for other high-risk activities.

  It is also important to choose a stable and secure operating system that supports necessary security applications, such as SIEM, vulnerability management tools, and log management tools.

  Having an efficient storage infrastructure is essential for storing the collected security data. Security data can be stored on local disks, shared disks, or network

storage systems like SAN and NAS. Selecting a storage solution that aligns with the organization's capacity, performance, and cost requirements is vital.

1.4.2.2 Generation and Collection of Security Events

The collection of security events allows the SOC to monitor network, system, and application activities and detect potentially malicious anomalies.

Security events can include firewall alerts, audit logs, user activity records, and intrusion detection alerts. Security event collection tools must be configured to capture relevant events and store them securely. Careful attention should be given to selecting security event collection tools and integrating them with other security tools.

Accurate clock synchronization is necessary to insure correlation and consistency of security events collected from different sources. If clocks are not properly synchronized, inconsistencies in the timestamps of collected security events may hinder threat detection correlation. It can also delay the resolution of security incidents. Therefore, establishing a reliable Network Time Protocol (NTP) server is important to guarantee precise clock synchronization across all security data collection devices.

1.4.2.3 Vulnerability Management

It is practically impossible not to have vulnerabilities in a system, so it is essential to have a clear definition of how the SOC manages vulnerabilities, as well as support from management to enforce associated policies. Vulnerabilities can be caused by poor software configuration or errors in network architecture, weak security policies such as using short and predictable passwords, hardware or software manufacturing defects, lack of information about potential threats, weaknesses in ports or protocols used, and much more.

In general, vulnerability management is a cyclical process that involves identifying, classifying, remediating, and mitigating vulnerabilities. There are several methods for managing vulnerabilities, and organizations can utilize services such as compliance audits, vulnerability assessments, configuration evaluations, and penetration testing to identify vulnerabilities.

Compliance audits assess the risk level of a system or application, evaluate risks related to network architecture design, or assess existing controls against a set of standards or guidelines. Vulnerability assessments and penetration tests aim to identify vulnerabilities in devices, operating systems, and applications using automated scanning tools. Once vulnerabilities are identified, it is necessary to prioritize them based on severity and exploitability. Critical vulnerabilities should be addressed first, while less critical ones can be managed later.

The primary objective of vulnerability management for a SOC is to reduce the risk associated with technical weaknesses to an acceptable level. There will always be risks within the organization, so it's essential to recognize that. Similar to risk management, vulnerability management is an ongoing process of risk reduction rather than a risk prevention effort.

1.4.2.4 Personnel and Processes

The success of a SOC largely depends on the quality of its team and the establishment of effective processes to manage security activities.

- **Design and Establishment of The SOC Team**

  - **Defining the SOC Mission**: It is important to clearly define the mission of the SOC in collaboration with the stakeholders of the organization. This step establishes security priorities and the necessary security services to achieve organizational objectives. The mission should align with the company's strategic goals and describe the core activities that the SOC is responsible for. A well-defined mission also helps identify the responsibilities and roles of SOC team members and guides design and implementation decisions.
  - **Focusing on Security Services to Provide:** The SOC must be designed to deliver specific security services created for the organization. These services include security event monitoring, incident management, vulnerability management, and the collection and analysis of security data. This step helps determine personnel requirements, the necessary skills for various roles, and the processes needed to deliver these services.
  - **Working with the Human Resources (HR) Department:** HR can provide support by creating detailed job descriptions for each role, using effective selection methods, and offering training and development programs to help team members enhance their skills and maintain their certifications. Collaborating closely with HR can secure that the SOC has qualified and competent team members necessary to carry out its missions. Leveraging their expertise in recruitment and personnel management, HR can help build a strong and well-structured team to assure the security of the organization.

- **Processes and Procedures**
  Working with a set of processes and procedures is essential for the success of a SOC, as they help control how SOC services will be delivered.

  It is important to distinguish between processes and procedures and work on both to ensure optimal SOC functioning. Processes are general methods of work that describe how specific tasks and activities should be carried out. Procedures, on the other hand, are detailed and specific descriptions of how a task should be performed.

  The SOC must make use of a number of processes and procedures to guarantee effective security monitoring. It is essential to work closely with enterprise service management processes to ensure that event management, incident management, problem management, vulnerability management, and other IT management processes align with SOC processes. This insures optimal security monitoring efficiency and swift incident resolution. In addition to working with IT management processes, the SOC must also develop its own processes and procedures to ensure effective security monitoring.

  It is essential that SOC processes and procedures are customized to the company's needs and are flexible enough to adapt to evolving security threats. The benefits of processes and procedures lie in ensuring consistent and efficient security monitoring and enabling a swift and appropriate response to security incidents. However, an excess of processes and procedures can slow down incident response time, while a lack of processes and procedures can lead to errors and inconsistencies in security monitoring. Therefore, the SOC must strike a balance to guarantee effective security monitoring while adapting to the company's requirements.

1.4.3 Construction Phase

1.4.3.1 Technology Selection

Selecting the right technologies is essential for building an effective SOC. It is crucial to choose solutions that address the specific needs of the organization in terms of security monitoring, detection, and incident response. This may include tools such as SIEM systems, IDS, EDR solutions, vulnerability management solutions, firewalls, and other security devices.

A thorough evaluation of vendors and available solutions in the market is necessary to make informed decisions and assure seamless integration into the overall SOC architecture.

1.4.3.2 Securing the SOC Network

Securing the network infrastructure is of huge importance and must be a priority. This includes network segmentation, which is one of the key strategies to ensure adequate protection against potential threats. By dividing the internal network into different zones with varying levels of trust, we create barriers and access controls that limit attackers' opportunities for lateral movement and attacks.

To securely connect remote networks and enable the sharing of internal resources, the use of VPNs is recommended. Site-to-site VPNs establish secure tunnels between remote networks, ensuring the confidentiality and integrity of exchanged data. Host-based VPNs provide similar protection for remote users connecting to the SOC's internal network. These solutions enable secure communication while minimizing exposure to potential threats on unsecured networks.

Security for systems and endpoints is also essential, and measures such as hardening, patch management, and intrusion prevention should be implemented to ensure their integrity and protection against threats

1.4.3.3 Storage and Data Protection

SOCs place significant importance on data analysis to detect and prevent threats. This activity involves the massive collection and storage of electronic data containing necessary information for the organization, including personal data related to employees, clients, and partners, as well as other relevant information. Managing and protecting this data is critical to ensure its confidentiality, integrity, and availability.

It is essential to define data backup and restoration procedures, as well as data retention policies that comply with regulatory and industry-specific requirements.

1.4.3.4 Formation and Collaboration of SOC Teams

SOC team members must be trained in the implemented technologies, operational procedures, best practices for detection and incident response, as well as crisis management and communication skills. Regular simulation exercises and incident management drills can be organized to enhance skills and test operational processes in a controlled environment.

Effective collaboration within the SOC is essential to ensure a coordinated response to security incidents. SOC team members should be able to collaborate closely with various groups within the organization, such as human resources, technical support, external vendors, and organizational leaders. The use of collaboration tools, such as email, inter-

nal sites, conferences and file sharing facilitates communication and promotes collective action. These tools should be adapted to the specific needs of the SOC.

1.4.4 Operational and Maintenance Phase

1.4.4.1 Incident Management

When a security incident is confirmed, a swift and coordinated response is essential to mitigate risks and limit potential damage. As Hans Selye aptly put it, "It's not stress that kills us, it's our reaction to stress." This quote underscores the importance of SOC analysts' response to the challenges and stressful situations they face while managing security incidents.

Case management systems (also known as investigation management systems) are used to coordinate investigations into potential and confirmed incidents. Creating an incident case begins with gathering essential information, such as the specific nature of the incident, observed suspicious activities, affected systems or users, and any other relevant data available. It is also important to document the steps taken to contain or resolve the incident, providing a clear record of actions taken.

Once the incident case is created, it is necessary to assign it a priority based on severity and impact on the organization. Best practices involve establishing objective criteria for prioritization, considering factors such as the sensitivity of involved data, the scale of the incident or its potential impact on business operations. This prioritization allows resources and efforts to focus on the most critical incidents.

Maintaining traceability of activities carried out to resolve the incident is essential. Recording the steps performed, outcomes achieved, and decisions made enables tracking the incident's progression, measuring the effectiveness of actions taken, and ensuring that issues are adequately resolved.

Incident case management may also involve collaboration with other members of the SOC team or other departments within the organization. Information exchange and team discussions are essential for sharing knowledge, gaining diverse perspectives, and making informed decisions. Internal communication within the SOC is therefore a key element of incident management.

1.4.4.2 Maintenance, Evaluation, and Enhancement of the SOC

The maintenance of a SOC requires rigorous management and the establishment of continuous improvement processes. These processes help maintain and enhance SOC operations in response to the evolving security needs of the organization.

A widely used model to achieve this objective is the PDCA cycle (Plan-Do-Check-Act). This model consists of four key steps (figure 1.3):

Plan: In this initial phase, the SOC defines its strategy, goals, and objectives. It plans how to implement security measures effectively and efficiently.

Do: During this stage, the SOC puts its plans into action. It deploys security tools, establishes monitoring processes, and responds to incidents as they occur.

Check: The SOC continuously assesses its performance and effectiveness. It evaluates the outcomes of its actions, monitors security metrics, and identifies areas for improvement.

Act: Based on the evaluation in the previous step, the SOC takes corrective actions. It adjusts its processes, updates its tools, and enhances its capabilities to better address security challenges. By following the PDCA cycle, the SOC can continuously assess, adjust, and enhance its operations to align with the organization's security objectives.

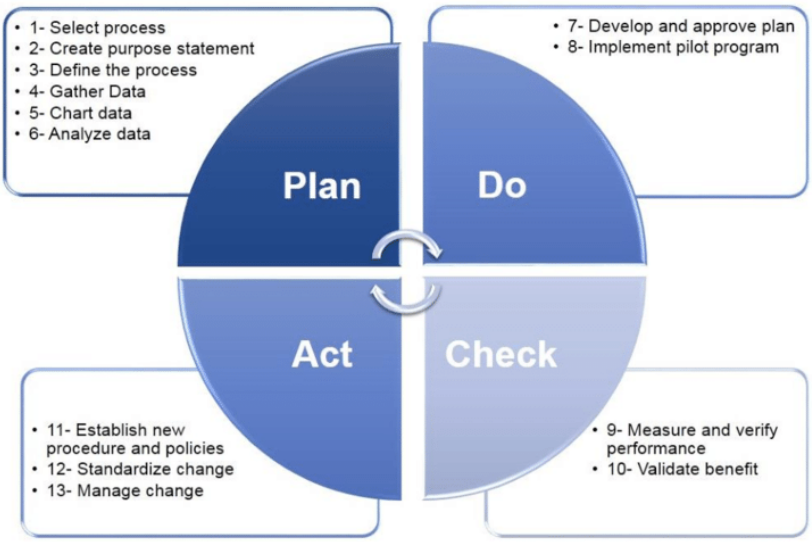

Figure 1.3: The PDCA cycle [1]

This ensures a proactive response to threats, effective incident management, improved SOC resilience, and overall optimization of the organization's security posture.

1.5 Security Information and Event Management (SIEM)

The SIEM system is a complex collection of technologies designed to provide vision and clarity on the corporate. Security professionals and analyst use the SIEM system to monitor, identify, document, and sometimes respond to security affronts. The SIEM system can also identify more elusive security events. A major objective for the security analysts using SIEM system is to reduce the number of false-positive alerts, such as the IDS that is famous for alerting on many false-positive events, that can waste time and energy [3].

1.5.1 Anatomy

SIEM can be compared to a complex machine, in that a SIEM has several moving parts, each part preforming a specific job that need to work properly together or else the entire system will fail [3].

A simple SIEM can be broken down into six separate pieces or processes: source device, log collection, parsing/normalization, rule engine and correlation engine, log storage and monitoring (figure 1.4)[3].

1.5.1.1 Source Device

The source device is the device, application, or some other type of data that an organization wants to retrieve logs from, store and process in the SIEM, the source device is not a part of the SIEM [3].

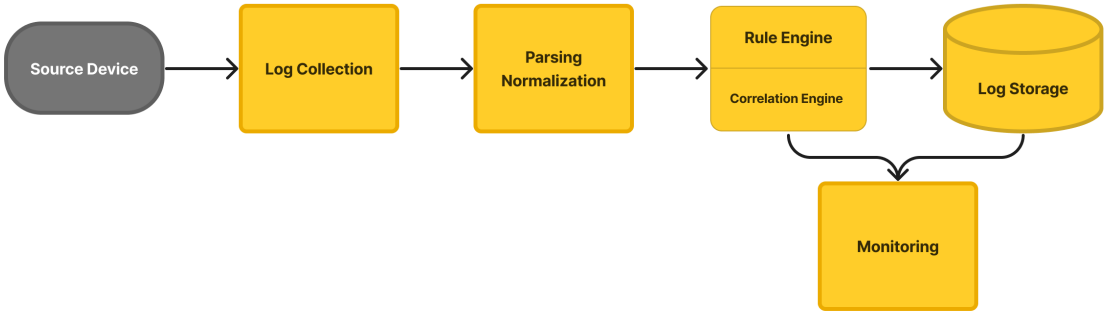

Figure 1.4: Anatomy of a SIEM [3]

1.5.1.2 Log Collection

It's how to get all these different logs from their native devices to the SIEM, the log collection processes can be broken down into two fundamental methods of collection:

- **Push Method:** the source device sends its logs to the SIEM. it's easy to setup and configure, setting up a receiver and then pointing the source device it's enough (for example, syslog).
- **Pull Method:** the SIEM reaches out and retrieves the logs from the source device, the SIEM is the one that initiates the connection to the source device and actively retrieves the logs from the source device, for example the logs are stored in flat text files on a network share.

Most environments will have more than one device, which means that will need multiple methods of log collection are needed, combine devices to use the same collection methods and, therefore, minimize the number of methods being used for log collections [3].

1.5.1.3 Parsing/Normalization of Logs

Normalization is an act of changing all these different types of logs into a single format, all the logs from devices look the same in the SIEM. Normalization of the events does not only make it simpler to read logs, but allows for a standers format of rule generation [3].

1.5.1.4 Rule Engine/Correlation Engine

The rule engine expands upon the normalization of events from different sources in order to trigger alerts within the SIEM due to specific conditions in these logs. The SIEM rules usually starts off fairly simple, but can become extremely complex, the rules are writing in a form of Boolean logic to determine if specific conditions are met and examine pattern matching within the data fields. The correlation engine is a subset of the rule engine, it matches multiple standard events from different sources into a single correlated event, it's used to simplify incident response procedures [3].

1.5.1.5 Log Storage

To work with the logs that come into the SIEM, they are stored for retention purposes and historical queries.The storage of logs in a SIEM system can be achieved through three distinct methods: database, flat text file, or binary file [3].

1.5.1.6 Monitoring

This is a method of interacting with the logs stored in The SIEM, SIEM will have an interface console (web-based or application-based) that allows to interact with the data stored in the SIEM, and manage the SIEM [3].

1.5.2 Solutions in The Market

There are several SIEM solutions available in the market, each offering unique features. Some of the well-known ones.

- **Splunk:** offers a comprehensive set of features, including real-time monitoring, event correlation, threat detection, incident response, compliance reporting, and user behaviour analytics. It is known for its scalability, flexibility, ease of use and extensive integration capabilities. It supports integration with a vast ecosystem of third-party tools, technologies, and threat intelligence feeds.[24]
- **IBM QRadar:** provides robust features for log management, threat detection, incident response, and compliance reporting. It includes advanced analytics, threat intelligence integration, and user behaviour analytics capabilities. It also offers a complex platform with a wide range of features which may lead to a steeper learning curve compared to other solutions. It integrates well with other IBM security products and third-party solutions.[25]
- **Elastic:** offers features such as threat detection, centralized log management, security analytics, and machine learning powered anomaly detection. Elastic SIEM is known for its ease of use and seamless integration with other components of the Elastic Stack, such as Elasticsearch, Kibana and Beats. It offers a user-friendly interface and provides extensive documentation and community support.[26]

The use of the SIEM solutions depends on the needs and capacity of the organization. The table below shows the advantages and inconveniences of the SIEM solutions.[27] [28]

We chose Elastic Security as our SIEM solution, because it provides a robust SIEM

Table 1.1: Comparison between the SIEM solution in the market

solution that empowers security teams to detect, investigate, and respond to evolving, we will now explain its capabilities [26]:

- **Open-source solution:** Elastic is an open-source solution, which means it is free to download and use. Organizations can save significant costs compared to proprietary SIEM solutions.
- **Easy Integration:** Elastic seamlessly integrates with many common security tools, such as firewalls and antivirus solutions. Data from these tools can be aggregated and analyzed using Elastic to provide comprehensive visibility into the security of the entire network.
- **Ease of Use:** Elastic provides an intuitive user interface for visualizing security data. Kibana, Elastic's data visualization interface, allows users to create custom dashboards to monitor real-time security events and visualize trends over time.

Solution	Advantage	Disadvantage
IBM QRadar	• Suitable for mid to large-scale industries. • Easy to deploy. • Automates threat detection and prioritization. • Complex algorithms to calculate and prioritize threats.	• Lack of adequate pricing information. • Integration is not as broad as Splunk's. • Absence of free trial. • Not suitable for small organizations. • Steep Learning Curve.
Splunk	• Robust log analysis for effective management features. • Automated risk-based alerting. • Free training courses and certifications. • Free trial available.	• Not easy to deploy. • Lack of adequate pricing information. • Not suitable for small organizations.
Elastic	• Excellent for search and analytics use cases. • Open-source and free trial for premium plans. • Adaptable to all organization sizes. • Scalable and highly flexible. • Over 300 integrations for data ingestion.	• May require additional components for full SIEM functionality. • Steep learning curve.

- **Advanced Data Analysis Features:** Elastic is capable of analyzing large amounts of real-time log data to detect suspicious activities. Elastic's advanced data analysis features, such as anomaly detection and event correlation, enable organizations to quickly identify abnormal behaviors and take preventive measures.
- **Scalability Over Time:** Elastic's scalability ensures that management tools can grow and adapt as organization increase in complexity and size. Elastic can handle the extra load whether it's data storage, processing power, or user traffic.

1.6 Incident Response (IR)

The IR program is a subset of the organization's overall security program that deals with unexpected violations to the policy defined as "acceptable and expected use" of the IT systems. The primary goal of an IR program is to develop a team, infrastructure, and procedures to identify security breaches quickly and then to adjust the IT environment rapidly to minimize or halt the losses of IT assets, while also minimizing the impact on the organization's primary objectives (like keeping the revenue-generating functions operational). Ideally, this means the IR team must stop the security breach or attack without slowing or shutting down the organization's main functions.[3]

Responding to incidents starts by first detecting that an incident has actually occurred and is within the scope assigned to the security operations team.[1]

Preparing a SOC to manage incidents extends to cover people, processes, and of course, technology. For example, a SOC is usually expected to educate users about how they must

report security incidents and keep informed of the channels available for users to report what is perceived as a security incident.[1]

1.6.1 The Timeline

A typical incident-handling process follows the list of steps presented in the incident response (IR) timeline(figure 1.5).[1]

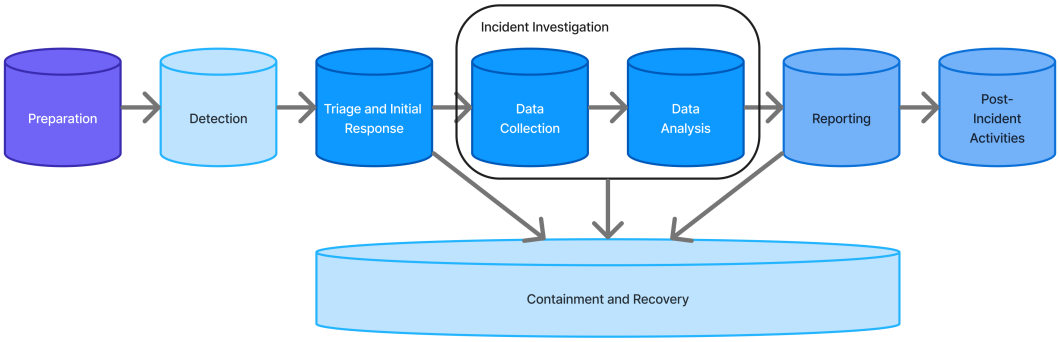

Figure 1.5: Incident Response Timeline [1]

1.6.1.1 Incident Detection

Detection refers to the phase in which an incident is observed and reported by people or technology, and the process that handles the reporting aspects.

1.6.1.2 Incident Triage

Incident triage represents the initial actions taken on a detected event that is used to determine the remaining steps according to the incident response plan. The triage phase consists of three sub-phases: verification, initial classification, and assignment.

The triage process needs to be developed to prioritize incidents and move them along the incident response timeline to be analyzed and eventually conclude with some form of resolution.[1]

1.6.1.3 Incident Resolution

The life-cycle of an incident should eventually lead to some form of resolution, this may include data analysis, resolution research, a proposed or performed action and recovery. The objective of this phase is to discover the root cause of the incident, while working on containing the incident at the earliest stage possible.

During the analysis phase, the SOC team and the other teams should collaborate to achieve the quickest and best form of resolution.

The containment phase involves the actions performed to quickly stop a computer security incident from escalating or spreading to other systems, the containment phase can happen before, during, or after the analysis phase.

1.6.1.4 Incident Closure

Closing a computer security incident refers to the eradication phase in which vulnerabilities that lead to the incident have been closed and all the incident traces have been cleansed. The closure process also includes testing systems to ensure that the eradication steps and controls were effective and that the vectors used by the attack do not exist anymore or are ineffective. Predefined actions to consider include applying any final information about the event, its final classification, any external notifications, and archiving information about the incident.

If the incident involved violating regulatory requirements or resulted in the infringement of law, the SOC might be obliged to notify external entities.

1.6.1.5 Post-Incident

This is the *"lessons-learned"* phase in which it is desired to improve the IR processes and reflect on other people, processes, and technology controls. Post-incident activities will vary depending on the severity of the computer security incident. Valuable knowledge gained from computer security incidents can be useful to prevent/mitigate future incidents in the form of proactive services such as enhancing security features of functions within defenses.

There exists several incident response plan templates provided by security organisations, and for the most part they follow the same methodology except for a few differences.

1.6.2 The NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a set of guidelines for mitigating organizational cybersecurity risks. It was published by the U.S. National Institute of Standards and Technology (NIST) and is based on existing standards, guidelines, and practices. The purpose of the these guidelines is to improve cybersecurity and risk management at an organizational level. One of them is the NIST incident response process used to identify and manage cybersecurity incidents.

The NIST framework integrates industry best practices and real-world situations, providing a comprehensive approach to incident response from preparation to post-incident activities.

1.7 Conclusion

In this chapter, we covered various aspects of information security. Then, we focused on the SOC, highlighting its Services, central components and set-up methodology. Then, we explored the SIEM technology, its anatomy, the most popular SIEM solutions that exist in the market and why we chose Elastic.

Chapter 2

Design of The SOC Solution at MNA Group

2.1 Introduction

In this chapter, we will begin by first summarizing the SOC set-up methodoly. After that, we will describe the host organisation MNA Group, its goals and its network architecture. Then, we are going to analyse its security needs. Next, we will present and explain our proposed solution and its technologies and architecture. Finally, we will detail the different SOC processes including incident response, log retention and rule detection creation fallowing with the list of the detection rules that has been created.

2.2 The SOC Set-Up methodology

the main objective of this project is to develop a SOC for the host organization "MNA Group". In this context, we identified these pillars of SOC which are shown in the figure bellow:

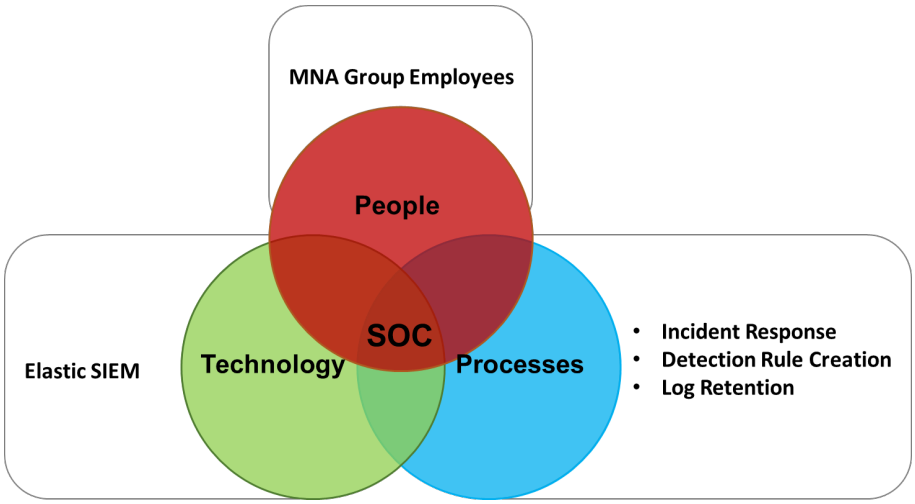

Figure 2.1: The pillars of SOC in MNA Group

We used the SOC set-up methodology that was mentioned in the first chapter, we will highlight the most important points to design and implement the SOC in MNA Group in the following table 2.1.

Phase	Step	Established work
Plan phase	**Identification of the organisation's goals**	**Business goals :** • Offer cybersecurity and governance advices and strategies • Cyber resilience and crisis management • Support the cybersecurity function • Management of cybersecurity risks • Cybersecurity audits **IT goals:** • Protection of sensitive client and company documents and data. • Infrastructure protection and prioritizing safeguarding critical components. • Availability for clients across all communication channels. • Continuous enhancement of security solutions and updating.
	Existing security measures	• Endpoint detection and response (EDR Sophos) • Firewall (Sophos XG firewall) • Access control with active directory • Server racks locks • Security cameras and door locks
	Information collection	• **Access control policy:** outlines user permissions, authentication methods, and authorization controls. • **Infrastructure protection documentation:** covers security configurations, access controls, and monitoring practices. • **Availability policies:** defines response times, service level agreements (SLAs), and uptime requirements. • **System description document:** includes architecture diagrams, components, and interconnections. • **Risk assessment reports:** assesses impact and likelihood of security incidents. • **Network diagrams and topology maps:** helps identify critical points, communication paths, and potential weaknesses.
Design Phase	**Infrastructure design**	• **Integration with Existing Employees:** due to the small size of the organization, managing the SOC can be seamlessly incorporated into the daily tasks of existing employees. • **Efficient Task Execution:** the SOC team is adept at efficiently handling their tasks using their own workstations, without relying on specialized workstations for SOC-related activities. • **SIEM Server:** handle the Elastic SIEM components (Elasticsearch and Kibana) along with reverse proxy and host firewall. • **Syslog Server:** configure with syslog server to collect the events from network devices like firewall and routers.
	Network design	• **Enhanced Infrastructure:** an additional server has been introduced specifically to manage the SOC operations. • **Isolated Network Segment:** this server operates within its own VLAN, ensuring a secure and segregated environment. • **Dedicated IP Addresses:** each workstation within the SOC team has its own unique IP address, facilitating efficient communication and management.
	Generation and collection of security events:	• Operating systems (windows, Linux) • Directory service (active directory) • Applications (Nginx, Dockers) • Network (firewall, NIC) • Cloud (Sophos central) • Files integrity

	Personnel and processes	**SOC team:** • SOC analyst L1: junior consultant • SOC analyst L2 : senior consultant • SOC manager: Cybersecurity manager • In addition, the network administrator and HR can help managing the SOC in some cases. **Processes and Procedures:** leveraging the NIST framework, playbooks and runbooks were specifically tailored for incident response. These comprehensive guides ensure a swift and effective approach when addressing security incidents.
Construction Phase	**Technology selection**	SIEM solution using Elastic Stack: • **Elasticsearch:** handles data storage and correlations, allowing efficient retrieval and analysis of security-related information. • **Kibana:** provides powerful data visualizations, aiding in understanding trends, anomalies, and patterns. It also assists with agent configuration. • **Elastic Agent:** responsible for data collection and normalization from various sources, ensuring consistent and structured data for analysis.
	Security of the SOC network	• **Access Control with Reverse Proxy:** access control using white list of subnet of the SOC team, ensuring secure and controlled access to SIEM services. • **Host Firewall for SIEM Server and Syslog Server:** the servers are fortified with a host firewall managed, safeguarding it from unauthorized network traffic. • **SSH Key-Based Authentication:** to enhance security, SSH connections are allowed exclusively through key-based authentication.
	Storage and data protection	• Encryption and access control to safeguard storage and sensitive data. This ensures confidentiality, integrity, and resilience against unauthorized access. • Article 11 of Law No. 09-04 of 14 Chaabane 1430, corresponding to August 5, 2009, concerning the prevention and fight against offenses related to information and communication technologies, stipulates that data retention duration is set at one (1) year.
	Formation and collaboration for the SOC team	• ISO 27001 LI & LA • ISO 27005 RM • ISO 27032 CM • EBIOS RM • CCNA certificate • CLEH (Certified Lead Ethical Hacker)
Operational and maintenance phase	**Incident management**	• **Kibana Cases for Case Management:** implemented a robust case management system using Kibana **Cases**, allowing efficient tracking and resolution of security incidents. • **Incident Response Playbooks and Runbooks:** comprehensive playbooks and runbooks were created for efficient incident response. These guides ensure a swift and effective approach when addressing security incidents.
	Maintenance, Evaluation, and Enhancement of the SOC	Using the Plan-Do-Check-Act cycle (PDCA) in all the processes of the maintenance, evaluation, and enhancement of the SOC: • Creation of new detection rule process

Table 2.1: The SOC Set-Up in MNA Group

2.3 Presentation of The Host Organization (Planning Phase)

Mare Nostrum Advising Group (MNA Group) is a renowned company in the field of information security. Equipped with a team of highly qualified and experienced professionals, it stands out for its specialization in cybersecurity auditing, consulting and support [29].

MNA Group also has a dedicated and QUALIOPI-certified, structure known as "MN Advising Cert", which provides high-level training programs. Leveraging their expertise and appropriate tools, the company's consultants effectively train employees of client organizations, enhancing their information security skills [29].

2.3.1 The Organization Goals

There exists two type of goals, business goals and IT goals, all organizations define and try to achieve those goals. In MNA Group those goals are:

2.3.1.1 Business Goals

Business goals are the desired outcomes that an organization aims to achieve within a specific time frame. These goals help define the purpose and direction of the company, guiding decision-making and resource allocation. MNA Group provides these services to other companies:

- Cybersecurity and governance advices and strategies.
- Cyber resilience and crisis management.
- Support the cybersecurity function.
- Management of cybersecurity risks.
- Cybersecurity audits.

2.3.1.2 IT Goals

IT goals are specific business objectives that aim to upgrade and enhance the operations within an organization's IT department. These goals are typically part of the IT governance framework and align with and support the broader goals of the organization.

- Protection of sensitive client and company documents and data, prioritizing safeguarding information, ensuring the utmost security for both client and company data.
- Infrastructure protection and prioritizing safeguarding critical components such as servers and workstations, ensuring their resilience and security.
- Availability for clients across all communication channels ensure seamless accessibility for the clients through various communication channels, including email, phone, and online meetings.

- Continuous enhancement of security solutions, commitment to constantly updating and improving security solutions and ensuring robust protection against emerging threats.

2.3.2 Existing Security Measures

Like any organization, MNA Group must be provided with security measures to protect it's business from any type of attacks and can affect their images and infrastructures, this is list of what they have:

- **Sophos EDR:** each workstation is integrated with a EDR that monitors, detects and prevents threats in real time. The EDR sends its logs to Sophos central where they are stored and analysed.
- **Sophos XG firewall:** product provided by the company Sophos, it serves as a first line of defense against external threats, which is a stateful firewall that can be managed and configured in a platform with other Sophos products(Sophos EDR).
- **Access control with active directory:** used for managing user accounts, permissions, and access control in a Windows-based network environment, it use Group policies (GPOs) and role-based access control (RBAC).
- **Servers racks locks:** protecting valuable hardware and sensitive data, using locked rack cages provides an additional layer of physical protection against tampering and unauthorized access.
- **Security cameras and door locks:** security cameras with door locks provides enhanced safety and convenience for the company location (building)

2.3.3 MNA Group Network Architecture

The figure below describes the network architecture and its main components:

- **Sophos XG firewall:** a product provided by the company Sophos, it works also as Router (connected with the Router provided by the ISP) to connect with the external network(Internet).
- **Sophos central:** is a platform provided by the Sophos company for its clients to manage and configure their products remotely. It can store and manage the logs sent by the EDRs and firewall.
- **Active directory:** Windows server 2022 is used to share data over the network and manage employees user accounts.
- **Test server:** the test server exists to examine and check new configurations and/or malware analysis.

all the workstations access the network through an access point while the Active Directory server uses a switch, both are connected directly to the firewall. The purpose of this separation is segmenting the network.

The organization has a network document that contains the network diagram and all the information about the devices and their configurations.

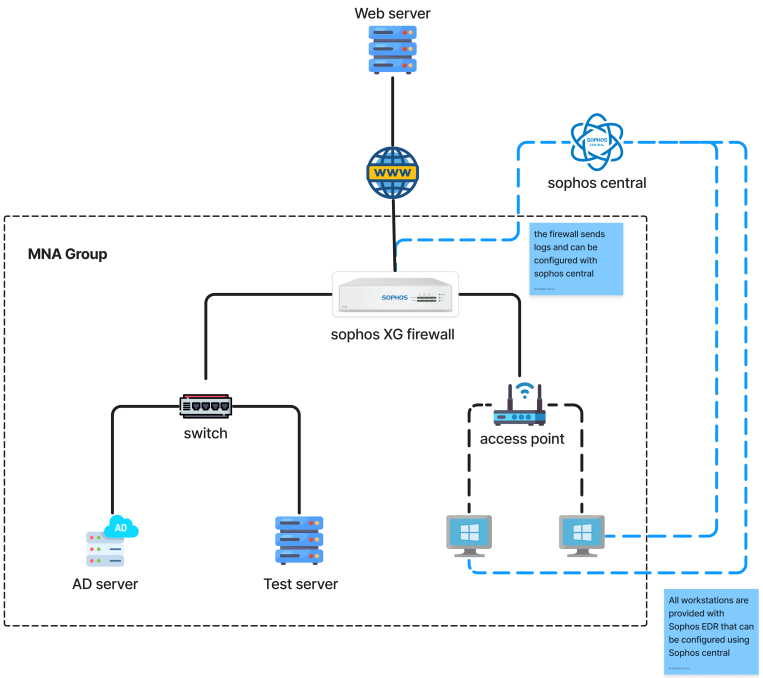

Figure 2.2: MNA Group network architecture diagram

2.3.4 Security Needs Analysis

MNA Group already has several defense measures in place, including a Sophos XG firewall and Sophos EDR solution, which serve as a first line of defense to protect their infrastructure. Firewalls default configurations often allow all outbound traffic, are weak against attacks from the intranet itself and can't prevent Application Layer threats like SQL injection or weak SSH passwords. EDR solutions focus on protecting endpoints and not the whole network. The main objective is having a center to manage the current security solutions and provide maximum protection to the organisation from threats the available solutions can't detect.

Our proposed solution to the organization is setting up a small SOC with a SIEM and incident response processes. The implementation of a SOC within MNA Group will significantly strengthen its security posture. A SOC will ensure real time monitoring of network connections, user activity, unauthorized access attempts and abnormal behaviors. This approach will allow for the rapid detection of any suspicious or malicious activity, effective incident response, and continuous security improvement, which will strengthen customer trust and MNA Group's reputation as a service provider specializing in information security.

2.4 SOC Team Assignment (Design Phase)

Given the modest scale of the organization, comprising merely of 10 to 15 employees, the SOC team responsibilities may be integrated into the routine tasks of the current staff utilizing two SOC Analysts (level 1 and level 2) and a SOC Manager. By allocating all duties among them, the Network Administrator and Human Resources personnel can

provide assistance in certain scenarios (table 2.2).

Role	Name	Email/Phone	Responsibilities
SOC Analyst L1			• Monitors SIEM alerts, manages and configures security-monitoring tools. • Prioritizes and triages alerts and issues to determine whether they are real security incidents or not (false positives). • Correlates with threat intelligence to identify the threat actor.
SOC Analyst L2			• Receives incidents and performs deep analysis. • Defines and executes on strategy for containment, remediation, and recovery. • When a major incident occurs, teams with the Level 2 Analysts are responsible for responding to and containing it. • Conducts vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence, and security data.
SOC Manager			• Responsible for hiring and training SOC staff, in charge of defensive and offensive strategy. • Manages resources, priorities and projects, and manages the team directly when responding to business-critical security incidents.
Network Administrator			• Network setup and maintenance • Troubleshooting and issue resolution. • User account management. • Policy and procedure development.
HR			• Designing workplace policies. • Keeping track of external factors that affect the organization and its employees, like the use of technology, global developments, social media networking, etc...

Table 2.2: SOC Team Assignment and contact at MNA Group

2.5 Presentation of the SIEM Solution (Design and Construction Phase)

In this section, we will describe in a general manner the architecture, workflow of the SIEM and explain our choice of runtime environment of each component, then summarize the integrations and SOC analysts daily work.

2.5.1 SIEM Architecture

All the main components of the architecture, including source devices (workstations, firewall, Sophos Central, AD server), SIEM servers (SIEM server and Syslog server) and SOC process documents, along with descriptions and reasons for their necessity in our solution:

- **Workstations:** each workstation is installed with an Elastic Agent to collect the system and user activity logs. They also have Sophos EDR, which automatically

sends its logs to the Sophos central platform. All the workstations have the same policy.

- **Active directory server:** Active directory is an integral part of windows server 2022, configured with all workstations for authentication and sharing files. The logs generated by the active directory are regarded as Windows system logs and are collected along the system logs. This server has its own policy.
- **Sophos firewall:** is configured as a syslog client to send its logs to the syslog server that is installed and configured in the Syslog server.
- **Sophos Central:** using the API key provided by the Sophos platform, Sophos central sends the logs generated from the workstations EDRs to the agent using the special integration Sophos central.
- **SIEM Server:** the Elastic Agent that's implemented in the SIEM server collects the logs of the operating system , the containers and the reverse proxy server.
- **Syslog Server:** the logs are sent from the firewall and sophos central to this server, where they will be collected and sent to Elasticsearch by the agent.
- **SOC Process Documents:** detail the actions that need to be taken in the case of an incident, the process of creation of detection rules and log retention.

2.5.1.1 Syslog Server Technologies

This server is built with good storage to receive and store the huge amount of data coming from the firewall and EDRs. The syslog protocol is used for logging and monitoring network devices and servers. It consists of the following components:

- **Syslog Client (Sender):** a device or application that generates log messages.
- **Syslog Server (Receiver):** a centralized server responsible for receiving and storing log messages from multiple clients, in this case will be the Syslog server.
- **Syslog Message:** the log message itself, following a specific format consisting of a priority value, timestamp, hostname, and the actual message.

2.5.1.2 SIEM Server technologies

we added this server specifically to host Elasticsearch and Kibana, it's main characteristics are its processing power, abundant memory and spacious hard drive. The reason for having a strong processing power and a large memory is to handle Elasticsearch's demands, the large storage is for the massive amount of data saved in Elasticsearch. For Elasticsearch and Kibana, we chose for runtime environment containers. A container is a standard unit of software that packages up code and all its dependencies. It allows applications to run quickly and reliably across different computing environments. This choice comes with many advantages, some of them are:

- **Isolation and Consistency:** containers provide isolation for Elasticsearch and Kibana, ensuring that they don't interfere with each other. Each one has its own file system, libraries, and runtime environment.

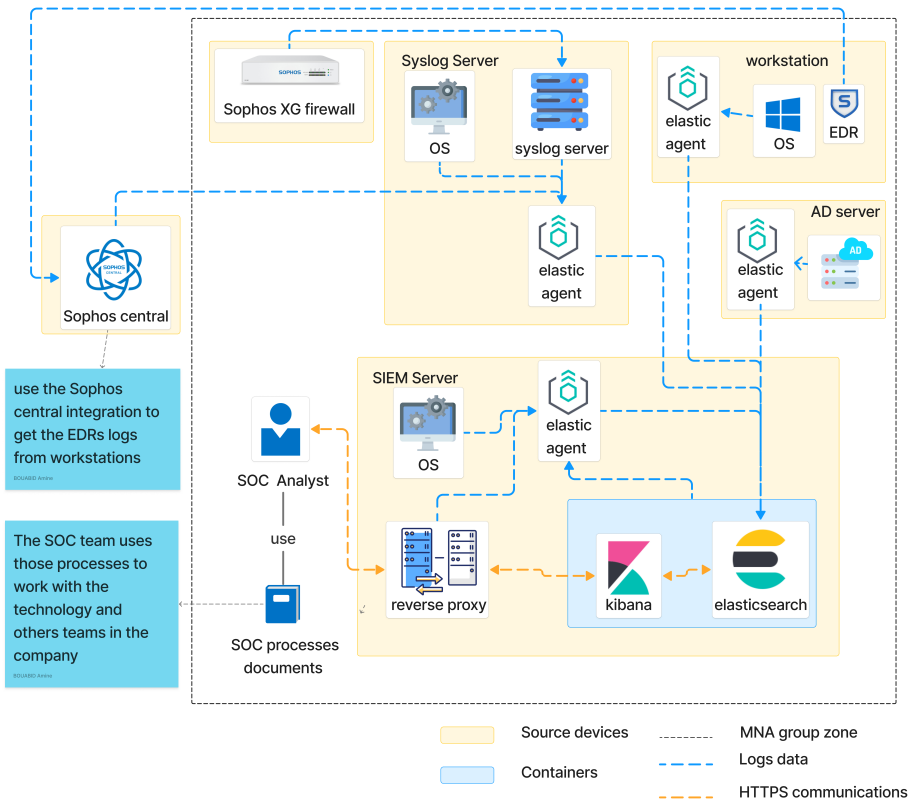

Figure 2.3: Elastic SIEM architecture in MNA Group

- **Portability:** containers encapsulate an application and its dependencies, making Elasticsearch and Kibana highly portable. This also means that more instances within the same machine of them can be created if needed.
- **Fast Deployment and Scaling:** containers start quickly, allowing to deploy and scale the applications rapidly. Containers enable seamless scaling up or down based on demand.

In order to enhance the security, speed, and reliability of the connection between the users (SOC team) and the SIEM server (Elasticsearch and Kibana), as well as to ensure future scalability and mitigate single points of failure, a reverse proxy server was deployed and configured. This addition was made to our architecture to leverage the following benefits:

- Reverse proxies shield backend servers from direct exposure. In the case of server shutdown, the proxy automatically redirects user requests to the next available server.
- Sensitive data and services remain hidden, as the proxy forwards only authorized requests, which provides an additional layer of security by filtering and controlling incoming traffic.
- A Reverse proxy allows for dynamic scaling by adding or removing servers based on traffic volume, which makes them available and optimized without interruptions during scaling events.

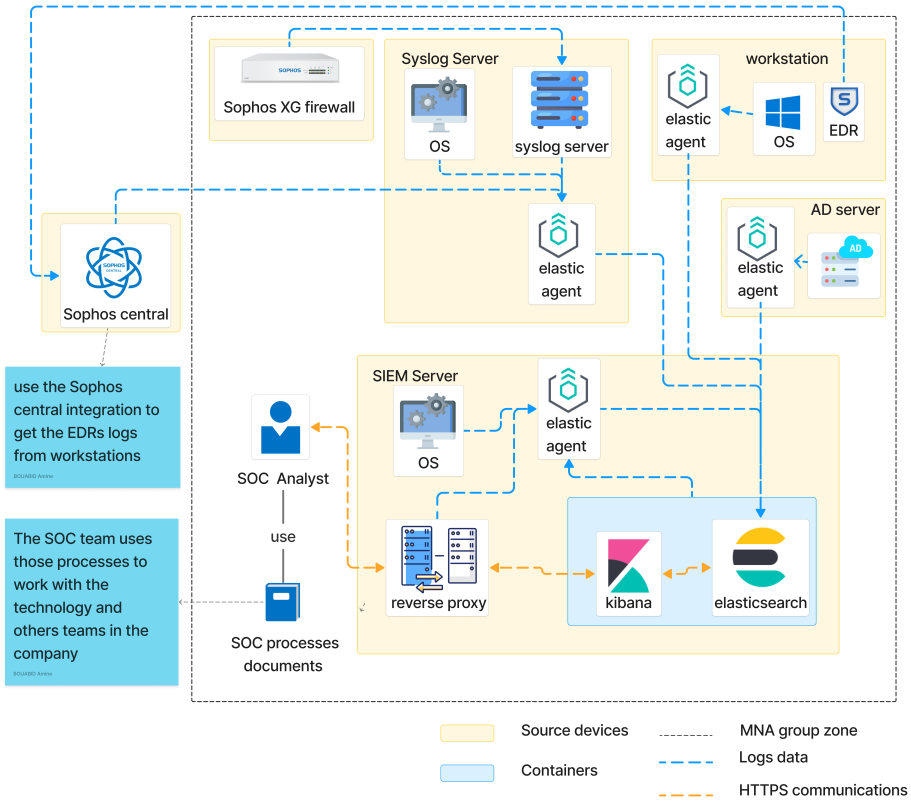

Figure 2.4: Elastic SIEM architecture in MNA Group

2.5.2 Elastic Stack as SIEM

The figure 2.5 describes how the Elastic stack[1] works together to form a SIEM

- **Source devices:** when considering the primary sources of logs within an organization, the firewall and workstations emerge as essential entities for the collection and analysis of their respective logs. The firewall works as a central channel through which all network traffic traverses, while workstations represent crucial components supporting the organization's services. These entities are frequently exposed to security breaches originating from both external and internal sources. Additionally, the integration of servers as log sources is deemed necessary to fortify the overall SIEM framework.

- **Elastic Agent:**the primary responsibility of the Elastic Agent involves the collection of logs from various devices, based on specific configurations determining the types of logs to be gathered. After that, the agent is required to process and standardize the accumulated logs into a unified format pre-defined by Elastic ECS(Elastic common scheme) before transmitting them to Elasticsearch.

- **Elasticsearch:** is a distributed search engine deployed for the purpose of searching and consolidating a vast volume of data (logs). It serves as a platform for storing JSON documents, with or without a predefined schema, thereby facilitating the handling of unstructured data. It is equipped with a detection mechanism that

[1]Elastic Stack is Elastic products (elasticsearch, kibana and Elastic Agent)

employs rules to facilitate the identification of threats and anomalies. These rules are capable of correlating one or multiple logs to ascertain whether alerts should be generated or not. Elasticsearch relies on restful APIs that utilize the JSON format for the purpose of interacting with other components.

- **Kibana:** provides the interface and functionality for the other Elastic solutions, in addition to administration and management options for the core components Kibana also has other features such as Discover, Visualize, and Dashboards that can be used to explore, interrogate, and visualize the data provided by Elasticsearch.
- **SOC analysts:** employ specialized workstations to enable efficient access, monitoring, and supervision of the SIEM components. Upon the generation of an alert, they analyse the logs responsible for the alerts to ascertain the legitimacy of the alert. They use the SOC documents as a reference to guide them through incident response and other processes.
- **SOC Documents:** detail the processes and policies used by the analysts which include playbooks and runbooks for malware outbreaks and network attacks using the NIST framework, log retention and rule detection creation processes, as well as network diagrams and topology maps, infrastructure protection documentation and other documents.

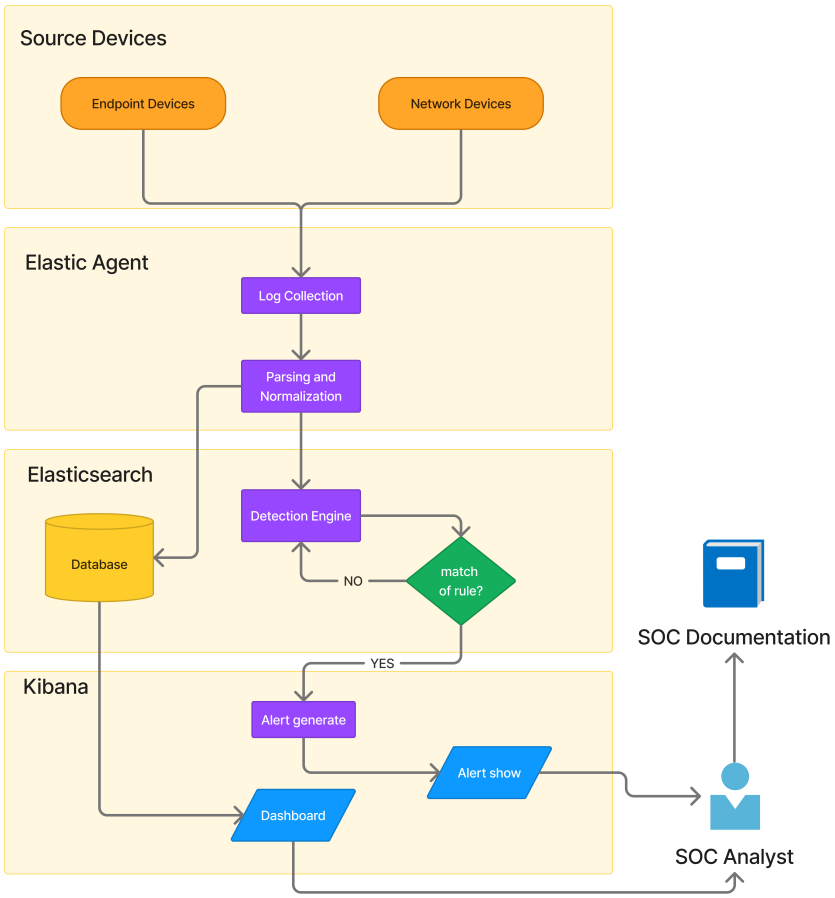

Figure 2.5: Flowchart of Elastic stack as SIEM

2.5.3 Policy Configuration Set-Up

The figure 2.6 describe how Elastic Agents policies are configured and managed, few concepts related to it should be explained:

- **Integration:** are light applications that decide the data that is collected from agents, each integration collects from a specific application or system, for example the Windows integration collects only the logs of the Windows operating system.
- **Policy:** instead of setting integrations for each agent, all integrations needed are Grouped into a policy. An agent policy is a configuration file that contains all the integrations specified for the agent to collect and send data to Elasticsearch. A single policy can be applied to multiple agents and differs with the role of the user or the device type.
- **Fleet:** is a special mode of Elastic Agent(integration) is needed to send the policies to all agents, this mode is called the fleet server. The fleet server is composed of 2 components:
  - **Fleet UI:** is a kibana application with a user interface for users to unboard and configure , administer agents and manage data.

  - **Fleet Server:** is a back-end component that Elastic Agent can connect to, to retrieve agent policies, updates and management commands.

This configuration is mainly composed of two steps: **A: policy settings and deployment** and **B: data collection, storage and display**

- **A1:** the SOC team uses the fleet UI to create the policies needed for every Group of users or machines. Each policy needs to contain all of the needed integrations and their correct configurations to avoid any data loss or unnecessary data. A separate policy needs to be created for the fleet server that contains the fleet server integration. Then, each agent must be assigned his policy.
- **A2:** Kibana then must send the policy configurations to Elasticsearch, these configurations are saved and sent if requested by the agents.
- **A3:** before distributing the policies to the Elastic Agents , the fleet server must configured and assigned his policy and running healthily. Elasticsearch sends the policy of the agent. The agent has the Fleet Server integration which requires Elasticsearch to send all the policy configurations of the agents enrolled in the fleet to the Fleet Server.
- **A4:** the agents must be installed in the machines and enrolled in the fleet and running healthily. the policies will be sent to their agents and each agent will begin collecting the logs specified by the integrations and sending them to Elasticsearch.
- **B1:** the agents will send the logs precised by their policies to Elasticsearch, after which Elasticsearch will store and index them, apply them to detection rules.
- **B2:** there is constant communication between Kibana and Elasticsearch using restful-APIs. Kibana provides different dashboards for integrations and detection and response.
- **B3:** the SOC analysts must confirm that all agents are sending all the logs specified by their policies. When it is confirmed that the SIEM is running without problems, the analysts can start their usual tasks of monitoring and analysing the logs, and checking for alerts.

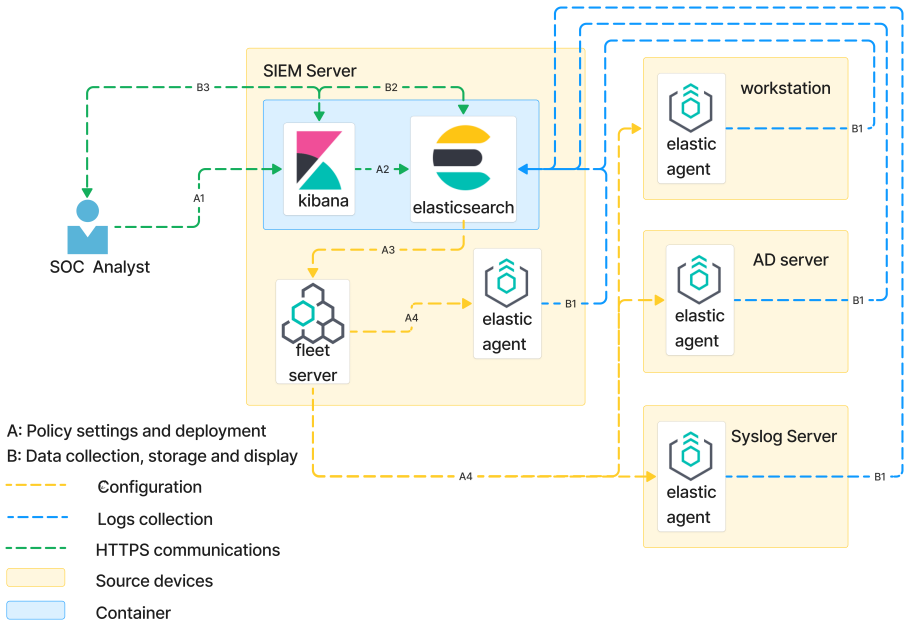

Figure 2.6: Elastic SIEM policy configuration

2.6 Development and Management of SOC Processes (Operating Phase)

2.6.1 Incident Response Management

To ensure effective management of security incidents, we have implemented an incident response process. The objective of this process is to provide clear guidelines to the MNA Group SOC team on how to handle security incidents efficiently. This process is based on best practices defined by the NIST Computer Security Incident Handling Guide framework. The key aspects of this framework:

- **Preparation and Prevention:** establishing policies, procedures, and tools to prevent and respond to incidents, also focusing on proactive measures to minimize risks and enhance security posture and consider preventive actions such as vulnerability management, access controls, and security awareness training.
- **Detection and Analysis:** identifying and assessing the nature and scope of incidents, monitor systems, logs, and network traffic for signs of suspicious or malicious activity, and analyzing incident-related data to understand the impact and severity.
- **Containment, Eradication, and Recovery:** isolating and containing the threat to prevent further damage, removing the threat from affected systems (eradication) and restoring normal operations (recovery) while ensuring the integrity of systems and data.
- **Post-Incident Activity:** reviewing and learning from the incident response process and implementing lessons learned to improve future incident handling.

To optimize response time during incidents, we have developed specific incident response posses documents for two critical incident types at MNA Group: malware incidents,

DoS/DDoS attacks and social engineering attack, Additional information on the created incident response documents are found in the **annex A** section **Incident Responses Document**.

2.6.2 Log Retention Process

In parallel with the incident response process, we have also established a log retention process. This process ensures the backup and restoration of logs using Elastic. It guarantees appropriate storage and preservation of logs generated by various systems and devices within the MNA Group infrastructure. The logs are centralized and securely stored in accordance with data retention policies and relevant regulations.

In the event of log restoration needs, we have a clear procedure that describes the steps to retrieve data from backups and restore it. This procedure is regularly tested and validated to ensure a reliable and swift log restoration in case of incidents or investigative requests.

A document was created to detail the process of creating a log retention policy and repository, and demonstration of that in MNA Group SOC, the information on the document can be found in the **annex A** section **Log Retention Document**.

2.6.3 Detection Rules Creation Process

Along with the other processes, we also established the process of creating detection rules in Elastic Security Solution. Identifying threats and anomalies can be accomplished through various methods, of which the following are accessible within the Elastic security:

- **Defining The Rule Type:** elastic SIEM supports the following rule types for detections:
  - **Custom Query:** custom query detections can be used to search for a specific activity, although detections can run across multiple data sources, the actual activity must be limited to a single event. Kibana query language (KQL) is used in this type of detection where a single log is enough to trigger an alert.
  - **Event Correlation and Sequence Detection:** this type of rule is used in case the detection requires a chain of events within a single or multiple data sources. The detection uses a query language called Event Query Language (EQL) in this case.
  - **Threshold:** this type of rule is used to detect when a single event has occurred several times within a specified time window (e.g., bruteforce). Like custom queries, KQL is used to define the event of interest but it's also required specifying the number of events generated and the time window .
  - **Indicator Match:** is used primarily to detect indicators of compromise (IOC).[2] A threat intelligence module is used to match with the logs of the environment (e.g., malicious IP addresses, websites...). This type of detection uses KQL and the specified field from the threat intelligence API and its match from the environment.
  - **Machine Learning:** machine-learning rules are used to look for changes in standard behaviour in the environment and detect malicious behaviour. Using

[2] An IOC refers to evidence of malicious activity that can be used to identify whether a breach occurred and the severity and extent of the compromise.

machine learning jobs can alert analysts to such activity without having to create and maintain many low-fidelity detection rules.[3]

- **ES|QL:** uses Elasticsearch Query Language (ES|QL) to query the source events and aggregate event data. Query results are returned in a table with rows and columns. Each row becomes an alert.

- **Configuring Basic Rule Settings:** such as the rule name, a description of what the rule does, and severity level of alerts created by the rule.
- **Configuring Advanced Rule Settings (Optional):** this step includes adding specific conditions, a list of common scenarios that may produce false-positive alerts, relevant MITRE framework tactics, techniques, and sub-techniques, or additional filters.
- **Setting Up The Rule's Schedule:** defines how often the rule should run with an additional look-back time(e.g., every 5 minutes and look-back 1 minute).
- **Setting Up Alert Notifications (Optional):** notifications are sent via other systems when alerts are generated, like who should receive alerts when the rule is triggered and connector type.[3]
- **Setting Up Response Actions (Optional):** this process defines the automated actions to take when the rule detects an issue (e.g., trigger an email notification, create a ticket, or execute a custom script).[3]

Using the PDCA cycle, the organization needs to go through an internal process in order to create a new detection rule:

- **Plan:** The team can propose in regular meetings suggestions of new use cases, or in the case of discovery of critical events internally or externally.
- **Do:** After the approval of the SOC manager, the team conducts a research to find the case's triggers.
- **Check:** The test phase takes place in a test server to observe and verify the alerts generated and try to adjust the rule to limit the false positives.
- **Act:** A report is written and submitted to the SOC manager outlining the functionality of the rule and its associated issues, after which he decides whether to implement it into the SOC, or improve it and go through this process again.

A document that explains the process of the creation of a detection rule was created, details on the document is available in the **annex A** section **Detection Rule Creation Document**.

2.6.4 Detection Rules List

When it comes to detection rule creation, it has to be customized to face the organization use cases, so we suggested a list of the rules to MNA Group shown in table 2.3 to be created and tested using Elastic SIEM and **Creation of Detection Rule using Elastic SIEM** document.

[3]These options require having the appropriate license or using a cloud deployment.

Data Source	Use Case	Alert generated
Windows OS	**Unauthorized access & use activities**	Multiple Password Changes in short time
		User account added/removed in admin Group
		Account modified by a normal user account
		Successful login as windows admin using consent
		Users created/removed within a short period of time
		Logs files deleted
		Privilege escalation using cmd or powershell
		Multiple windows accounts locked out
		Multiple password Changes in short time
		Detection of system time changes (Boot time)
		Windows ACL set on admin group members
		Failed Windows login with an expired account
		Successful SSH connection
		Multiple SSH connection failures in a short amount of time
		Shell session initiated by user
		Firewall Disabled via PowerShell
AD server	**Unauthorized access & use activities**	Failure account access to AD server
		Not admin access to the DC server via ssh
		Attempting to gain unauthorized access to sensitive files or folders
Linux OS	**Unauthorized access & use activities**	Change or deletion in sensitive files
		Users Group change
		Failed login as root
		Password changed
		Successful SSH connection
		Multiple SSH connection failures in a short amount of time
		Shell session initiated by user
OS	**Malware detected**	Malicious port connection
		Malware detected by antivirus
Nginx	**Unauthorized access**	Brute force attempt Elastic account
		Unauthorized attempted access to Elastic SIEM
Network (NIC, Firewall)	**Unusual activity**	Suspicious/unethical websites
		Firewall CPU high usage
		IP address successful connection after multiple blocks
		High number of denied events
		IP address successful connection after multiple blocks
		Ports scanning attempt
	Network attack	Alert from an external source
		Endpoint health status red
	Network administrator	Multiple Network administrator firewall authentication fails in short time(brute force)
	P2P traffic	Network P2P traffic detected
	DoS attack	DoS attacks on SIEM Server
Docker	**Error**	Elasticsearch container error
		Kibana container error

Table 2.3: Detection and Correlation Rules List

The syntax of some of the rules created are available in the **annex B**, the syntax of other rules is not available due to them not using query language.

2.7 Conclusion

In this chapter we covered the introduction of the host organization, it's network diagram and security needs. Then, we showcased how we designed SIEM architecture using Elastic, assigned the SOC team and created SOC document for incident response, log retention and detection rule creation processes using the SOC set-up methodology. We also created a list of the detection rules based on the company needs ,what triggers the rules and their source devices. This is very important to set-up the SOC, because it shows the main elements and defined set-up steps.

Chapter 3

SOC Implementation, Deployment and Testing

3.1 Introduction

In the final chapter, we will first present the implementation steps to our proposed SOC solution and integrate the source devices . Then, we will explore the various types of rule detection and conduct tests to validate the SOC.

3.2 Tools And Technologies

We integrated several tools and technologies into our environment for security and optimisation:

- **Docker:** is a containerization software that uses OS-level virtualization to deliver software in packages called containers. The software that hosts the containers is called Docker Engine.
- **Nginx:** is an open source web server designed for maximum performance and stability. In addition to its HTTP/HTTPS server capabilities, NGINX also functions as a reverse proxy and load balancer for HTTP/HTTPS, TCP, and UDP servers.
- **Firewalld:** is a zone-based host firewall that monitors traffic and takes actions based on a set of defined rules applied against incoming/outgoing packets.
- **Rsyslog:** is an open-source software tool used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol and extends it with additional features, extends it with content-based filtering, rich filtering capabilities, queued operations to handle offline outputs.
- **Network File System (NFS):** is a feature in Linux for efficient file sharing and network management. It allows users to share large files or volumes of files across multiple computers within a network, making it particularly useful in educational settings and for reducing storage costs and licensing fees. NFS works by allowing a server to export a directory of files to a client, which can then mount the directory and access the files within it.

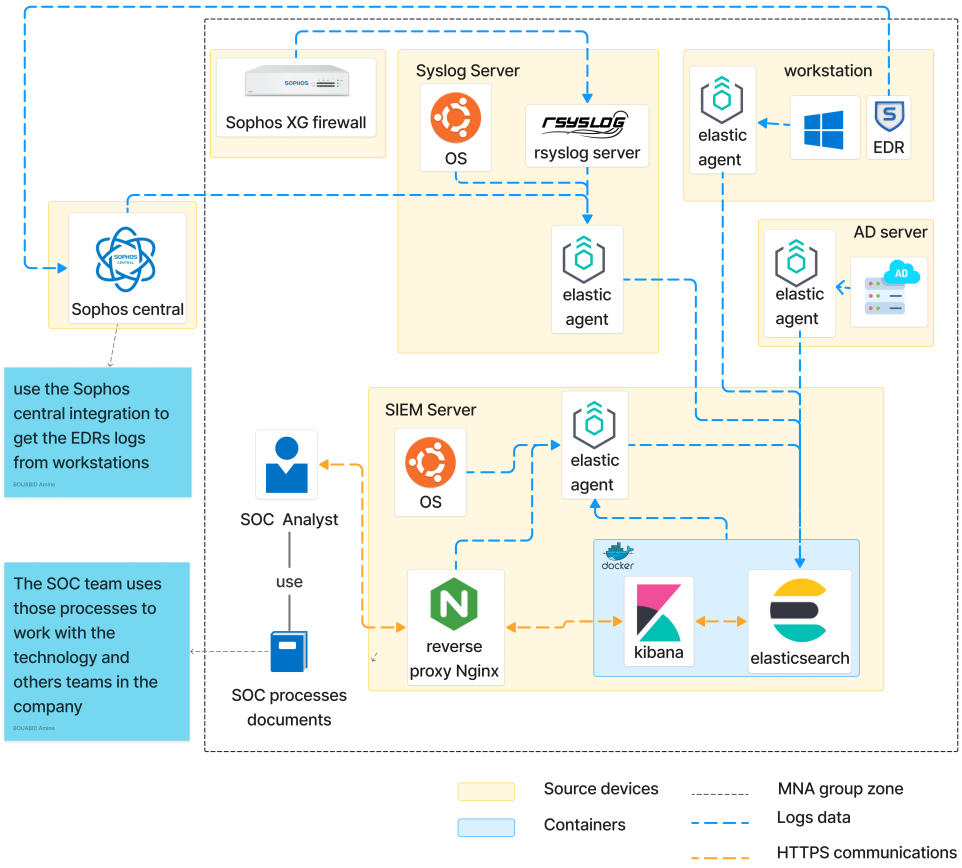

Figure 3.1: MNA Group SIEM Architechture with Technologies

This table describes the deployment, capacity, and technologies used for both the SIEM server and the Syslog server.

Table 3.1: Technologies used in the servers

Device	Mamery (RAM)	Storage	Operating System	Technologies
SIME Server	16 GB	500 GB	Ubuntu 22.04.4 LTS	Nginx reverse proxy server firewalld Docker Engine
Syslog Server	8 GB	1 TB	Ubuntu 22.04.4 LTS	Rsyslog server firewalld

3.3 Elastic SIEM Server Set Up

When it comes to Elasticsearch and Kibana, there exists numerous approaches to installation, including direct host installation, deployment via docker, utilization within kubernetes, or with cloud platforms(elastic cloud enterprise). After deploying the server side of the SIEM, our next step involves enhancing security through the incorporation of several measures and the utilization of various tools.

3.3.1 Technology Deployment Location Choice

Our preference for this organization leaned towards the deployment of Elastic server within docker containers. They share the host operating system and only virtualize at a software level, resulting in reduced overhead and efficient resource utilization.

3.3.2 Downloading and Installing Elasticsearch

There are several steps that need to be taken in order to integrate Elasticsearch into our environment with Docker:

3.3.2.1 Pull Elasticsearch image:

Docker registry provides the community with latest versions of Elasticsearch and Kibana images to use (version 8.13.3). First, we need to pull Elasticsearch and kibana images from the Elastic official website using the Docker and the **image pull** tool to get the Elasticsearch image with the version number.

```
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.13.3
```

3.3.2.2 Elasticsearch Signature verification:

The next step is verifying if the images are from the official website which will ensure that we are running on our environment the trusted versions. The Cosign command is used here to verify the images signature. this step in an optional one, and it has no effect to the installation steps.

```
wget https://artifacts.elastic.co/cosign.pub
cosign verify --key cosign.pub docker.elastic.co/elasticsearch/
    elasticsearch:8.13.3
```

3.3.2.3 Creating A docker Volume

We need to create a docker volume to mount the file that will be used to store the snapshots.

```
docker volume create volume01
```

3.3.2.4 Installing and running the Elasticsearch image:

Next, to run Elasticsearch's container for the first time, we need to use the run command, provided with the following flags:

- **–name**: assigns a custom name of the container.
- **–net host**: runs the container on the host network using the machine NIC directly

- **-it**: keeps the container running in the interactive mode to get the enrollment token to enroll with kibana and password of elastic when logging in for the first time.
- **-m**: sets memory limit(RAM) for Elasticsearch to consume. In our case, we decided that using 8GB is enough for our environment.[1]
- **-v** : mounts the Docker volume named **volume01** to the **/media** directory inside the container.
- **image name**: specifies the Elasticsearch image to use, along with version number.

```
docker run --name elasticsearch01 --net host-it -m 8GB -v volume01:/media
    docker.elastic.co/elasticsearch/elasticsearch:8.13.3
```

3.3.3 Downloading and Installing kibana

The steps to installing and running Kibana images are essentially the same as Elasticsearch with the exception of not limiting the memory for the container of kibana.

3.3.3.1 Pulling Kibana's Image:

Like in Elasticsearch's case, we need to pull Kibana image from Elastic official website using Docker and its tool **image pull** followed by the name of Kibana's image with the same version of Elasticsearch(8.13.3).

```
docker pull docker.elastic.co/kibana/kibana:8.13.3
```

3.3.3.2 Kibana's Signature verification:

As in Elasticsearch signature verification, The next step is verifying if the images are from the official website . This step in an optional one, and it has no effect on the installation steps.

```
wget https://artifacts.elastic.co/cosign.pub
cosign verify --key cosign.pub docker.elastic.co/kibana/kibana:8.13.3
```

3.3.3.3 Installing and running the Kibana image:

Next, to run the Kibana container for the first time, we need to use the run command, provided with the following flags:

- –**name**: assigns a custom name of the container.
- –**net host**: runs the container on the host network using the machine NIC directly
- **-it**: keeps the container running in the interactive mode to get the enrollment token to enroll with kibana and password of elastic when logging in for the first time.
- **image name**: specifies the Kibana image to use, along with version number.

```
docker run --name kibana01 --net host docker.elastic.co/kibana/kibana
   :8.13.3
```

[1] not using this flag requires manually setting the JVM size.

3.3.4 Configuration of Elasticsearch and Kibana

Once we have confirmed that Elasticsearch and Kibana containers are running successfully, we obtain the link for Kibana to register securely and enroll the kibana instance in Elasticsearch using the enrollment token and verification code.

3.3.4.1 Elasticsearch Enrollment Token

To generate this enrollment token, we execute the **elasticsearch-create-enrollment-token** tool to obtain an automatically generated enrollment token for Kibana.

```
docker exec -it elasticsearch01 /usr/share/elasticsearch/bin/
elasticsearch-create-enrollment-token -s kibana --url https://localhost
:9200
```

This command generates a **BASE64** token, then we copy and paste this token in the Elastic SIEM page using browser like in this image capture 3.2.

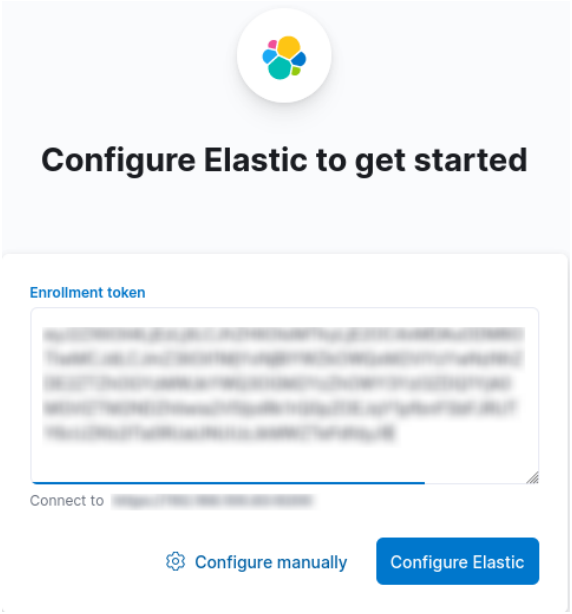

Figure 3.2: Image Capture of Enrollment Token Input

3.3.4.2 Kibana Verification code

After entering the enrollment token of Elasticsearch into Kibana, a verification code is required for security like in this image capture 3.3. This command is used to retrieve a

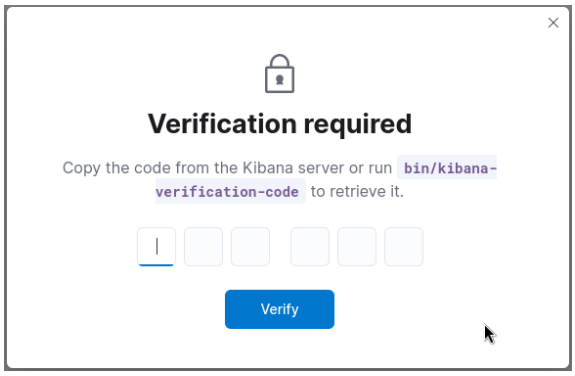

Figure 3.3: Image Capture of Verification code Input

verification code for Kibana, the code is a 6 digit number.

```
docker exec -it kibana01 /usr/share/kibana/bin/kibana-verification-code
```

3.3.5 Securing Elasticsearch and Kibana

To ensure a secure communication between Elasticsearch and Kibana, and between Kibana and the browser, we used TLS protocol. Using this protocol requires creating certificates for Elasticsearch and kibana using Elasticsearch's tools[2], but first we have to create a self-signed certificate authority for our environment.[3]

3.3.5.1 Creating a Certificate Authority (CA)

Using the **Elasticsearch-certutil** command in Elasticsearch's container allows us to create the certificate authority(CA).

```
./bin/elasticsearch-certutil ca --pem
```

This command generates a ZIP file that contains the CA private key and the CA certificate, unzip the file in new folder called **ca**.

3.3.5.2 Creating and Signing Elasticsearch's Certificate

First, we create certificate signature request(CSR). This command generates both the private key and CSR.

```
./bin/elasticsearch-certutil csr -name elasticsearch-cert
```

[2]To perform this steps, we need to enter the Elasticsearch container and execute the commands using another Docker tool called **exec**. Specifically, run the following command: **docker exec -it elasticsearch01 /bin/sh** to run shell inside the container

[3]in a production deployment, there exists two choices : using a company-managed, or a root trusted certificate authority.

This command also create a ZIP file **elasticsearch-cert** contains both of Elasticsearch's request certificate and private key, unzip the file before signing the certificate.

After that, using the CA key and certificate, we sign CSR of Elasticsearch using the **openSSL** tool.[4]

```
openssl x509 -req -in elasticsearch-cert.csr -CA /usr/share/elasticsearch/
    ca/ca.crt -CAkey /usr/share/elasticsearch/ca/ca.key -CAcreateserial -
    out elasticsearch-cert.crt -days 365
```

After that, we reconfigure the Elasticsearch configuration file **/usr/share/elasticsearch/config/elasticsearch.yml** to add the certificate and the private key.

```
xpack.security.enabled: true
xpack.security.enrollment.enabled: true

xpack.security.http.ssl:
  enabled: true
  key: config/certs/elasticsearch/elasticsearch-cert.key
  certificate: config/certs/elasticsearch/elasticsearch-cert.crt
  certificate_authorities: config/certs/ca/ca.crt

xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  key: config/certs/elasticsearch/elasticsearch-cert.key
  certificate: config/certs/elasticsearch/elasticsearch-cert.crt
  certificate_authorities: config/certs/ca/ca.crt
```

Listing 3.1: Elasticsearch HTTPS configuration

3.3.5.3 Creating and signing kibana's certificate

This process follows the same steps as creating Elasticsearch's certificate. First, the kibana certificate is created and signed in Elasticsearch's container, then the ZIP file that contains both the certificate and private key.

```
    ./bin/elasticsearch-certutil csr -name kibana-cert
```

Then we sign the Kibana CSR using also **openSSL**.

```
openssl x509 -req -in kibana-cert.csr -CA /usr/share/elasticsearch/ca/ca.
    crt -CAkey /usr/share/elasticsearch/ca/ca.key -CAcreateserial -out
    kibana-cert.crt -days 365
```

Using the Docker tool **cp**, the is copied Kibana signed certificate and private key along with CA certificate into kibana's container.

```
docker cp elasticsearch01:/usr/share/elasticsearch/kibana-cert/kibana-cert.
    key kibana01:/usr/share/kibana/config/certs/kibana
docker cp elasticsearch01:/usr/share/elasticsearch/kibana-cert/kibana-cert.
    crt kibana01:/usr/share/kibana/config/certs/kibana
docker cp elasticsearch01:/usr/share/elasticsearch/ca/ca.crt kibana01:/usr/
    share/kibana/config/certs/ca
```

After that, we reconfigure the Kibana configuration file **/usr/share/kibana /config/kibana.yml** to enable the SSL protocol and add the certificate and private key.

[4] we fixed 365 days for all the certificates

```
SERVER_SSL_ENABLED=true
SERVER_SSL_CERTIFICATE=config/certs/kibana/kibana-cert.crt
SERVER_SSL_KEY=config/certs/kibana/kibana-cert.key
SERVER_SSL_CERTIFICATEAUTHORITIES=config/certs/ca/ca.crt
```

Listing 3.2: Kibana HTTPS configuration

3.3.5.4 Securing Objects Saved in Kibana

In order to create and manage the detection rules and visualize alerts, an encryption key is required by Kibana, showing in the message 3.4.

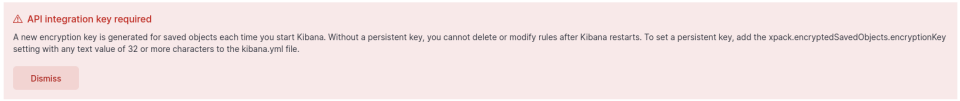

Figure 3.4: Image Capture of Encryption Key Required

First the kibana-encryption-key tool is used to generate a 32 bits key.

```
docker exec -it kibana01 /usr/share/kibana/bin/kibana-encryption-keys
    generate
```

Which is then copied into Kibana's container in the **kibana.yml** configuration file.

```
xpack.encryptedSavedObjects.encryptionKey: <32 digit>
```

Listing 3.3: kibana encryption key configuration

3.4 Syslog Server Deployment

In order to receive logs from network devices(Sophos XG firewall), we deployed and configured an rsyslog server, which will act as a centralized log receiver. We created a configuration file **/etc/rsyslog.conf** which will allow our rsyslog server to receive logs from the firewall via the syslog protocol.

```
$template myFormat,"%rawmsg%\n"
$ActionFileDefaultTemplate myFormat

# configure the the events file of the firewall in /var/log/rsyslog/@IP
# keep the events in the orignal format
$template DynaFile,"/var/log/rsyslog/%FROMHOST-IP%/%syslogfacility-text%.
    log","%rawmsg%"
*.* ?DynaFile
&~
# Filter duplicated messages
$RepeatedMsgReduction on
```

Listing 3.4: Rsyslog server configuration

3.4.1 NFS Configuration

To save the log data of the organization, we installed and configured an NFS server in the Syslog server, and shared with the SIEM server to make Elastic send the log snapshot to the this volume before the delete them. We enabled the read and write with synchronization between the tow servers in any changing.

```
/media/backup    SIEM-server-IP@(rw,sync,no_subtree_check,all_squash,
    no_root_squash)
```

After that the SIEM server need to mount the file in order be able to access[5].

```
mount -t nfs4 syslog-server-IP@:/media/backup /var/lib/docker/volumes/vol/
    _data/backup
```

3.5 Policies Creation and Integrations Selection

After confirming the proper functionality of the SIEM server, the upcoming step required is to develop all requisite policies for each sources devices and incorporate the necessary integrations into each policy.

The fleet UI in the **Management** section, The **Agent Policies** section allows us to create and update agent policies.

3.5.1 SIEM Server

For the SIEM server policy, the following integrations were included in the table 3.2

3.5.2 Syslog Server

In addition of **System**, **Linux Audit**, **Network Packet Capture**,**Elastic Defend** and **OSquery** integrations, we need to add integrations to collect and send the data of the Shopos XG firewall and Shopos central, table 3.3

3.5.3 Windows Workstations

All workstations have Windows OS, so a **Windows** integration along with **file integrity** is plenty to collect all the information about the employees activities.

- **Windows:** collects logs from Windows OS, services and processes.

3.6 Data Sources Integration

After the creation of the policies, we have now to install the Elastic agents on all machines, assign to each agent his appropriate policy and secure the two servers.

3.6.1 SIEM Server

Before adding the other agents, we need to first install the fleet server on the SIEM server in order to enroll the agents in the fleet.

[5]the SIEM need to install a **NFS client** to connect to the **NFS server**

Table 3.2: Integrations List for SIEM Server

System	log data streams collected by the System integration include application, system, and security events on Windows, auth and syslog events on macOS or Linux.
Linux audit	collects logs from Linux audit daemon
Docker	collects data of Docker Engine and the containers that are running for monitoring Elasticsearch and Kibana health to ensure that the SIEM is working.
Network Packet Capture	sniffs network packets and captures the network traffic on a host and dissects known protocols.
Elastic Defend	Elastic Defend provides an endpoint security layer with prevention, detection, and response capabilities that comes with different configuration presets.
OSquery	is an agent that allows to view data on operating systems using SQL-like queries live on one or more agents
Nginx	the Nginx integration allows the monitoring and collection of data from the Nginx server that has been installed in the Elastic server
Fleet Server	this integration is added to configure an Elastic Agent as a Fleet server, which is a sub-process that runs inside a deployed Elastic Agent. This integration is dedicated to running Fleet Server as a communication host and not configured for data collection, this makes it so that the agents get their policy updates from the Fleet Server.
File integrity monitoring	This integration uses features of the operating system to monitor file changes in realtime, the file location is manually selected by the user.

3.6.1.1 Fleet Server Deployment

First we need to access to Fleet UI in **Management** section. Then, we have to select in the **Add Fleet Server**, write the server name and the host URL, then select the policy of the SIEM server that has been created.

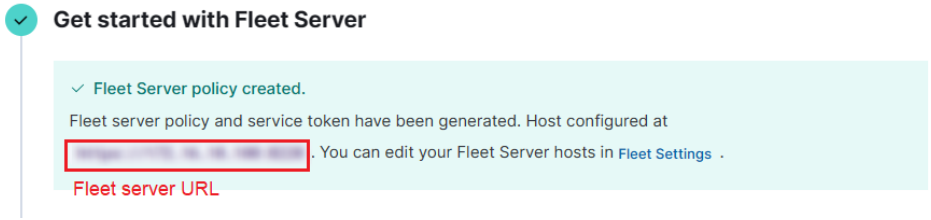

Figure 3.5: Create Fleet server and assign its policy

After that, the list of commands that needs to be executed to download and install the agent in the SIEM server will be generated by the Fleet UI.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/
    elastic-agent-8.13.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.13.2-linux-x86_64.tar.gz
```

Table 3.3: Integration List for Syslog Server

Sophos	collects logs of the Sophos XG firewall that has been send to Rsyslog server in the syslog format
Sophos central	collects logs of the Sophos EDRs from the Sophos central platform
AbuseCH	is a platform that ingests threat intelligence indicators from other websites(URL Haus, Malware Bazaar, and Threat Fox feeds). The integration collects the logs from the platform and sends them to the agent

```
cd elastic-agent-8.13.2-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://https://Elastic-SIEM.com \
  --fleet-server-service-token=<64 bit token> \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=<CA certificate fingerprint> \
  --fleet-server-port=<Fleet server port>
```

After the installation is complete, Elastic Agent will send the logs files to Elasticsearch.

3.6.1.2 Reverse Proxy Deployment

In the policy creation section, we added **Nginx** integration to the SIEM server policy, Now we need to download and configure the Nginx configuration file **/etc/nginx/nginx.conf** as a reverse proxy server, add a white list for access control and cache for more performance to enhance the SOC team's experience.

```
server {
         # HTTPS
         listen       443 ssl;
         server_name  kibana.com;
         # reverse proxy certificate
         ssl_certificate      /etc/nginx/cert/nginx2.crt;
         ssl_certificate_key  /etc/nginx/cert/nginx2.key;
         # TCP connection configuration
         ssl_session_cache    shared:SSL:1m;
         ssl_session_timeout  5m;
         ssl_ciphers  HIGH:!aNULL:!MD5;
         ssl_prefer_server_ciphers  on;
         location / {
                 # white list control
                 allow SOC-team-sunbet;
                 deny all;
                 # cache configuration
                 proxy_buffers 16 4k;
                 proxy_buffer_size 2k;
                 # connecte to Kibana
                 proxy_pass https://kibana.com;
            }
        }
```

Listing 3.5: nginx as reverse proxy over SSL

3.6.1.3 Securing the Server

To add more security to the SIEM server, we implemented the server with a host firewall **Firewalld**, the host firewall restricts the usage of ports to only the ones needed using access control lists(ACL).

```
firewall-cmd --list-all
```

This command shows all the firewalld configuration

```
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
# allow HTTPS over port 443 and SSH over port 22
  services: https ssh
# those ports for Elasticsearch and Fleet server connections
  ports: 9200/tcp 8220/tcp
  .....
```

Listing 3.6: print firewalld configuration

3.6.2 Sophos XG Firewall

Next, we need to configure the firewall to send its logs to Rsyslog server, which is done using its graphic interface.

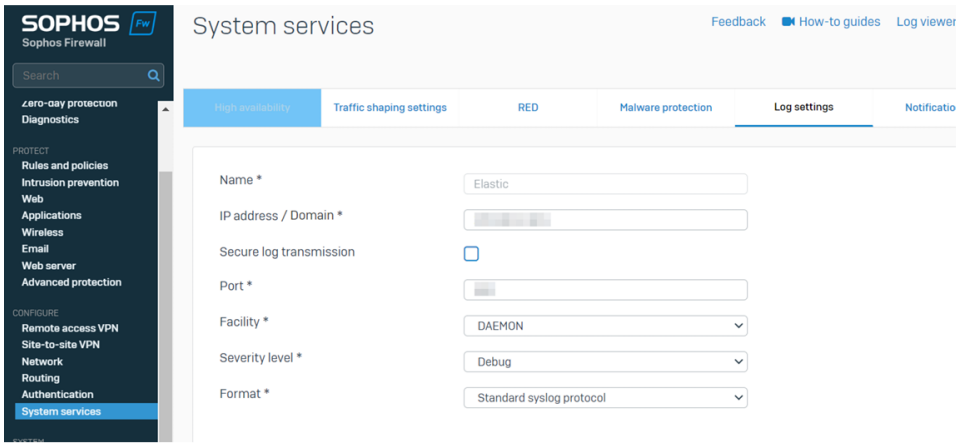

Figure 3.6: Configuration of Sophos XG firewall

3.6.3 Syslog Server

The steps that need to be taken in this server are installing the Elastic Agent, assign its policy and ensuring that the agent is sending the logs of the system, the firewall and sophos central.

3.6.3.1 Elastic Agent installing

First, we need to access the Fleet UI in **Management** section. Then, we have to select the **Add Agent** button, choose the option **Enroll in fleet** and select the fleet server that

the agent will be enrolled in.[6] Then, we need to select the policy created for the Server.

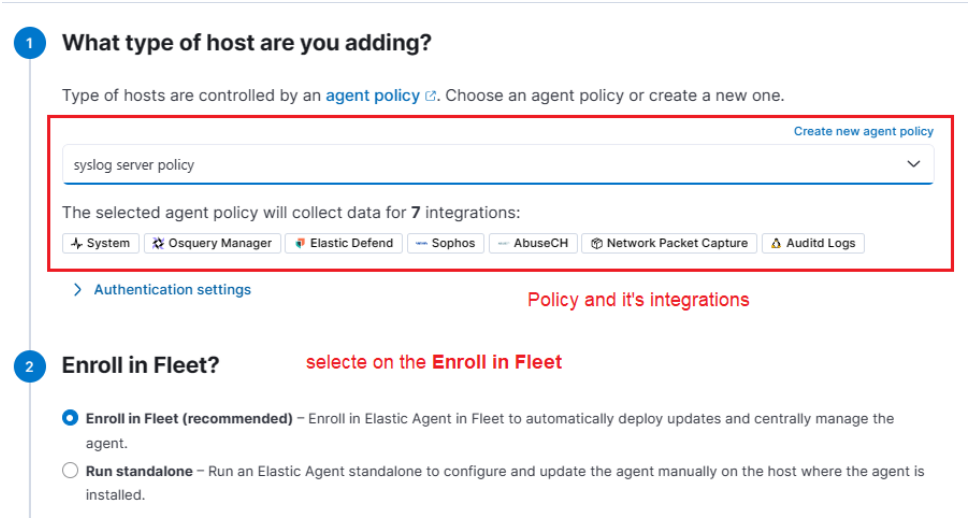

Figure 3.7: Create Fleet server and assign its policy

After that, the list of commands that needs to be executed to download and install the agent in the server will be generated by the **Fleet UI**.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/
    elastic-agent-8.13.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.13.2-linux-x86_64.tar.gz
cd elastic-agent-8.13.2-linux-x86_64
sudo ./elastic-agent install --url=https://Fleet-server-URL.com --
    enrollment-token=<64 bit token>
```

After executing the commands, we have to wait for the **fleet UI** to confirm that the agent is enrolled in the fleet and the logs are being sent to Elasticsearch.

3.6.3.2 Securing Server

To secure this server, we added the host firewall **Firewalld** which is configured to restrict the usage of ports using access control lists like the SIEM server.

3.6.4 Windows Workstations

3.6.4.1 Elastic Agent Installing

The procedure for installing agents on workstations matches that of installing them on Syslog server while ensuring the selection of the suitable policy.

[6] there is another option, **Run standalone** mean that to configuring and updating the agent is done manually from the host.

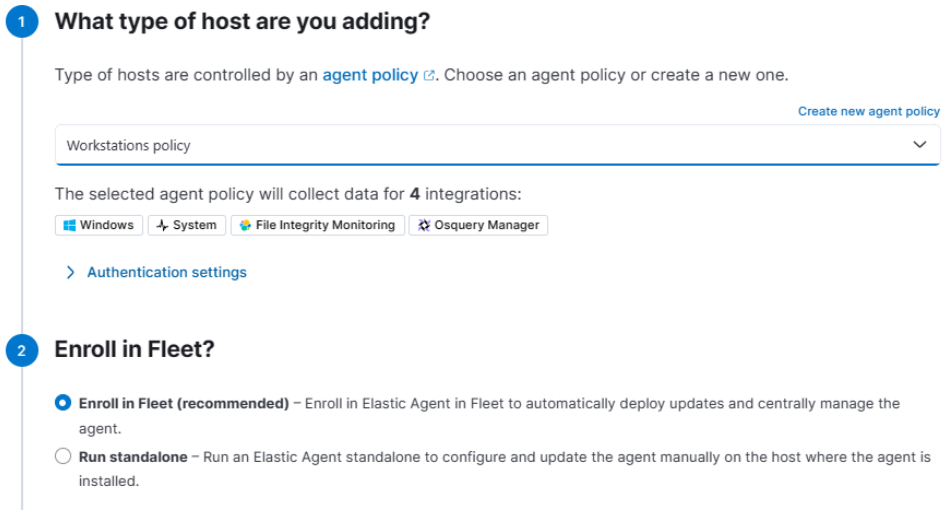

Figure 3.8: Select the workstation policy

3.7 Creating and Testing Detection Rules

After we make sure that all the source devices are running the Elastic Agents healthily and sending the logs, we have to create detection rules using the **Detection Rule Creation in Elastic SIEM** process[7], conduct tests on the SOC to check its ability to detect, analyze, and respond to security incidents as part of evaluating its effectiveness.

3.7.1 Unauthorized access and use activities Attempt In Windows

In any company, the workstations and user accounts are managed by centralize server like Active Directory(DC), all the workstation has a non administrative account with minimum privilege to make the employees to work and all of them have the same administrative account to manage and configure the workstations, but some employee try gain to access to the administrative account for fun or malicious attempt.

```
sequence by host.name, user.name with maxspan=1m
  [ authentication where event.code : "4625"  and event.outcome : "failure"
     and (winlog.event_data.SubStatus : "0xc000006a" or winlog.event_data.
    SubStatus : "0xc0000064") and process.name:"consont.exe"] with runs=3
```

This rule triaged when the user try to access to administrative account 3 time or more in 1 minutes and failure to do.

[7]Create Detection Rule using Elastic SIEM document

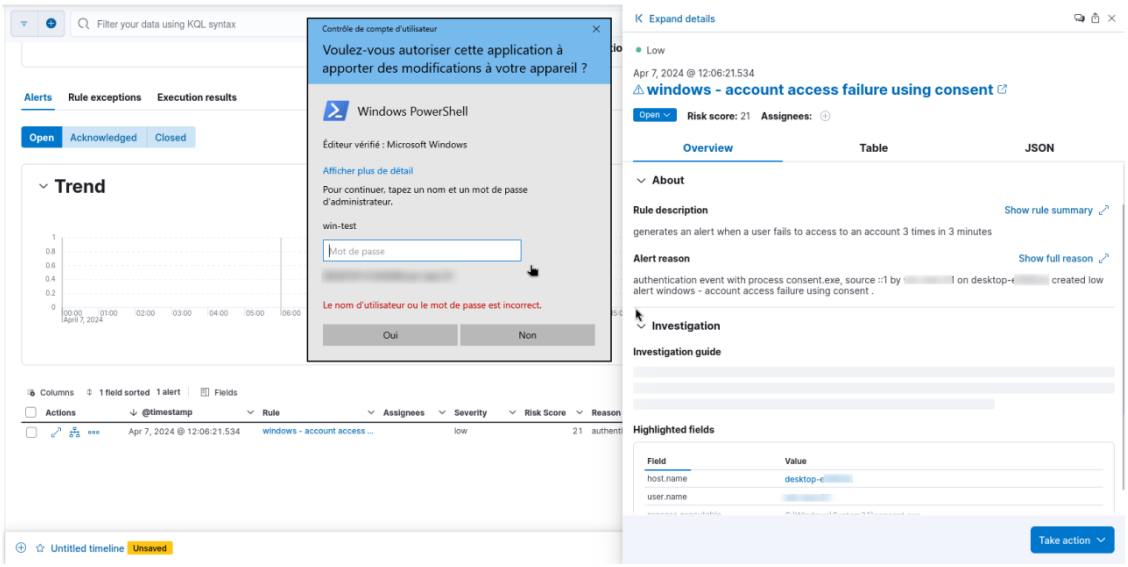

Figure 3.9: Image Capture Show Detection of Unauthorized Access Attempt

3.7.2 SSH Brute Force Attempt

Multiple SSH connection failures in a short amount of time indicate that the system is under a brute force attack. In Linux, the SSH connections events are generated for success or failed connection, this is done by monitoring SSH failed connections in short time using Threshold. The following alert when the rule detects many SSH failed attempts within a short time period.

```
sequence by host.name with maxspan=30s
  [ authentication where event.action : "ssh_login"  and system.auth.ssh.
    event:"Failed"] with runs=15
```

This rule triaged when the user try to brute force for 6 time or more in 30 seconds and failed.

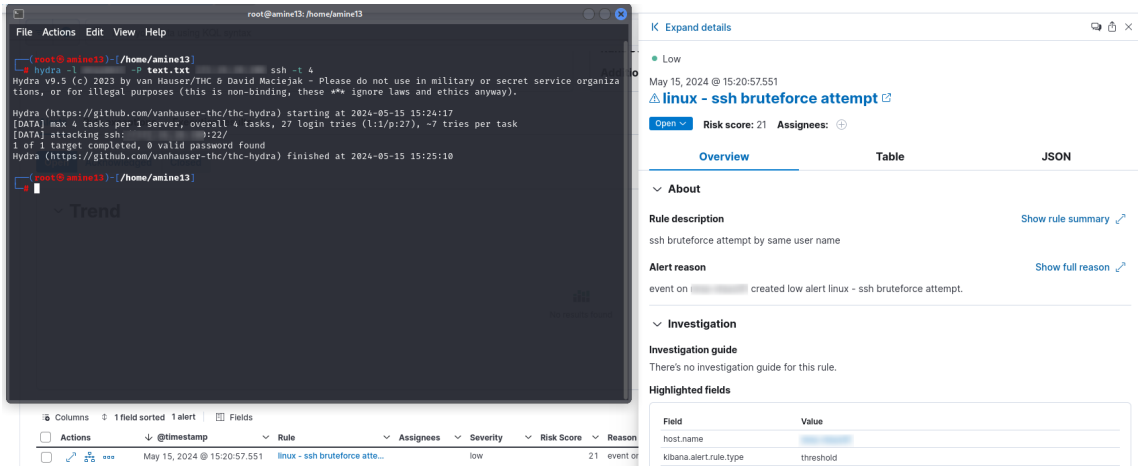

Figure 3.10: Image Capture Show Detection of SSH Brute Force

3.7.3 URL threat intelligence

Elastic offers a feature that allows integrating threat intelligence sources into the SIEM system. Among these sources, we find Abuse CH, which is a threat intelligence platform providing information about URLs and IP addresses associated with malicious activities on the Internet. In our case, we used Abuse CH to supply the SIEM with a stream of malicious URLs or IP addresses. Using this integration, we can monitor all the packets of the firewall logs to detect a malicious source. The rule we created monitors the URLs accessed by the users and correlates with the IP addresses and URLs provided by the integration. We can check if the IP address is a malicious source from one of the most

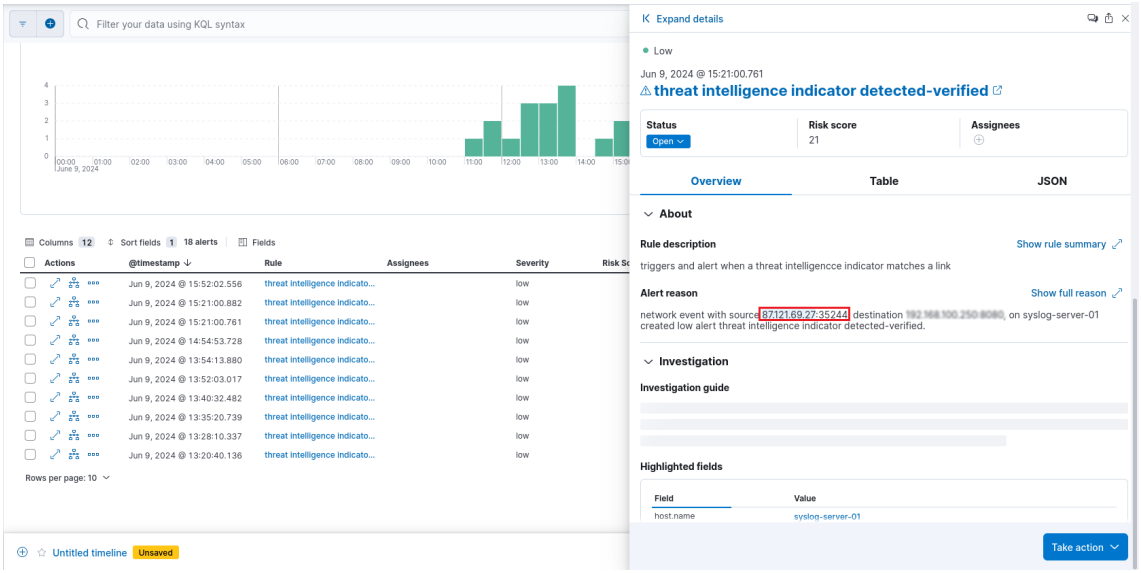

Figure 3.11: Image Capture Show Detection of Malicious IP Address

reliable source of threat intelligence, **Virus Total**.

Figure 3.12: Image Capture Show That The IP Address is a Malicious Source in Virus Total Platform

3.7.4 DoS Attack

The Elastic SIEM platform must be available all the time for the SOC team to keep monitoring the environment and respond to incidents, a DOS attack can affect the availability of the platform, so detecting a DOS attack on the SIEM Server is important. Using ES|QL, we can aggregate the number of the requests in 1 minute, if there are more than 1000 request/minute, we can assume that there is a DOS attack.

```
from logs-* | where host.name like SIEM-server and event.category like "
    network" |EVAL time = DATE_TRUNC(1 minutes, @timestamp) | stats nb =
    count(*) by time | stats nb_max = max (nb) | where nb_max > 15000
```

This rule triaged when the SIEM server get more the 15000 packets request in 1 minute, indicate there is a more than normal requests to the SIEM server.

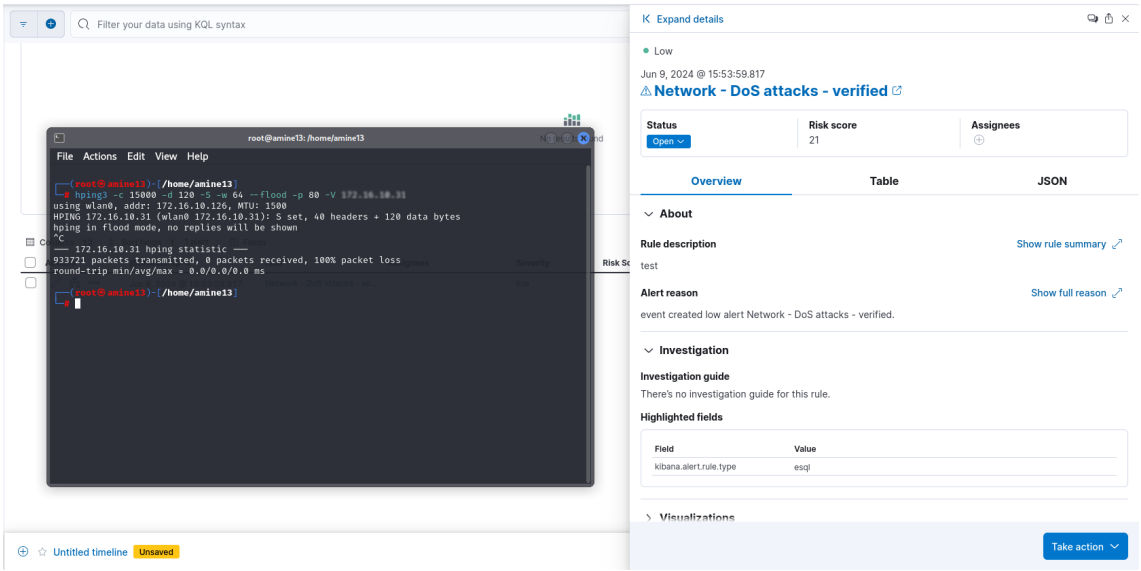

Figure 3.13: Image Capture of a Detection of DoS Attack

3.8 Conclusion

In this chapter, we explained the set up process of our SOC solution, mainly Elastic SIEM. We configured and integrated the necessary data sources to ensure thorough monitoring of our environment. We ensured that our solution was well-prepared for surveillance and detection of suspicious activities. Then, we explained some of the attacks and the rules we created to detect them.

General Conclusion and perspectives

This project showed us that the cyber attacks are getting more complex and the needs for a SOC to detect, analyze and respond to security incidents is more important than ever. Using Elastic SIEM has proven essential as a key component of the SOC, providing a centralized platform for environment monitoring, data collection, correlation, and security analysis, also making automation and integrated response actions for those incidents.

Throughout our project we have implemented a SOC based on Elastic SIEM at MNA Group in order to enhance its cyber-security. Throughout the various chapters of this project, we covered information security basics, the SOC set-up methodology, our specific SOC design at MNA Group and finally, the deployment of Elastic SIEM and SOC documents.

Using the methodology to set up a SOC, we first set up a server to host the main components of our SIEM system. We then installed Elasticsearch and Kibana, ensuring they were functioning properly. After that, we secured the server by adding a host firewall and a reverse proxy server. Next, we established policies for each type of agent and deployed agents to various source devices, including Sophos Central, workstations, and the Active Directory server. We verified that each agent was transmitting all the logs specified in its assigned policy. We then documented the incident response process, the creation of detection rules, and log retention procedures. Following this, using those documents, we created around 50 detection rules and fine-tuned them to minimize false positives. Finally, we established a repository for log retention and defined a log retention policy.

Our approach offers several advantages. It is based on a robust methodology and professional recommendations, including guidelines from Cisco. We utilized the latest Elastic Stack, featuring Elastic Agents, Elasticsearch, and Kibana, to ensure advanced data collection, analysis, and visualization capabilities. We created comprehensive detection rules for all data sources, documented incident response processes based on the NIST framework, and established a log retention policy and repository using NFS. Additionally, we enhanced scalability and security by incorporating a reverse proxy into the system and using containerisation for the core components of our system.

Regarding the outcome, there are numerous chances for improvement and development. First and foremost, integrating machine learning and artificial intelligence techniques into the SOC could improve the detection and prevention of attacks by automatically identifying abnormal patterns and behaviors. Additionally, it would be relevant to further develop rules related to other source devices like Sophos Central and make use cases of

Elastic SIEM to potential threats scenarios. This will enhance overall the SOC performance. Finally, from a broader perspective, MNA Group could consider sharing this accomplishment to other companies and organizations to address the importance of SOC in securing from cyberattacks which will spread the security awareness and the dangers of security attacks.

Bibliography

[1] Joseph Muniz, Gary McIntyre, and Nadhem AlFardan. *Security operations center: Building, operating, and maintaining your SOC*. Cisco Press, 2015.

[2] *information security - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/information_security. [Accessed 17-02-2024].

[3] David R Miller et al. *Security information and event management (SIEM) implementation*. McGraw Hill Professional, 2010.

[4] *threat - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/threat. [Accessed 17-02-2024].

[5] *vulnerability - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/vulnerability. [Accessed 17-02-2024].

[6] *risk - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/risk. [Accessed 17-02-2024].

[7] *asset - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/asset. [Accessed 17-02-2024].

[8] *risk assessment - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/risk_assessment. [Accessed 17-02-2024].

[9] *log - Glossary— CSRC(csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/log. [Accessed 17-02-2024].

[10] *Malware - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/malware. [Accessed 17-02-2024].

[11] *virus - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/virus. [Accessed 17-02-2024].

[12] *trojan horse - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/trojan_horse. [Accessed 17-02-2024].

[13] *worm - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/worm. [Accessed 17-02-2024].

[14] *denial of service(DoS) - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/denial_of_service. [Accessed 17-02-2024].

[15] *distributed denial of service(DDoS) - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/distributed_denial_of_service. [Accessed 17-02-2024].

[16] *social engineering - Glossary— CSRC(csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/social_engineering. [Accessed 17-02-2024].

[17] *red team - Glossary— CSRC(csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/red_team. [Accessed 17-02-2024].

[18] *blue team - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/blue_team. [Accessed 17-02-2024].

[19] *encryption - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/encryption. [Accessed 17-02-2024].

[20] *firewall - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/firewall. [Accessed 17-02-2024].

[21] *authentication - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/authentication. [Accessed 17-02-2024].

[22] *access control - Glossary— CSRC (csrc.nist.gov)*. https://csrc.nist.gov/glossary/term/access_control. [Accessed 17-02-2024].

[23] Don Murdoch. *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: Notes from the Field (V1. 02): a Condensed Field Guide for the Security Operations Team*. Amazon, 2018.

[24] *SIEM — Splunk*. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html. [Accessed 17-04-2024].

[25] *IBM Security QRadar SIEM*. https://www.ibm.com/products/qradar-siem. [Accessed 17-04-2024].

[26] *SIEM Solution & Security Analytic — Elastic Security*. https://www.elastic.co/security/siem. [Accessed 17-04-2024].

[27] *Splunk vs Elastic Security — — Which SIEM Tools Wins In 2024*. https://www.gartner.com/reviews/market/security-information-event-management/compare/elasticsearch-vs-splunk. [Accessed 17-05-2024].

[28] *IBM QRadar vs Elastic Security — Which SIEM Tools Wins In 2024*. https://www.selecthub.com/siem-tools/ibm-qradar-vs-elastic-security/. [Accessed 17-05-2024].

[29] *MNA Groupe — mnagroupe.com*. https://mnagroupe.com/. [Accessed 22-05-2024].

Annex A: SOC Processes Documents Description

Log Retention Document

Title	Log retention process
Author	BOUABID Abou El Kacem Amine ZOUBIRI Abdelmalek
Date	10/6/2024
File Type	PDF
Structure	
Length	13 pages/ 1305ko
Version	1.0
Abstract	This document's purpose is providing information the log retention and guiding the SOC team through its process in Elastic.

Figure 14: Description of Log Retention Document

Detection Rule Creation Document

Title	Log retention process
Author	BOUABID Abou El Kacem Amine ZOUBIRI Abdelmalek
Date	10/6/2024
File Type	PDF
Structure	
Length	13 pages/ 1305ko
Version	1.0
Abstract	This document's purpose is providing information the log retention and guiding the SOC team through its process in Elastic.

Figure 15: Description of Detection Rule Creation Document

Incident Responses Documents

DoS/DDoS Attacks

Title	Incident Response Playbook: DoS/DDoS
Author	BOUABID Abou El Kacem Amine ZOUBIRI Abdelmalek
Date	09/06/2024
File Type	PDF
Structure	
Length	13 pages/724Ko
Version	1.0
Abstract	This document provides information about DoS/DDoS attacks and the steps to preventing, dealing with them.

Figure 16: Description of DoS/DDoS Attacks Incident Response Document

Social Engineering

Title	Incident Response Playbook: Social engineering
Author	BOUABID Abou El Kacem Amine ZOUBIRI Abdelmalek
Date	09/06/2024
File Type	PDF
Structure	
Length	27 pages/4192Ko
Version	1.0
Abstract	This playbook serves as a comprehensive guide for the MNA Group's SOC to respond effectively to malware outbreaks and social engineering (SE) incidents. It outlines procedures, best practices, and tools necessary for SOC analysts, managers, and incident response teams to detect, analyse, and mitigate security threats.

Figure 17: Description of Social Engineering Incident Response Document

Malware Outbreak

Title	Incident Response Playbook: Malware Outbreaks
Author	BOUABID Abou El Kacem Amine ZOUBIRI Abdelmalek
Date	09/06/2024
File Type	PDF
Structure	
Length	13 pages/440Ko
Version	1.0
Abstract	This playbook is designed for the MNA Group to guide the (SOC) in responding to malware outbreaks and social engineering (SE) incidents. It provides detailed procedures and best practices to enhance SOC effectiveness in detecting, analyzing, and mitigating security threats. The playbook is structured to support SOC analysts, managers, computer security incident response teams, and system/network administrators.

Figure 18: Description of Malware Outbreak Incident Response Document

Annex B: Syntax of Some of the Rule Detection

Rule name	Query language	Syntax
Linux - change or deletion in sensitive files	Kibana query language	event.module : "file_integrity" and event.action : "deletion" or event.action : "change" and file.path :"etc/netplan/50-cloud-init.yaml" or file.path: "/etc/sudoers" or file.path: "/etc/rsyslog.conf" or file.path: "/etc/shadow" or file.path:"/etc/passwd" or file.path: "/etc/passwd-"
Linux - group change	Kibana query language	host.os.type: "linux" and event.dataset : "system.auth" and (log.syslog.appname : "usermod" or log.syslog.appname :"gpasswd") and message:"*to group *"
Linux - failed login as root	Event query language	authentication where host.os.type:"linux" and log.syslog.appname:"sudo" and event.outcome:"failure"]\n[process where host.os.type:"linux" and log.syslog.appname:"sudo" and system.auth.sudo.error:"*incorrect password attemp*"
Windows - Firewall Disabled via PowerShell	Event query language	process where host.os.type == "windows" and event.action == "start" and\n (process.name : ("powershell.exe", "pwsh.exe", "powershell_ise.exe")) and process.args : "*Set-NetFirewallProfile*" andn (process.args : "*-Enabled*" and process.args : "*False*") andn (process.args : "*-All*" or process.args : ("*Public*", "*Domain*", "*Private*"))"
windows - failed login with account expiration	Event query language	"sequence by host.name with maxspan=5m [authentication where event.code: "4625" and event.outcome : "failure" and winlog.event_data.SubStatus : \"0xc0000193\"] with runs=3
Windows - detection of system time changes (Boot time)	Event query language	sequence by host.name with maxspan=1s [configuration where host.os.type:"windows" and event.code : "4616" and not winlog.event_data.SubjectUserName : "SERVICE LOCAL" and not winlog.event_data.ProcessName : "C:\\\\Windows\\\\System32\\\\svchost.exe"] with runs=2
Firewall - high number of denied events	Event query language	sequence with maxspan=1s [network where data_stream.dataset : "sophos.xg" and event.action : "denied" and event.code : "01001"]with runs=100

Firewall - endpoint health status red	Kibana query lagunage	event.dataset:"sophos.xg" and sophos.xg.log_component: "Endpoint" and sophos.xg.hb_status : "Red"
Firewall - failure event	Kibana query lagunage	data_stream.dataset : "sophos.xg" and sophos.xg.status : "Failed" and event.severity <= 5
DC - failed account access to AD server	Event query language	sequence by user.name with maxspan=3m [authentication where event.code: "4776" and event.action :"credential-validated" and event.outcome : "failure" and host.name : "AD-server" and input.type : "winlog" and winlog.keywords : "Échec de l'audit"] with runs=3