

**UNIVERSITY OF HERTFORDSHIRE**



**A Project Report**

**On**

**“Designing and Implementing a SOC2 Compliant Network  
Infrastructure for Hierarchical Access Limited (HAL) Using  
AWS, IDS/IPS systems, and SIEM Tools”**

*In partial fulfilment of the requirement for the award of the degree of*

**MASTER OF SCIENCE**

**In**

**CYBER SECURITY**

*Submitted by*

Muhammad Umer Jamil

Student ID: 21067344

*Under the Supervision of*

**Dr. Nnamdi Nwanekezie**

**Department of Computer Science (2022-2024)**

## ***DECLARATION***

---

This report is submitted in partial fulfilment of the requirement for the degree of Master of Science in Cyber Security at the University of Hertfordshire (UH). It is my own work except where indicated in the report. I did not use human participants in my MSc Project. I hereby give permission for the report to be made available on the university website provided the source is acknowledged.

**Muhammad Umer Jamil**

**Student ID: 21067344**

## ***ACKNOWLEDGEMENTS***

---

While working on this thesis, I came across some persons that made significant contributions to my field of research and deserve special recognition. It's a joy to express my gratitude to each of them.

First and foremost, I'd certainly want to convey my heartfelt thanks and indebtedness to my supervisor, **Dr. Nnamdi Nwanekezie**, for his essential encouragement, suggestions, and support from the beginning of this project and for presenting me with wonderful experiences throughout the process. Above all, his priceless and attentive supervision at every stage of work inspired me in countless ways.

I especially thank him for his guidance, oversight, and invaluable assistance throughout this project. His interest in imaginative thinking has prompted and nurtured my intellectual development, which will benefit me for a long time to come. I am pleased to have the opportunity to work with an extraordinarily experienced supervisor like him.

# ***CONTENTS***

---

<b>Declaration.....</b>	<b>2</b>
<b>Acknowledgement.....</b>	<b>3</b>
<b>Table of Content .....</b>	<b>4-6</b>
<b>Abstract.....</b>	<b>7</b>
<b>CHAPTER 1 (INTRODUCTION) .....</b>	<b>8-12</b>
1.1        Introduction.....	8
1.2        Aim .....	8
1.3        Objectives .....	8-9
1.4        Background and Context .....	9-10
1.5        Problem and Statement .....	10
1.5.1    Justification .....	11
1.6        Research Question .....	11
1.7        Consideration of Ethical, Professional and Social issues .....	11
1.7.1    Ethical Considerations .....	11
1.7.2    Legal Considerations .....	11
1.7.3    Professional Considerations.....	12
1.7.4    Social Considerations .....	12
<b>CHAPTER 2 (LITERATURE REVIEW).....</b>	<b>13-16</b>
2.1        Searching for Literature .....	13
2.2        Literature Review .....	13
2.2.1    SOC2 Compliance and ISO Standards .....	13-14
2.2.2    SOC2 Compliance as a Cornerstone of Network Security .....	14
2.2.3    Network Infrastructure Design .....	14-15
2.2.4    Risk Mitigation and Incident Response .....	15
2.2.5    Cloud Computing and Security Tools .....	15
2.2.6    Challenges and Considerations for small and medium-sized Enterprises .....	15
2.3        Research Gap and Proposed Study .....	15-16
2.4        Proposed Study .....	16
2.5        Expected Outcomes .....	16

<b>CHAPTER 3 (METHODOLOGY)</b>	<b>17-21</b>
3.1 Research Design	17
3.2 Data Collection and Analysis	17
3.3 Development Approach	18
3.4 Development Phase	18-19
3.5 Techniques and Approaches to Create a Secured Network	19-21
3.6 Critical Reflection	21
 <b>CHAPTER 4 (DEVELOPMENT, IMPLEMENTATION AND TESTING THROUGH EXPERIMENTATION, RESULTS AND DISCUSSIONS)</b>	 <b>22-49</b>
4.1 Network Structure	22-23
4.2 Implementation of SOC2 Compliance Program	23
4.2.1 Identify the type of SOC2 Report	23
4.2.2 Define the scope of Audit	23-24
4.2.3 Internal Risk Assessment	24
4.2.4 Perform Gap Analysis and Remediations	24
4.2.5 Establish Continuous Monitoring Practices	24
4.3 Deployment of Network Infrastructure	24-25
4.4 Implementation [on-premises]	25-26
4.5 Implementation [aws]	26
4.6 Load Balancer	27-30
4.7 EKS Cluster	30-33
4.8 Implementation of firewall inbound and outbound rules	33
4.9 Inbound Rules	34
4.10 Outbound Rules	35
4.11 Required Ports	35-36
4.12 Implementation of Security Policies	36
4.12.1 Implementation of Account and Password	36-38
4.12.2 Elastic Stack	38-41
4.12.3 Implementation of Two-Factor Authentication (2FA)	31
4.12.4 Implementation of Disaster Recovery Plan	42
4.12.5 Implementation of Monitoring & Logging Management	42
4.13 Incident Responses	42-43
4.13.1 Incident Responses Preparation	43
4.13.2 Creation of Initial Alert	43

4.13.3	Incident Identification .....	44
4.13.4	Isolation and Containing .....	45-46
4.13.5	Containing.....	47
4.13.6	Recovery and Eradication .....	47-48
4.13.7	Post Incident.....	49
4.14	What are the results of the audit you have done as blue team on your project?.....	49-50
4.15	Detailed Findings .....	51
<b>CHAPTER 5 (DISCUSSION AND EVALUATION).....</b>		<b>53</b>
5.1	Summary of Findings.....	53
5.2	Evaluation of Achievements .....	53
5.3	Reflection on Methodology.....	54
5.4	Challenges and Limitations .....	54
5.5	Commercial and Economic Context .....	54
5.6	Project Management Reflection.....	54
5.7	Future Work.....	55
5.8	Conclusion .....	55
<b>REFERENCES .....</b>		<b>56-58</b>

## ***ABSTRACT***

---

In today's active cybersecurity and emerging threats environment securing network infrastructures has become extremely important for organizations that provide digital services. This thesis provides a comprehensive case study of designing and implementing a SOC 2 compliant network infrastructure for Hierarchical Access Limited (HAL) using Amazon Web Services (AWS), Intrusion Detection and Prevention Systems (IDS/IPS), and Security Information and Event Management (SIEM) tools. The primary goal of this research is to improve HAL's network security to meet minimum security criteria while protecting sensitive data from potential attackers.

HAL offers fast internet connectivity, web registration, and hosting services to Small Office/Home Office (SOHO) clients, requiring strong security measures and quick incident response methods throughout its digital estate. This case study describes how to build a secure network architecture that includes authentication, authorization, and asset accounting, as well as key features like load balancing and cluster management to provide redundancy and risk mitigation.

This project's key components include AWS deployment for scalable and flexible cloud infrastructure, IDS/IPS implementation for active threat detection and prevention and SIEM technologies for real time monitoring and incident response. The priority is to achieve SOC 2 compliance to meet the severe security needs of HAL's VIP clients, ensuring that their data is managed with the greatest degree of safety and integrity.

This study's findings show that a well design network architecture, along with modern security technologies and compliance controls, greatly improves the resilience and security posture of HAL's services. This work adds useful insights into best practices for safeguarding network infrastructures in cybersecurity, serving as a template for organizations seeking to safeguard their digital assets in an increasingly threat environment.

## **INTRODUCTION**

### **1.1 Introduction**

Network infrastructure has become the backbone of many organizations in the modern digital era, determining their operational efficiency and security protocols. (Bhalla et al., 2023). For Hierarchical Access Limited (HAL), a business that requires a safe and effective method for managing its network assets, the main goal of this project is to build a strong network infrastructure.

Only authorized users will be able to access these assets thanks to this infrastructures assurance of authentication, authorization, and accounting, which also makes sure that every operation is precisely documented. Additionally, SOC 2 compliance is the goal of the project, which is a technical audit meant to evaluate how well a company agrees to one or more of the five trust principles outlined by the American Institute of CPAs (AICPA) (Wang, 2022).

HAL needs to comply with this standard to get a contract with VIP Tech clients, who require their third-party vendors to do the same. In conclusion, this project is a complete attempt to address the needs of VIP Tech clients by improving the security and effectiveness of HAL's network infrastructure and achieving SOC 2 compliance.

In addition to securing the contract with VIP Tech, the project's successful completion will establish HAL as a business dedicated to industry best practices for network management and security. (Muhammad Jamshid Khan, 2023)

### **1.2 Aim**

The aim of this project is to design and develop a SOC 2 compliant network architecture for Hierarchical Access Limited (HAL) using Amazon Web Services (AWS), Intrusion Detection and Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) technologies. This architecture will improve HALs network security by introducing strong authentication, authorization, and asset accounting procedures and will provide redundancy and risk mitigation through load balancing and cluster management. Additionally, the project aims to build comprehensive security incident response capabilities to safeguard HAL's digital assets while meeting the strict security needs of its customers.

### **1.3 Objectives**

The major objective of this case study is to improve the network infrastructure of Hierarchical Access Limited (HAL), ensuring that all systems adhere to high-security standards and successfully safeguard data from possible breaches.



- **Secure Network Infrastructure:** Upgrade and design HAL's network to meet or exceed minimum security standards, ensuring complete protection against cyber threats.
- **Performance Improvement for SOHO Clients:**
  1. Provide fast and dependable internet connections.
  2. Provide fast web registration and hosting services adjusted to the requirements of small office/Home office (SOHO) individuals and businesses.
- **Incident Response Framework:** Create a strong mechanism for detecting, collecting, and responding to security issues throughout HAL's full digital environment, guaranteeing timely and effective threat mitigation.
- **Authentication and Authorisation Network:** Create a secure infrastructure for authentication, authorisation, and asset accounting, with controlled access and transparency.
- **Redundancy and Risk Reduction:** Using technologies like load balancing and cluster management to ensure high availability while lowering the risk of failure or service disruption.
- **SOC 2 Compliance:** Satisfy the strict standards of HAL's VIP clients by achieving SOC 2 compliance, which ensures trust and reliability in HAL's services.  
By focussing on these objectives, HAL will protect its network infrastructure and improve its service offerings, ensuring dependability, trustworthiness, and resilience in the face of emerging cyber threats.

## 1.4 Background and context

In today's world, a solid network infrastructure serves as the foundation for modern organizations. Due to the fast-emerging expansion of networked devices and the ongoing rise of cyber threats, companies must prioritize the security and efficiency of their digital ecosystems. Hierarchical Access Limited (HAL) understands that meeting the criteria of competitive VIP Tech clients and achieving business objectives relies on having a secure, dependable, and compliant network infrastructure. (Ryan et al., 2022)

Research has shown many times that complete network security frameworks that are in line with industry best practices are important. (Jeong and Lingga, 2023). More and more companies are depending on compliance standards like SOC 2 to protect sensitive data, preserve operational continuity, and reduce risk factors.

A complete technique for assessing a service organization's controls across the five trust service criteria—security, availability, processing integrity, confidentiality, and privacy is provided by SOC 2, which was developed by the AICPA. HAL can prove its dedication to protect customer data and compliance to industry accepted security standards by obtaining SOC 2 compliance.

The critical need HAL has for a network infrastructure that emphasizes security, effectiveness, and compliance is immediately addressed by this initiative. By implementing protocols for authentication, authorization, and accounting (AAA), network assets will be carefully controlled. (López-Fernández et al., 2014). Permissions will only be issued to authorised individuals, and all actions will be recorded. Creating and implementing thorough security policies that are adapted to industry standards and HAL's unique needs will offer a methodical way to reduce risks and maintain the security of confidential data.

Given how disruptive unexpected occurrences and technicality faults can be this effort emphasizes business continuity planning. If HAL has a well-developed plan, it will be able to reduce downtime and maintain important operations even in the face of adverse conditions.

By introducing system redundancy into the network architecture, single points of failure can be reduced, increasing availability and reliability. Furthermore, this project will discuss building and deploying multiple cyber defense measures in recognition of the always-changing cyber threat landscape to preserve HAL's irreplaceable digital assets from a variety of malicious actors.

## **1.5 Problem and Statement**

- **State of problem**

Existing literature fully describes the complexities and problems of achieving and sustaining SOC 2 compliance. These issues include technical obstacles, resource limits, employee opposition, and the ongoing possibility of security breaches.

- **Research Gap**

While research recognizes these problems, there is still a lack of understanding of the unique obstacles that small and medium-sized organizations (SMEs) experience in achieving SOC 2 compliance. These organizations frequently work with limited budgets, resources, and cybersecurity knowledge, making the compliance process very difficult. Plus, there is a lack of study into complete solutions customized to the specific restrictions of SMEs attempting to negotiate the complexities of SOC 2 compliance and create a strong security posture.

- **Research problem**

This research investigates the multifaceted issues that HAL faced as it worked towards SOC 2 compliance. It seeks to address the following research question: How can SMEs with limited resources and experience efficiently overcome the technological, financial, and human resource challenges associated with SOC 2 compliance to earn essential agreements, improve their market reliability, and protect confidential data?

### 1.5.1 Justification

Addressing the research gap is critical for a variety of reasons. Initially SOC 2 compliance is fastly becoming a requirement for SMEs to enter commercial collaborations with larger organisations. Failure to meet this level may lead to missed opportunities, stunted growth, and a competitive disadvantage. Secondly, successfully completing the SOC 2 compliance procedure can demonstrate a SME's commitment to data security and improve its reputation in its sector. Finally, by creating a comprehensive roadmap for overcoming the unique challenges that SMEs face in achieving SOC 2 compliance, this study can provide invaluable insights and guidance to other organisations embarking on a similar journey, fostering a safer and stronger company environment.

### 1.6 Research Question

Considering the theoretical framework and empirical evidence presented in the literature review, this thesis will focus on the following research questions:

1. How can a SOC 2 compliant network infrastructure be designed and implemented for a Small to Medium-sized Enterprise (SME) like Hierarchical Access Limited (HAL) using AWS, IDS/IPS systems, and SIEM tools, while considering their specific constraints and requirements?
2. How can we improve and enhance the security posture of Hierarchical Access Limited (HAL), implement SOC2 compliance, secure network infrastructure, and mitigate risks associated with network vulnerabilities, resource strain, and compliance requirements?

### 1.7 Consideration of ethical, professional and social issues

Designing and implementing a SOC 2-compliant network infrastructure, especially one that collects and analyses sensitive data, demands careful consideration of ethical, legal, professional, and social implications. This study is committed to upholding the highest levels of research integrity and following all applicable policies and guidelines.

#### 1.7.1 Ethical Considerations

- **Anonymity and Confidentiality:** All identities, as well as any data that could be used to identify them, will be totally secret. Data will be anonymised and securely kept to safeguard participants privacy.
- **Data Security:** All collected information, including vulnerability scan results, test findings, and transcripts, will be protected by strong security measures. Data will be encrypted, and only authorised person will have access to it.

#### 1.7.2 Legal Considerations

- **Data Protection:** All data collection and processing activities must follow applicable data protection laws, such as the General Data Protection Regulation (GDPR). This involves gaining express agreement for data gathering, verifying data accuracy, and granting persons the ability to access and correct their personal information.
- **Cybersecurity Regulations:** The network infrastructure will be built to comply with applicable cybersecurity laws, including the UK Cybersecurity Act 2018 and the

Network and Information Systems (NIS) legislation 2018. This ensures that HAL's systems and processes meet or exceed the basic security requirements.

### 1.7.3 Professional Considerations

- **Research Integrity:** The project will be carried out with the highest integrity and transparency. All research methods and conclusions will be accurately documented, and any limitations or limitations will be fully stated.
- **Professional Standards:** The project will follow the ethical norms and professional standards established by relevant professional organisations, including the British Computer Society (BCS) and the Association for Computing Machinery (ACM).

### 1.7.4 Social Consideration:

- **Societal Impact:** This study intends to contribute to the larger goal of improving cybersecurity for small and medium-sized enterprises (SMEs), which are critical to the economy. This study's practical suggestions and insights will help SMEs better protect their vital assets and data, resulting in a more secure digital ecosystem.
- **Public Awareness:** The findings of this study will be distributed through suitable means, such as academic publications and industry conferences, to increase understanding of the problems and opportunities related with SOC 2 compliance for SMEs.

By carefully investigating these ethical, legal, professional, and social factors, this project hopes to do research that is not only important and influential, but also responsible and useful to society.

### **LITERATURE REVIEW**

#### **2.1 Searching for Literature**

To find and collect scientific publications for evaluation, the following databases were used: IEEE Xplore, ACM Digital Library, ResearchGate, Google Scholar, and Semantic Scholar. To maximise search results the following keywords were used cyber-security, critical infrastructure, SOC2, AWS, load balancer, and training. The conditional logic statement below explains how the keywords were used to create search combinations: ((Cyber-security OR Cybersecurity) AND (Critical Infrastructure OR SOC2 OR AWS OR Load Balancer) AND (TRAINING)). This generated a total of eight keyword combinations. The initial database search produced 106,211 records. To avoid omitting significant articles from the evaluation, I expected the specified search term to produce many results, including duplicates and unrelated content.

#### **2.2 Literature review**

In the context of designing and implementing a SOC 2 compliant network infrastructure for Hierarchical Access Limited (HAL), the literature review will primarily focus on articles discussing the importance of strong cybersecurity infrastructure and the significance of SOC 2 compliance in protecting sensitive data and maintaining the confidence of clients. The papers on the use of AWS cloud services, load balancing, and other relevant technologies will also be reviewed, as they provide practical solutions and insights into constructing a secure and scalable network infrastructure that meets HAL's specific goals and objectives.

##### **2.2.1 SOC 2 Compliance and ISO Standards: A comprehensive Approach to Network Security**

With the growing complexity of cyber threats organisations of all sizes must prioritise effective network security. In keeping with previous research, this study acknowledges the importance of SOC 2 compliance, not only as a security framework but also as a demonstration of an organizations commitment to protecting sensitive data (Monev, 2020). The importance of SOC 2 compliance is heightened when combined with international standards such as ISO/IEC 27001 and ISO/IEC 27002, which provide a comprehensive framework for information security management systems (ISO/IEC 27001:2013; ISO/IEC 27002:2013).

These standards strengthen SOC 2 by providing extensive guidance on risk assessment, control selection, and continuous improvement, ensuring that security measures are not only deployed but also periodically examined and improved.

This study recognises the various approaches to network infrastructure design suggested in the literature, including the zero-trust model advocated by (Nadaf et al., 2014) . However, given the resource constraints that SMEs frequently confront, this research seeks to strike a balance between strong security and practicality. It will look at how AWS cloud services, together with IDS/IPS and SIEM technologies, can be used to create a secure but managed network environment that meets both SOC 2 and ISO standards.

Furthermore, the study will investigate the proactive strategy to risk reduction and incident response that has been highlighted in the literature(Johansen, 2023). This includes not only taking preventative measures, but also actively looking for vulnerabilities and devising quick reaction tactics. Organisations that take a proactive posture can greatly lessen the potential effect of security events.

However, as noted in the literature, transitioning to a SOC 2 compliant network infrastructure is not without obstacles especially for SMEs (Henriques et al., 2024).This study aims to fill this space by focussing on the specific setting of HAL. By studying HAL's specific limits and priorities, this study hopes to provide concrete advice that are both successful and feasible for organisations with low resources. The study will also assess the impact of the implemented solutions using quantitative measurements, in line with recent research that prioritises measurable results (Sun, 2022).

Furthermore, this study seeks to give a road map for SMEs to negotiate the complexities of network security and achieve SOC 2 compliance, thereby contributing to a more secure digital ecosystem.

### **2.2.2 SOC 2 Compliance as a Cornerstone of Network Security**

The rising complexity and frequency of cyber threats require strong security measures for organisations that handle sensitive data.(Wang et al., 2024). The AICPA (2018) developed the Service Organisation Control 2 (SOC 2) framework, which has emerged as a baseline for assessing security, availability, processing integrity, confidentiality, and privacy of service provider systems. (Kanpariyasoonporn and Senivongse, 2017)

Recent research has shown the link between SOC 2 compliance and a stronger security posture. The Ponemon Institute (2020) discovered that compliant organisations were far less likely to have data breaches. This correlation shows that SOC 2 strict controls make a major contribution to a stronger security environment.(Roy, 2020)

### **2.2.3 Network Infrastructure Design: Balancing Security and Performance**

Effective network architecture is essential for achieving SOC 2 compliance and improving overall security. A well designed infrastructure includes many layers of defence, such as firewalls, IDS/IPS and strict access controls. (Yang et al., 2018)

To achieve this level of balance, researchers have looked into numerous network topologies and technologies. (Ganesh et al., 2023) advocate for a zero-trust architecture, which views all people and devices as potential threats. This strategy reduces unauthorised access and lateral movement within the network. However, the increasing complexity of such systems may make implementation difficult, especially for organisations with limited resources.

#### **2.2.4 Risk Mitigation and Incident Response: A Proactive Approach**

A comprehensive network security plan, in addition to safeguards, requires strong risk mitigation and incident response capabilities. This includes detecting and assessing threats, developing reaction plans, and implementing detection and remediation technologies.

(Park and Ahn, 2021)

Proactive threat hunting is emphasised in modern literature. Rather than passively waiting for signals, security teams actively look for evidence of compromise. This proactive method provides early threat elimination, possibly avoiding significant damage. (Kumar et al., 2021)

#### **2.2.5 Cloud Computing and Security Tools: AWS, IDS/IPS, and SIEM**

Cloud platforms like Amazon Web Services (AWS) have changed IT infrastructure management. AWS provides a variety of security services, including VPCs, WAFs, and IAM solutions. These tools can be used to design a secure and scalable network infrastructure that meets SOC 2 requirements. (Bundela et al., 2022)

Integrating IDS/IPS and SIEM tools improves security. These solutions enable real-time visibility into network traffic, allowing for faster detection and reaction to security events. (Khande et al., 2023) However, the success of these technologies is heavily dependent on appropriate configuration and regular maintenance.

#### **2.2.6 Challenges and Considerations for Small and Medium-sized Enterprises (SMEs)**

While the advantages of SOC 2 compliance and strong network security are apparent implementation can be difficult, especially for SMEs. These organisations frequently have few resources and technical skills. According to (Kandpal et al., 2023) the most major obstacles to SOC 2 compliance for SMEs are cost and complexity. As a result, it is critical to investigate cost-effective alternatives and prioritise necessary security controls depending on the organizations unique risk profile.

### **2.3 Research Gap and Proposed Study**

While existing literature extensively covers individual components of network security, such as SOC 2 compliance frameworks, cloud-based infrastructure (AWS), and advanced security tools like IDS/IPS and SIEM, there is a noticeable gap in research that addresses the integration of these elements within the specific context of Small and Medium-sized Enterprises (SMEs). (Iyamuremye and Shima, 2018)

SMEs frequently confront obstacles in establishing strong security measures because to limited finances, technical resources, and the need to reconcile security with operational efficiency. This research space has resulted in a shortage of practical recommendations aimed to the needs of SMEs, limiting their capacity to effectively adopt comprehensive security solutions that meet the diverse character of modern cyber threats.(Fleron et al., 2023)

Furthermore, current research frequently focuses on large companies with extensive IT teams and resources. SMEs' particular constraints and requirements, such as small IT teams and financial limits, requires a network security strategy that is suited to their specific context and risk profile.(Mmango and Gundu, 2023)

## **2.4 Proposed Study**

This study aims to fill this gap by developing, installing, and assessing a SOC 2 compliant network architecture built exclusively for Hierarchical Access Limited (HAL), a fictitious SME. The study will take a mixed methods approach, collecting and analysing data using both quantitative and qualitative methodologies. (Alghamdi et al., 2019)

The qualitative part will involve a comprehensive assessment of HALs existing security infrastructure, policies, and procedures. This analysis will identify areas for improvement, potential vulnerabilities, and opportunities to align security measures with HAL's specific operational requirements and risk tolerance (Alghamdi et al., 2019).

The quantitative part will include deploying the specified solution with AWS cloud services, IDS/IPS systems, and SIEM tools, as well as thorough testing and analysis to determine its effectiveness. This will comprise vulnerability assessments, penetration testing, and incident response simulations to determine the resilience of the implemented infrastructure. (Arenda and Popov, 2019)

The study will also monitor key performance indicators (KPIs) such as the frequency of security events, mean time to detection (MTTD), and mean time to respond (MTTR) before and after implementing the solution. This will quantitatively measure the solution influence on HAL's security posture.

## **2.5 Expected Outcomes**

The outcomes of this study are expected to throw light on the challenges and best practices involved with deploying SOC 2 compliant network infrastructures for SMEs. The study will also provide a complete methodology and actionable recommendations for SMEs to improve network security and achieve SOC 2 compliance cost-effectively and efficiently. (Carias et al., 2020)

By addressing this research, this study hopes to add to the body of knowledge in network security and provide practical advice to SMEs looking to secure their essential assets and data in an increasingly complicated threat scenario.



### **Methodology**

#### **3.1 Research Design**

This research attempted a descriptive research design focusing on the analysis and synthesis of existing data security and protection regulations. This approach was chosen due to its suitability for investigating the complex and multifaceted nature of SOC 2 compliance, particularly within the context of Small and Medium-sized Enterprises (SMEs). Descriptive research allows for a comprehensive understanding of the current state of compliance practices and regulations, providing a solid foundation for developing effective solutions.

The reliance on secondary data sources including regulatory documents, industry reports, scholarly articles, and other relevant publications, was a deliberate choice. This approach circumvented the need for primary data collection from individuals or organizations, thereby eliminating the requirement for ethical approvals and potential limitations imposed by the university. Moreover, it granted access to a vast repository of reliable and comprehensive information on compliance practices, enabling a deeper exploration of existing frameworks and their industry specific applications. This proved instrumental in developing the infrastructure and security measures proposed in this thesis.

#### **3.2 Data Collection and Analysis**

The data collection process was systematic and rigorous, involving a combination of information research and a comprehensive review of online resources. Search strategies were carefully crafted to identify relevant regulatory documents, industry reports, and scholarly publications pertaining to SOC 2 compliance, network security, and data protection. To guarantee that the identified sources were of high quality and relevant, inclusion and exclusion criteria were developed.

Data extraction involved a meticulous review of the identified documents, focusing on key aspects such as existing regulations their applicability conditions compliance requirements across different industries and best practices for network security. Official regulatory publications and reports served as primary sources of information providing authoritative insights into current compliance standards and practices.

The collected data was then synthesized and interpreted to gain a big understanding of the compliance landscape and identify potential gaps or challenges faced by SMEs. This analysis informed the development of the proposed infrastructure, ensuring its alignment with regulatory requirements and industry best practices.

### 3.3 Development Approach

#### Agile with Lean Methodology

An Agile development approach infused with Lean principles guided the project's execution. This hybrid methodology fostered flexibility, adaptability, and customer-centricity, allowing for iterative development and responsiveness to feedback. The Agile framework enabled the project to be broken down into smaller, manageable iterations, with regular check-ins and reviews to ensure alignment with HAL's evolving needs.



The integration of Lean principles, such as value stream mapping and continuous improvement, played a pivotal role in optimizing processes and eliminating waste. By identifying and addressing inefficiencies, the project was able to enhance overall productivity and deliver value more effectively.

The combined Agile and Lean approach proved to be a powerful tool for navigating the complexities of the project. It facilitated effective collaboration, rapid progress, and a focus on delivering tangible value to HAL.

### 3.4 Development Phase

The development process unfolded in several distinct phases, each contributing to the successful implementation of the proposed solutions.

1. **Infrastructure Implementation:** This phase laid the groundwork for the project, involving the deployment of core infrastructure components such as Active Directory Domain Services (ADDS), DNS, DHCP, and RADIUS. These technologies enabled

centralized user and computer management, secure authentication, efficient name resolution, and streamlined device configuration.

2. **Security Enhancement:** A comprehensive security plan was devised and executed, encompassing various aspects such as network security, secure installations, and seamless integration with existing systems. This phase focused on fortifying HAL's defenses against cyber threats and ensuring compliance with SOC 2 standards.
3. **Security Assessments and Communication:** Extremely thorough and careful security assessments, including forensic audits, vulnerability scanning, and intrusion detection, were conducted to evaluate the effectiveness of the implemented security measures and identify any potential weaknesses. The findings of these assessments were communicated clearly and transparently to all stakeholders, fostering a culture of security awareness and accountability.
4. **Risk Management:** A thorough risk assessment was performed to identify potential vulnerabilities and threats. This analysis informed the development and implementation of appropriate mitigation strategies, proactively addressing potential risks before they could materialize.
5. **Testing and Review:** Prior to production deployment a sanity test was conducted to validate the functionality and effectiveness of the implemented solutions. The risk report and security measures were then thoroughly reviewed, ensuring a shared understanding of the security posture and a commitment to ongoing vigilance.
6. **SIEM Solution Refinement:** Following initial testing with Splunk and snort for security information and event management and IDS/IPS functionality we moved to Elastic stack. This decision was made because of Elastic stack superior integration capabilities and its strong machine learning features enabling more effective threat detection and providing HAL with a comprehensive security solution.

### 3.5 Techniques and Approaches to Create a Secured Network

A multilayered security approach was implemented, employing a range of methodologies and best practices to construct a secure and resilient network infrastructure:

- **In-depth Defense:** Multiple layers of security, including firewalls, intrusion detection and prevention systems, and antivirus software, were deployed to create a defense-in-depth strategy. This approach ensured that even if one layer of security was breached, others would remain in place to protect sensitive data and systems.
- **People and Processes:** Recognizing that technology alone is not sufficient to ensure security, a strong emphasis was placed on people and processes. Security policies were developed and enforced, regular security awareness training was suggested in the phase, and clear communication channels were established to report and address potential security incidents.
- **Security Zones and User Roles:** Network segmentation and the principle of least privilege were employed to restrict access to sensitive data and systems. User roles and

permissions were carefully defined to ensure that individuals had access only to the resources necessary for their job functions.

- **System Integrity:** Network devices, servers were hardened through regular updates, patches, and vulnerability scans. This proactive approach helped to minimize the risk of exploitation and ensure that systems remained secure and up to date.
- **Endpoint Compliance:** A strong endpoint compliance framework was implemented to control device network admission. This ensured that only authorized and secure devices could connect to the network, reducing the risk of unauthorized access or malware infections.
- **Network Management Protection:** Network management information was protected using VLANs and strong security mechanisms such as IPsec, SNMPv3, SSH, and TLS. This prevented unauthorized access to critical network configuration data and ensured the confidentiality and integrity of network management communications.
- **User Information Protection:** Sensitive user information was safeguarded through a combination of VPNs, encryption protocols, and network segmentation. This layered approach helped to protect against unauthorized access, data breaches, and spying.
- **Threat Awareness and Mitigation:** Proactive measures, such as anti-spoofing, bogon blocking, and denial-of-service prevention, were implemented to detect and mitigate potential threats. Regular security monitoring and analysis were conducted to identify and address emerging risks.
- **Security Tools:** A suite of security tools, including firewalls, intrusion detection and prevention systems, antivirus software, and vulnerability scanners, was deployed to provide comprehensive protection against a wide array of threats.
- **Event Management:** Security and audit event information was logged, correlated, and managed using a centralized system. This enabled the identification of patterns and trends, facilitating proactive threat detection and response.
- **Centralized Management:** A centralized network management system was implemented to streamline the administration and monitoring of network devices. This provided a unified interface for configuring and managing the network, improving efficiency and reducing the risk of errors.
- **Automated Monitoring and Alerting:** Automated monitoring and alerting systems were deployed to provide real-time visibility into the networks health and security posture. These systems generated alerts in response to potential issues, enabling rapid response and minimizing downtime.
- **Regular Audits and Assessments:** Periodic security audits and assessments were conducted to evaluate the effectiveness of security measures and identify areas for improvement. These assessments helped to ensure that the network remained compliant with SOC 2 standards and industry best practices.
- **Security Policies and Training:** Clear and comprehensive security policies were developed and enforced, outlining the roles and responsibilities of all personnel in maintaining network security. Regular security training was provided to ensure that all employees were aware of the latest threats and best practices for mitigating them.

This multi-faceted and proactive approach to network security aimed to create a strong and resilient infrastructure capable of withstanding the ever-evolving threat landscape while ensuring compliance with SOC 2 standards.

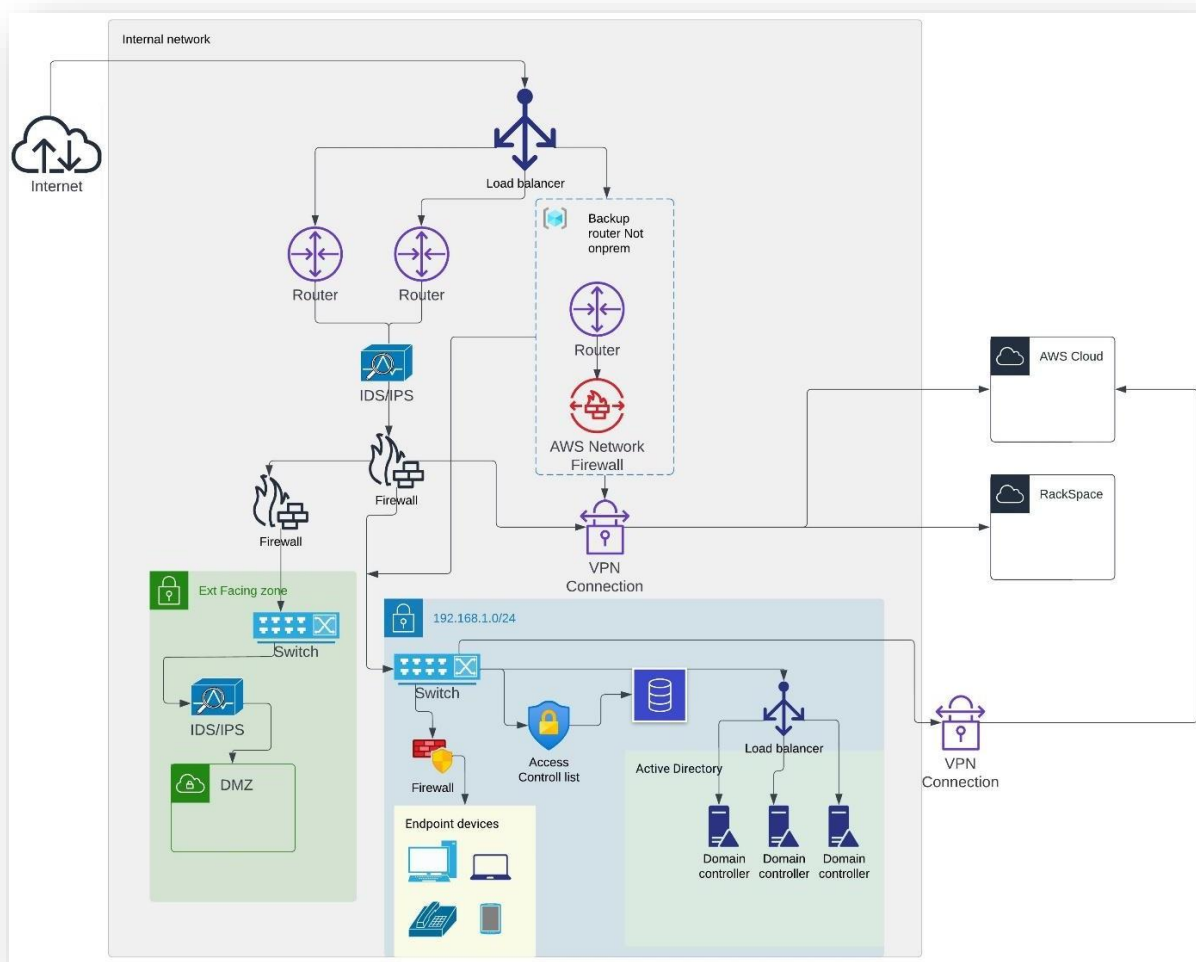
### **3.6 Critical Reflection**

The descriptive research design and reliance on secondary data sources proved effective in achieving the research objectives. The wealth of available information on compliance practices and regulations enabled a comprehensive understanding of the challenges faced by SMEs in achieving SOC 2 compliance. However, it is important to acknowledge that this approach may have inherent limitations. The reliance on secondary data may introduce potential biases or inaccuracies and the findings may not be generalizable to all SMEs due to the unique context of HAL. Future research could explore alternative methodologies, such as surveys or interviews, to gain further insights into the lived experiences of SMEs navigating the SOC 2 compliance journey.

## Development, Implementation and testing through Experimentation, results and Discussions

### 4.1 Network structure

To start, i need to recreate the network diagram to increase its resilience and improve overall network performance. To enhance network security, I have decided to implement the following network layout:



The proposed network structure includes a multi-layer architecture that divides the network into several layers, each with its own specific functions and access controls. For example, I suggest creating a DMZ layer to separate external-facing services like web hosting from internal networks. Internal networks should be further divided into subnets based on departments or

user roles, with appropriate access controls and firewalls.

For internal networks, I recommend dividing them into multiple subnets based on departments or user roles. This allows for more granular access controls and security measures. Each subnet should have appropriate firewalls and access controls to ensure that access is restricted to authorized personnel only. While this is not depicted in the diagram, it requires additional resources and time to plan, which can only be done after this model has been accepted.

Implement a secure VPN connection for remote access, segment the network to prevent unauthorized access and limit the spread of security breaches, and use an intrusion detection and prevention system to monitor the network for suspicious activity. I advise regularly updating and patching all systems, using strong authentication mechanisms and access controls, and performing regular security audits and assessments. By implementing these steps, I can ensure that the network is secure, properly maintained, and functioning at optimal levels. In addition, it is recommended to have a team member or an external service provider who is responsible for monitoring the network on a regular basis. This person should be well experienced in network security principles and should be able to promptly identify and address any difficulties that occur.

To ensure that the network is properly maintained, it is important to document all network configurations and changes. This documentation should be updated and freely accessible to all members of the team. By having clear documentation, team members can quickly troubleshoot any issues that arise, reducing downtime and ensuring that the network is functioning properly.

## **4.2 Implementation of SOC 2 Compliance Program**

### **4.2.1 Identify the type of SOC2 Report**

Since SOC 2 includes 2 types, Type I and Type II. The first one is a point-in-time report which assesses the company's policies, procedures, and security controls to see if they meet SOC 2 requirements or not. SOC 2 type II normally takes 6 – 12 months, because auditors must observe and evaluate all the evidence from the company's system to determine all of the designs & controls were operating effectively over time.

Since the HAL has never been certified before, Type I is a good starting point for the company at this time since it takes less time and effort to prepare and complete the report. After HAL computer network satisfies requirements, I can take advantage of certification oriented outcomes to achieve the SOC 2 type II later, which is more comprehensive and insightful.

### **4.2.2 Define the Scope of Audit**

The SOC 2 audit scope is based on five Trust Services Criteria: Security, Confidentiality, Availability, Processing Integrity, and Privacy. The scope is defined by HAL's business: the type of data that the company has been storing or transmitting. "Security", of course, is the first criterion on the list. "Availability" for down-time management. And "Confidentiality" is a must go option since HAL's been storing a lot

of sensitive and nondisclosure information. Since HAL isn't executing any critical operations, nor storing personally identifiable information, I can exclude Processing integrity and Privacy from the scope. Most of the Internet service providers only need Security, Availability, and Confidentiality criteria. For example: Amazon AWS and Microsoft Azure have claimed the same criteria.

#### **4.2.3 Internal Risk Assessment**

Risk Assessment and Mitigation are crucial, not only for SOC 2 compliance but also for any organization. Relevant departments (Application, Network, System...) must join to identify and assess all the possible risks involved in the company's daily operation and suggest control measures. This will help to eliminate the likelihood of threats, vulnerabilities, and data breaches, prevent fines and lawsuits, protect the company's resources, and especially, the success of this SOC 2 compliance.

#### **4.2.4 Perform Gap Analysis and Remediation**

Gap analysis is essential, IT departments need to review its existing policies, procedures, and controls to have a better understanding of company mission-critical, and current security posture, to see strengths and weaknesses and point out which controls need to implement to meet the applicable criteria.

After gap analyzing, HAL will need some time on remediation to ensure all the mandatory controls are being achieved. For instance, Security criteria require two-factor authentication, that is why I offer to employ Okta multi-factor authentication service in the proposal. Necessary changes and new implementation will be made to close the gaps.

#### **4.2.5 Establish Continuous Monitoring Practices**

I have been working on a Type I audit for HAL. After achieving the Type I report, I can be assured the process of monitoring is always in place to prepare the strong data for the next Type II audit which will be in the next 6 months. Furthermore, SOC 2 certification isn't a one-time event, the companies must be audited every year to maintain their compliant status.

### **4.3 Deployment of Network Infrastructure**

The current implementation of the infrastructure is limited due to resource constraints. However, we have still managed to deploy critical components such as the Domain Controller, RADIUS server, DNS, DHCP, Firewall, and identity/access management services.

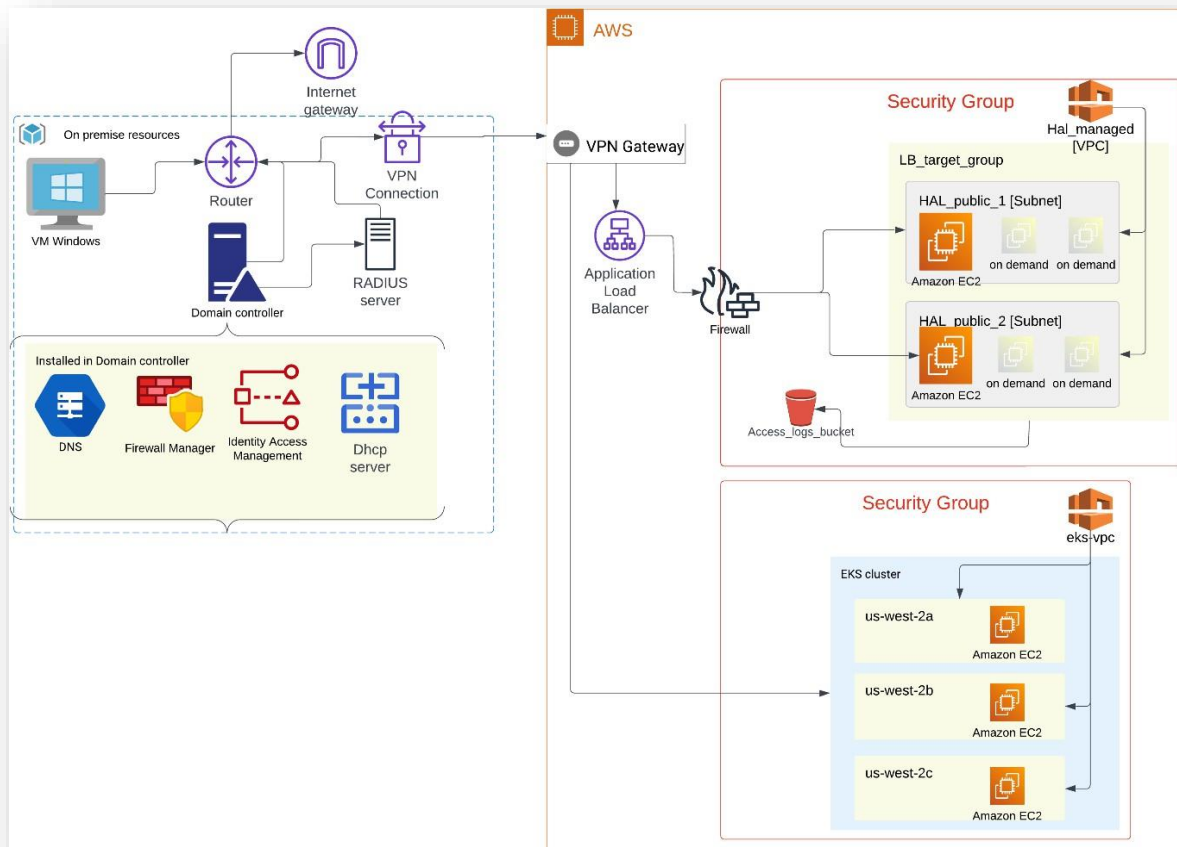
Once the plan is developed, I will move forward with the full-scale deployment of the infrastructure. This will allow us to deploy additional components and features that are necessary to meet the needs of an organization and enhance the functionality and security of our infrastructure.

By leveraging the latest technology and best practices, I will be able to ensure that organization's IT operations are secure, efficient, and reliable, helping us to achieve organizational goals and meet the needs of our clients and stakeholders.



The initial exploration of SIEM and IDS/IPS functionalities involved Splunk and Snort. However, to enhance threat detection and get advanced capabilities the project moved to Elastic Stack. This strategic shift was driven by Elastic Stacks seamless integration and its strong machine learning features empowering HAL with a more comprehensive security solution.

## Implementation of network



### 4.4 Implementation [on-premises]

The implementation of on-premises infrastructure, leveraging virtualization technology and incorporating a Domain Controller, RADIUS server, and other critical services, will be instrumental in helping achieve SOC2 compliance. SOC2 is a renowned standard for assessing the security, availability, processing integrity, confidentiality, and privacy of cloud and other SaaS-based service providers. SOC2 compliance requires the installation of a complete security program, which includes the use of physical and logical access controls, as well as the adoption of robust security mechanisms such as firewalls and intrusion detection and prevention systems. By implementing a Domain Controller, DHCP, DNS, Firewall, and identity/access management services within our infrastructure, we have already taken important steps towards meeting these requirements.

In addition, implementing a RADIUS server would improve network security by enabling network-level authentication, guaranteeing that only authorized users can access our network

resources. This will assist in preventing unauthorized access and potential data breaches, which are critical considerations for SOC2 compliance.

Using virtualization technology, I can simulate all of the components needed for infrastructure in a controlled environment, making it easier to manage and debug any difficulties that may develop. This will also allow us to test and assess the infrastructure and security measures in a safe and secure environment before deploying them in a production setting.

Finally, installing a client workstation that can connect to the domain will give us a realistic environment in which to test and demonstrate the functionality of infrastructure. This will assist me in identifying any potential security vulnerabilities and implementing extra security measures as required to guarantee compliance with SOC2.

Overall, my implementation of an on-premises infrastructure with virtualization technology, Domain Controller, RADIUS server, and other critical services will be instrumental in helping me achieve SOC2 compliance by meeting the requirements for comprehensive security programs and robust security measures, while also providing a controlled and realistic testing environment.

#### **4.5 Implementation[aws]**

In infrastructure implementation, I have decided to use Terraform as our infrastructure as code tool. Terraform enables us to generate and manage the entire infrastructure through a single file, which can be easily modified as needed in the future. This approach provides significant benefits, including improved agility, consistency, and automation.

SOC2 compliance requires that an organization maintain adequate controls to protect the security, availability, and confidentiality of its systems and data. The utilization of infrastructure as code, load balancers, and the EKS cluster assist in achieving these controls by delivering a secure, available, and resilient environment.

Terraform allows us to easily maintain the infrastructure in a consistent and repeatable manner, which helps to ensure that the infrastructure is secure and compliant with standards. The use of load balancers and EKS cluster enables us to ensure that our infrastructure is highly available and can handle significant loads, minimizing the risk of downtime or service disruptions.

Additionally, the automated change management provided by Terraform allows us to track any changes made to the infrastructure, ensuring that we maintain a clear audit trail and can easily identify any security issues or anomalies. This is critical to SOC2 compliance, as it enables us to demonstrate that our infrastructure is secure, available, and meets industry standards.

Furthermore, the asset management solution provided by Terraform ensures that we have a clear inventory of our infrastructure resources, which is essential to maintaining control over our systems and data. This helps us to ensure that we can quickly and easily identify any unauthorized changes or access to our infrastructure, which is a key component of SOC2 compliance.

Overall, the implementation of Terraform, load balancers, and EKS cluster, along with the

benefits of infrastructure as code, automated change management, and asset management, will provide us with the necessary controls to achieve SOC2 compliance. This will allow us to demonstrate to our clients and stakeholders that we take the security and privacy of their data seriously and are dedicated to upholding industry-leading security and compliance standards.

## 4.6 Load balancer

A load balancer is a networking device that distributes incoming network traffic among numerous servers, preventing any single server from becoming overwhelmed and unable to handle requests. The load balancer serves as a mediator between client devices and the server farm, receiving incoming requests and sending them to the proper server based on server availability, geographic location, and network congestion. This improves the availability, dependability, and scalability of a server infrastructure. Load balancers can be hardware or software-based, and they can serve a range of functions, including web applications, databases, and file servers.

```
# Configure the AWS provider
provider "aws" {
  region = "us-east-1"
}

# Create a VPC and subnets for the load balancer and EC2 instances
resource "aws_vpc" "Hal_managed" {
  cidr_block = "10.0.0.0/16"
}

resource "aws_subnet" "HAL_public_1" {
  cidr_block = "10.0.1.0/24"
  vpc_id     = aws_vpc.Hal_managed.id
}

resource "aws_subnet" "HAL_public_2" {
  cidr_block = "10.0.2.0/24"
  vpc_id     = aws_vpc.Hal_managed.id
}

# Create security groups for the load balancer and EC2 instances
resource "aws_security_group" "alb_sg" {
  name_prefix = "alb_sg_"

  ingress {
    from_port = 80
    to_port   = 80
    protocol  = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

resource "aws_security_group" "ec2_sg" {
  name_prefix = "ec2_sg_"
}
```

```

    ingress {
      from_port = 22
      to_port   = 22
      protocol  = "tcp"
      cidr_blocks = ["0.0.0.0/0"]
    }
  }

  # Create EC2 instances to balance traffic across resource "aws_instance" "EC2_instance_1" {
  ami          = "ami-0c55b159cbfafa1f0" instance_type = "t2.micro" subnet_id      =
aws_subnet.HAL_public_1.id vpc_security_group_ids = [aws_security_group.ec2_sg.id] tags
= {
  Name = "EC2-instance-1"
}
} resource "aws_instance" "EC2_instance_2" { ami          = "ami-0c55b159cbfafa1f0"
instance_type = "t2.micro" subnet_id      = aws_subnet.HAL_public_2.id
vpc_security_group_ids = [aws_security_group.ec2_sg.id] tags = {
  Name = "EC2-instance-2"
}
}

# Create the ALB and listener resource "aws_lb" "HAL_alb" { name_prefix = "halalb" internal
= false load_balancer_type = "application" security_groups =
[aws_security_group.alb_sg.id] subnets = [aws_subnet.HAL_public_1.id,
aws_subnet.HAL_public_2.id] access_logs { bucket = "HAL_alb-access-logs-bucket" prefix
= "lb" enabled = true
}

# Create a listener on port 80 that routes traffic to the target group

}

# Create a target group for the EC2 instances resource "aws_lb_target_group" "target_group1"
{ name = "exg" port = 80 protocol = "HTTP" target_type = "instance" vpc_id =
aws_vpc.Hal_managed.id

```

```

health_check {
  healthy_threshold = 2
  interval          = 30
  path              = "/"
  port              = "80"
  protocol          = "HTTP"
  timeout           = 5
  unhealthy_threshold = 2
}
}

output "arn_value" {
  value = aws_lb_target_group.target_group1.arn
}

# Register EC2 instances with the target group
resource "aws_lb_target_group_attachment" "target_group_attachment_1" {
  depends_on = [aws_lb_target_group.target_group1]
  target_group_arn = aws_lb_target_group.target_group1.arn
  target_id       = aws_instance.EC2_instance_1.id
  port           = 80
}

resource "aws_lb_target_group_attachment" "target_group_attachment_2" {
  depends_on = [
    aws_lb_target_group.target_group1
  ]
  target_group_arn = aws_lb_target_group.target_group1.arn
  target_id       = aws_instance.EC2_instance_2.id
  port           = 80
}

resource "aws_s3_bucket" "HAL_alb_access_logs_bucket" {
  bucket = "HAL_alb-access-logs-bucket"
  acl    = "private"

  versioning {
    enabled = true
  }

  # Block public access to the bucket and its contents
  block_public_acls       = true
  block_public_policy     = true
  ignore_public_acls     = true
  restrict_public_buckets = true

  tags = {
    Name = "HAL_alb-access-logs-bucket"
  }
}

```

First, I created the "us-east-1" region in the AWS provider to indicate where we wanted to create resources. I then used the "aws vpc" and "aws subnet" resources to set up a Virtual Private Cloud (VPC) and two subnets. The VPC's CIDR block is '10.0.0.0/16' whereas the subnets CIDR blocks are '10.0.2.0/24' and '10.0.2.0/24' respectively. These subnets are open to the public and connected to the VPC.

Following that, I used the "aws security group" resource to establish two security groups. The first security group is linked to the Application Load Balancer (ALB) and accepts inbound traffic on port 80 from any IP address. The second security group is associated with the EC2 instances and permits inbound access on port 22 (SSH) from any IP address.

Then, using the "aws instance" resource, I launched two Amazon Elastic Compute Cloud (EC2) instances in the previously configured subnets. Each instance is a member of the "ec2\_sg\_" security group, with the Amazon Machine Image (AMI) ID "ami-0c55b159cbfafa1f0" for Amazon Linux 2. We also named the instances "EC2-instance-1" and "EC2-instance-2".

I then used the "aws lb" resource to create an Application Load Balancer (ALB). The ALB is linked to the "alb\_sg\_" security group as well as the two public subnets. I enabled access logs for the ALB and configured them to be stored in an S3 bucket named "HAL alb-access-logs-bucket".

After that, I used the "aws lb target group" resource to create a target group. The target group specifies that traffic should be routed to HTTP instances on port 80. Health checks are set up to monitor the health of the instances by sending HTTP requests to "/" every 30 seconds with a 5 second timeout. The target group is named "exg" and is associated with the VPC.

Finally, I used the "aws lb target group attachment" resource to associate the EC2 instances with the target group. Each attachment contains the ARN of the target group, the instance ID, and the port number (80). In addition, I created an S3 bucket called "HAL alb access logs bucket" to store the ALB's access logs, and I restricted public access to the bucket's contents.

## 4.7 EKS cluster

I used Terraform to create an Amazon EKS cluster with 3 worker nodes on AWS. I started by creating a new configuration file using a text editor and pasting the Terraform code that we had provided. The configuration file consisted of several blocks of code that performed different tasks, such as creating a new VPC with subnets, creating a security group rule to allow worker nodes to communicate with the EKS control plane, and creating an EKS cluster with worker nodes. Once I had the configuration file ready, I ran the **terraform init** command to initialize the Terraform project and downloaded any necessary plugins. Then, I ran the **terraform apply** command to apply the configuration and create the EKS cluster with 3 worker nodes on AWS. During the process, Terraform created all the necessary resources, such as the VPC, subnets, security group rules, EC2 instances for the worker nodes, and the EKS cluster itself. Once the process was complete, Terraform provided us with the kubeconfig file, which we could use to authenticate and interact with the EKS cluster.

```

provider "aws" {
  region = "us-west-2"
}

module "vpc" {
  source = "terraform-aws-modules/vpc/aws"
  name   = "eks-vpc"
  cidr   = "10.0.0.0/16"

  azs          = ["us-west-2a", "us-west-2b", "us-west-2c"]
  private_subnets = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
  public_subnets = ["10.0.11.0/24", "10.0.12.0/24", "10.0.13.0/24"]
}

resource "aws_security_group_rule" "allow_worker_ingress" {
  type          = "ingress"
  from_port     = 0
  to_port       = 65535
  protocol      = "tcp"
  cidr_blocks   = ["10.0.0.0/8"]
  security_group_id = module.vpc.vpc.default_security_group_id
}

module "eks_cluster" {
  source = "terraform-aws-modules/eks/aws"

  cluster_name = "my-eks-cluster"
  subnets     = module.vpc.private_subnets

```

```

vpc_id = module.vpc.vpc_id

tags = {
  Terraform    = "true"
  Environment  = "dev"
}

}

output "kubeconfig" {
  value = module.eks_cluster.kubeconfig_filename
}

module "eks_nodes" {
  source = "terraform-aws-modules/eks/aws//modules/worker_nodes"

  cluster_name = module.eks_cluster.cluster_id

  instance_type = "t3.medium"
  desired_capacity = 3

  name_suffix = "worker"
  tags = {
    Terraform    = "true"
    Environment  = "dev"
  }
}

```

First, I declare that I am using AWS as our provider, with the region set to "us-west-2". Then, I use a pre-made module from the Terraform Registry called "terraformaws-modules/vpc/aws" to create a VPC with three private subnets and three public subnets. I name the VPC "eks-vpc" and assign it a CIDR block of "10.0.0.0/16". The VPC spans three availability zones in the "us-west-2" region.

I created an AWS security group rule to allow worker ingress traffic from the VPC CIDR block. I use another pre-made module from the Terraform Registry called "terraformaws-modules/eks/aws" to create an EKS cluster named "my-eks-cluster". I associate the EKS cluster with the private subnets created earlier and tag it as a Terraform-managed environment. I output the Kubeconfig file name generated by the EKS cluster module so that it can be used to configure kubectl.



Finally, I used a third Terraform Registry module called "terraform-aws-modules/eks/aws//modules/worker\_nodes" to build worker nodes for the EKS cluster. The worker nodes are launched in an EC2 Auto Scaling Group and connected to the EKS cluster. I said that I wish to use t3. medium instances and launch three of them. I additionally identify the EC2 Auto Scaling Group as a Terraform-managed environment.

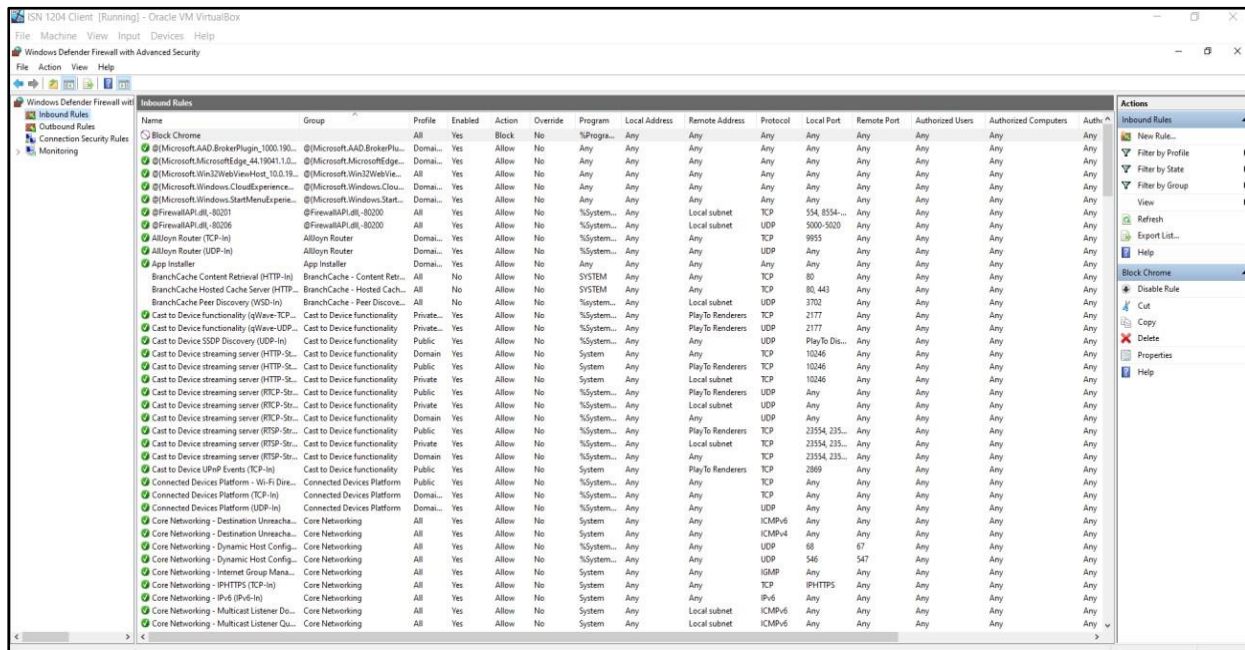
Using infrastructure as code can help by providing a clear and auditable record of the infrastructure configuration, which can be used to demonstrate that the infrastructure meets the requirements of SOC2. Additionally, using infrastructure as code can help ensure that the infrastructure is configured securely by reducing the risk of configuration errors and vulnerabilities. Finally, infrastructure as code can also help with the ongoing monitoring and auditing of the infrastructure configuration, as changes can be tracked and audited over time.

#### **4.8 Implementation of firewall inbound and outbound rules**

Windows Defender Firewall with Enhanced Security offers host-based, two-way network traffic filtering to prevent unauthorised network activity from entering or exiting the local device. The following best practices for installing Windows Firewall can help to maximize security for networked devices. These principles apply to both household and commercial desktop/server systems and encompass a wide range of implementations. Administrators will then need to employ rules (also known as filters) to modify these profiles so that they can be used with user apps or other types of software. For example, an administrator or user may opt to add a rule, open a port or protocol, or allow certain types of traffic to accommodate software. In numerous cases, allowing inbound traffic types will be necessary for apps to run on the network. While approving these incoming exceptions, administrators will consider the following rule precedence behaviors. The default block setting will be overridden by explicitly declared allow rules.

1. Any conflicting allow rules will be superseded by explicit block rules.
2. Unless there are explicit block restrictions, more particular rules will take precedence over fewer specific rules.

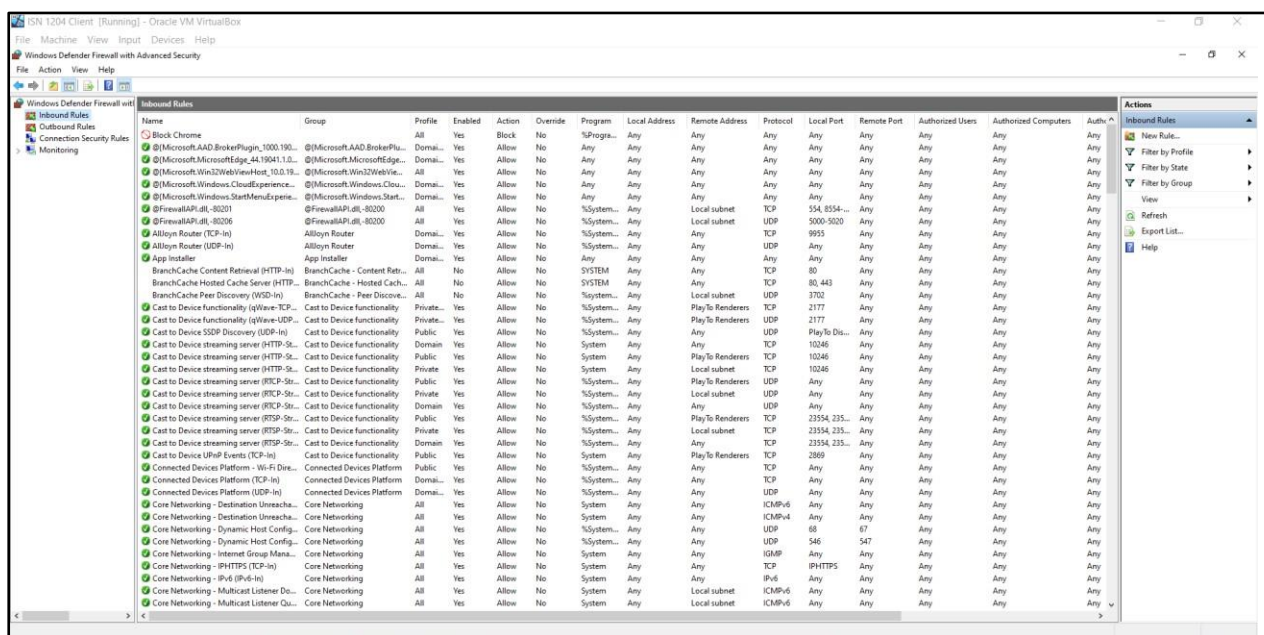
Because of point 1 and 2, it's crucial to check for any other explicit block rules that can unintentionally overlap with the set of policies we're building and impede the traffic flow we want to enable. However, wherever possible, utilize sequential ranges or subnets rather than single addresses or ports when enacting new rules that make use of ports or IP addresses. This strategy saves the development of many internal filters, minimizes complexity, and aid in preventing performance degradation.



## 4.9 Inbound rules

Following initial configuration, networked programs and services sent an alert call including the protocol and port information required for them to function properly. The Windows Defender Firewall has a default block action thus, inbound exception rules must be configured to enable this traffic. This firewall rule is normally added by the application or during installation. Additionally, a rule must be manually created by the user or the firewall administrator on their behalf. When an application is launched or attempts to connect to the network for the first time a dialogue box prompts the user to allow or block an applications packet if no active application or administrator defined allow rules exists.

The user will be asked if they have administrative privileges. Block rules will be set if they choose to ignore or act on the prompt. Typically, two rules are written: one for TCP traffic and another for UDP traffic. If the user does not have local administrator privileges, they will not be prompted. Block rules will normally be created



## 4.10 Outbound Rules

In some exceptionally secure scenarios, the Blocked for Outbound Rules default configuration can be used. However, the configuration of the incoming rule will never be changed such that traffic is accepted by default.

To ease app deployments, most deployments should be set to Allow Outbound by default, unless the firm priorities severe security limitations over usability.

In high-security environments, we, the administrators, will collect and log an inventory of all enterprise-spanning programs. Records include information on whether a particular app requires a network connection. When an app wants network access, we administrators create new rules for that app and distribute them centrally using group policy, mobile device management, or both (in hybrid or co-management setups).

## 4.11 Required Ports

To suit the needs of programmers and information technology (IT) specialists, the Windows Server system offers a thorough and integrated architecture. This system runs applications and services that let us rapidly and conveniently gather, analyse, and share information. These Microsoft client, server, and server program products communicate with client computers and with other server systems via the network using various network ports and protocols. We also need to have host-based firewalls, dedicated firewalls, and Internet Protocol security (IPsec) filters to assist safeguard the network. A specific server will stop responding to client queries if these technologies are set up to restrict the ports and protocols that it uses. The following list provides an overview of the different ports we will be using:

- Port 80 (HTTP): • This is the standard port for web traffic. It is used to deliver

web pages via the internet.

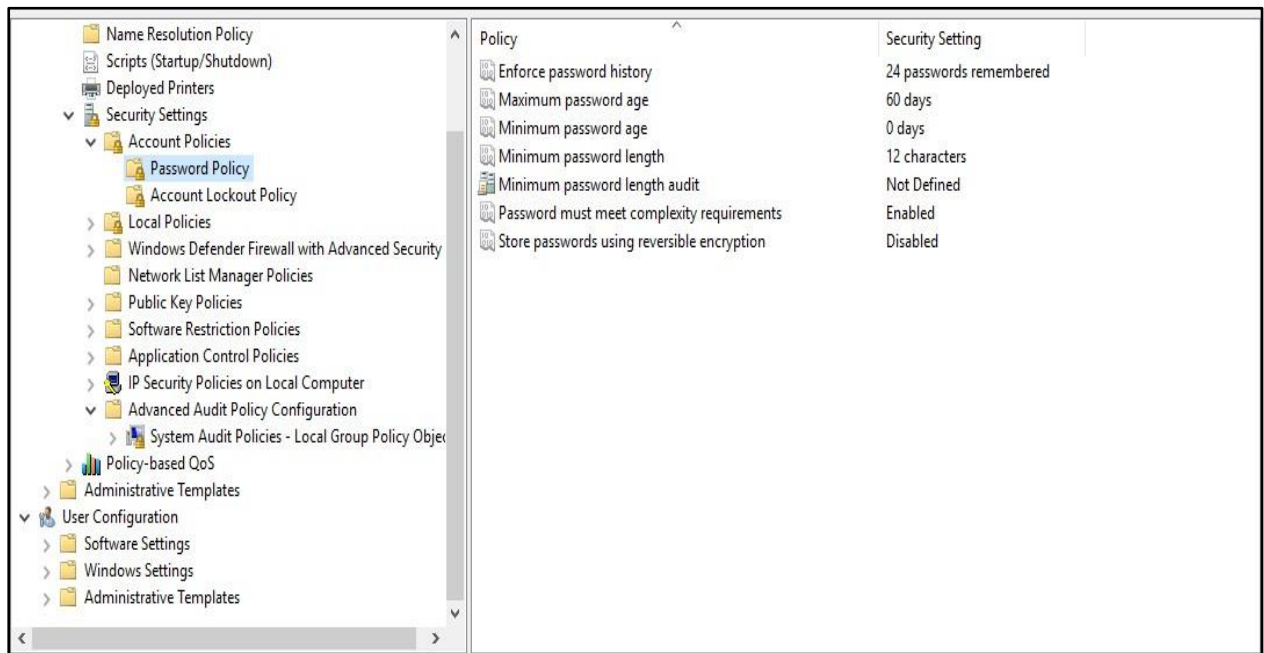
- Port 443 (HTTPS): This is the default port used for secure web traffic. It serves web pages across the internet with SSL/TLS encryption.
- Port 22 (SSH): This is the default port for SSH connections. It is used to remotely administer servers and securely transfer files.
- Port 21 (FTP): This is the default port for FTP connections. It is used to transport files from servers to clients.
- Port 25 (SMTP): This is the default port for SMTP connections. It's used to transfer email messages across servers.
- Port 143 (IMAP): This is the default port for IMAP (Internet Message Access Protocol) communications. It retrieves email messages from servers.
- Port 110 (POP3): This is the default port for POP3 connections. It is used to retrieve email messages from the servers.
- Port 3306 (MySQL): This is the default port used for MySQL database connections. It's used to manage databases and run SQL queries.
- Port 5432 (PostgreSQL): This is the default port used for PostgreSQL database connections. It's used to manage databases and run SQL queries.
- Port 27017 (MongoDB): This is the default port used for MongoDB database connections. It's used to manage databases and run queries.

## **4.12 Implementation of security policies**

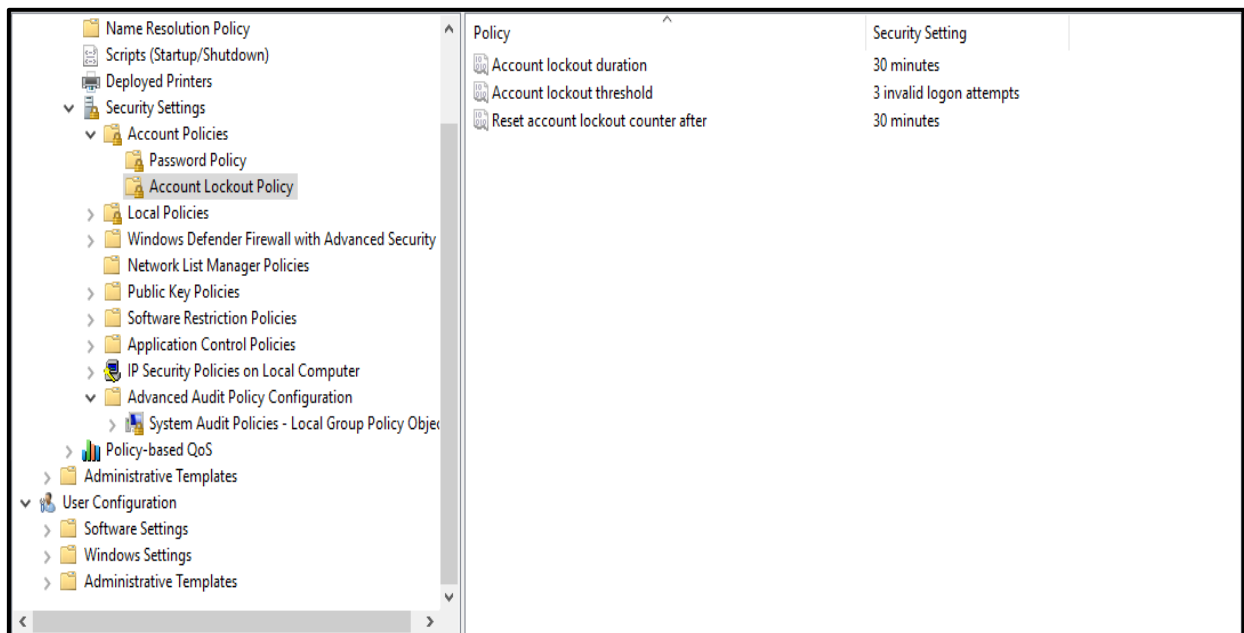
### **4.12.1 Implementation of Account & Password**

I started with enhancement of account & password policies which come along with Windows Active Directory Group Policies feature. First thing, I made some change in the Password policies, includes:

- 12 characters minimum password length with complexity enabling.
- 30 days of maximum password age.
- 24 passwords will be recorded and cannot be re-used.



To avoid brute force or dictionary attacks, I also implemented password lockout policies that apply 30 minutes lockout after 3 failed attempts.



And to improve the security level I also studied the IT Department experience at beginning of the project, to determine who and which level of access that individuals can have on specific resources. For example: Normal users cannot access to any servers, network devices; or

Network Engineer have limited access to Servers and the same for System Engineer on Router & Firewalls...

I also integrated multi-factor authentication (MFA) to Microsoft Active Directory and Office 365 that help secure the workplace environment. Amazon AWS were enabled with MFA, for those who are working on HAL infrastructure as well as managing customers' assets, they must authenticate themselves one more time before access to networks.

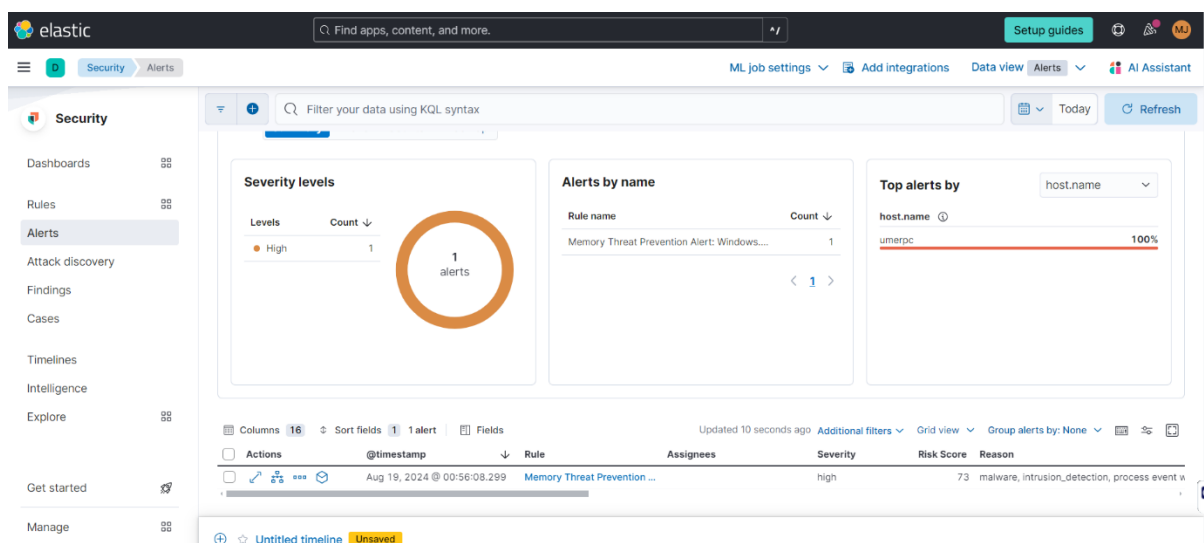
## 4.12.2 Elastic Stack

### IDS/IPS Rules Overview

Rule	Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
New Okta Authentication Behavior...	47	Med...	13 minutes a...	Warn...	1 hour ago	On	On
Privileges Elevation via Parent Pr...	73	High	5 minutes a...	Succ...	1 hour ago	On	On
Network Activity Detected via Kw...	21	Low	5 minutes a...	Succ...	1 hour ago	On	On
Persistence via Update Orchestr...	73	High	4 minutes a...	Succ...	1 hour ago	On	On
Unknown Execution of Binary wit...	47	Med...	3 minutes a...	Warn...	1 hour ago	On	On
Account Password Reset Remotely	47	Med...	3 minutes a...	Succ...	1 hour ago	On	On
Endpoint Security	47	Med...	4 minutes a...	Warn...	44 minutes ago	On	On
Incoming Execution via PowerSh...	47	Med...	3 minutes a...	Succ...	1 hour ago	On	On
Microsoft 365 Exchange Transp...	47	Med...	3 minutes a...	Warn...	1 hour ago	On	On

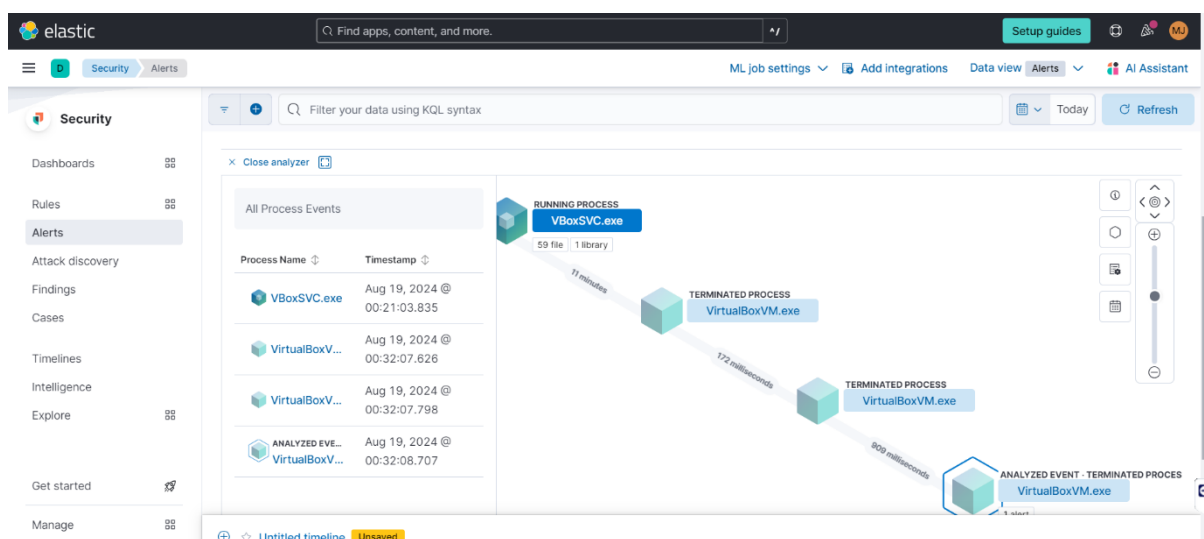
This graphic shows the Elastic Security SIEM interface, notably the "Rules" area. It showcases the use of pre-built Elastic detection rules to monitor and detect potential security threats. The key information shown is rule names, associated integrations, risk scores, severity levels, and enabled/disabled state. The interface allows for filtering, sorting, and managing these rules, as well as the ability to create custom rules, albeit none are currently present in this view.

## SIEM Alerts



This image displays the Elastic Security SIEM "Alerts" dashboard, which provides a visual overview of security notifications. The dashboard indicates one "High" severity alert linked to "Memory Threat Prevention," which affects the hostname "unrarc." This view allows for a fast assessment of the security situation and the prioritisation of incident responses.

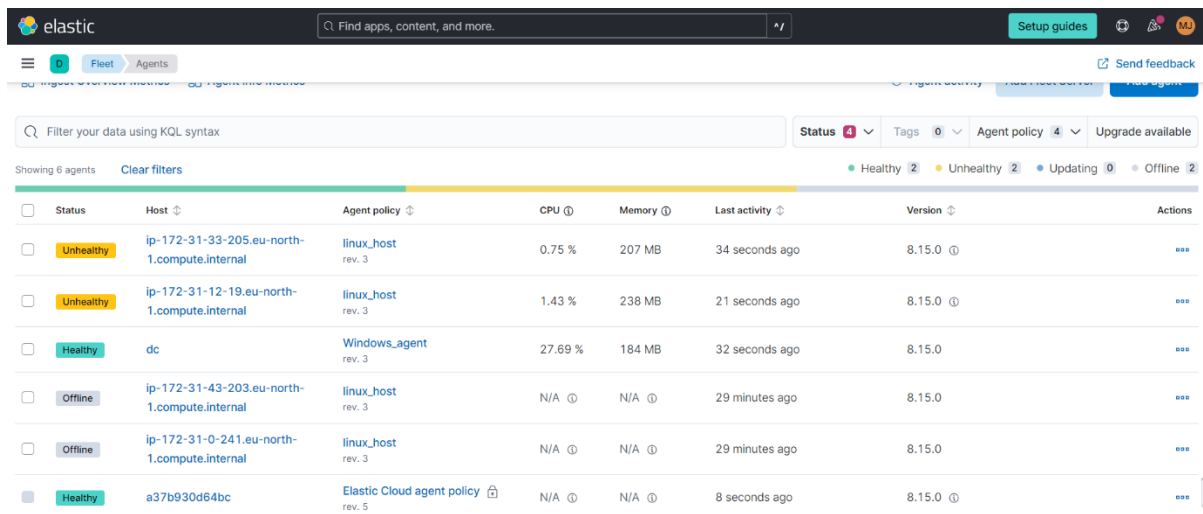
## Process timeline Visualisation



This graphic depicts the Elastic Security SIEM interface, with a focus on the process timeline visualisation. The timeline shows the execution and termination of various VirtualBox processes (VBoxSVC.exe, VirtualBoxVM.exe). The timeline view aids in understanding the order and linkages of various process events, which can be critical for security analysis and incident investigation.



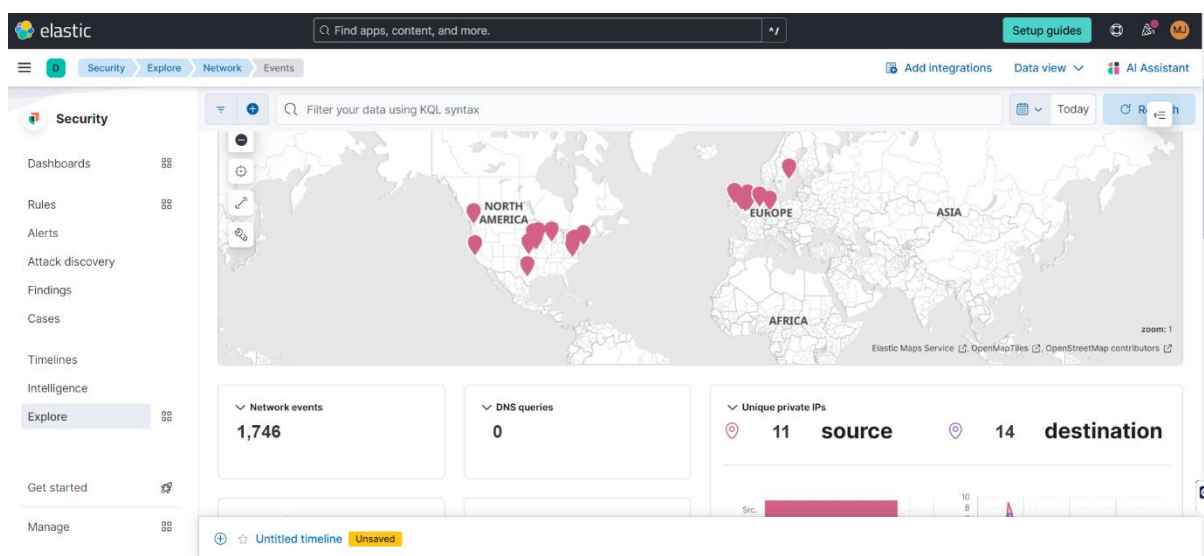
## SEIM Health



Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Unhealthy	ip-172-31-33-205.eu-north-1.compute.internal	linux_host rev. 3	0.75 %	207 MB	34 seconds ago	8.15.0	...
Unhealthy	ip-172-31-12-19.eu-north-1.compute.internal	linux_host rev. 3	1.43 %	238 MB	21 seconds ago	8.15.0	...
Healthy	dc	Windows_agent rev. 3	27.69 %	184 MB	32 seconds ago	8.15.0	...
Offline	ip-172-31-43-203.eu-north-1.compute.internal	linux_host rev. 3	N/A	N/A	29 minutes ago	8.15.0	...
Offline	ip-172-31-0-241.eu-north-1.compute.internal	linux_host rev. 3	N/A	N/A	29 minutes ago	8.15.0	...
Healthy	a37b930d64bc	Elastic Cloud agent policy rev. 5	N/A	N/A	8 seconds ago	8.15.0	...

This image shows the Elastic Fleet Agent management interface, which provides a real-time view of the health and status of deployed agents. It displays the status summary, agent details (such as host, policy, resource use, and version), filtering options, and upgrade availability. This view enables administrators to effectively monitor and manage their Elastic Agent fleet.

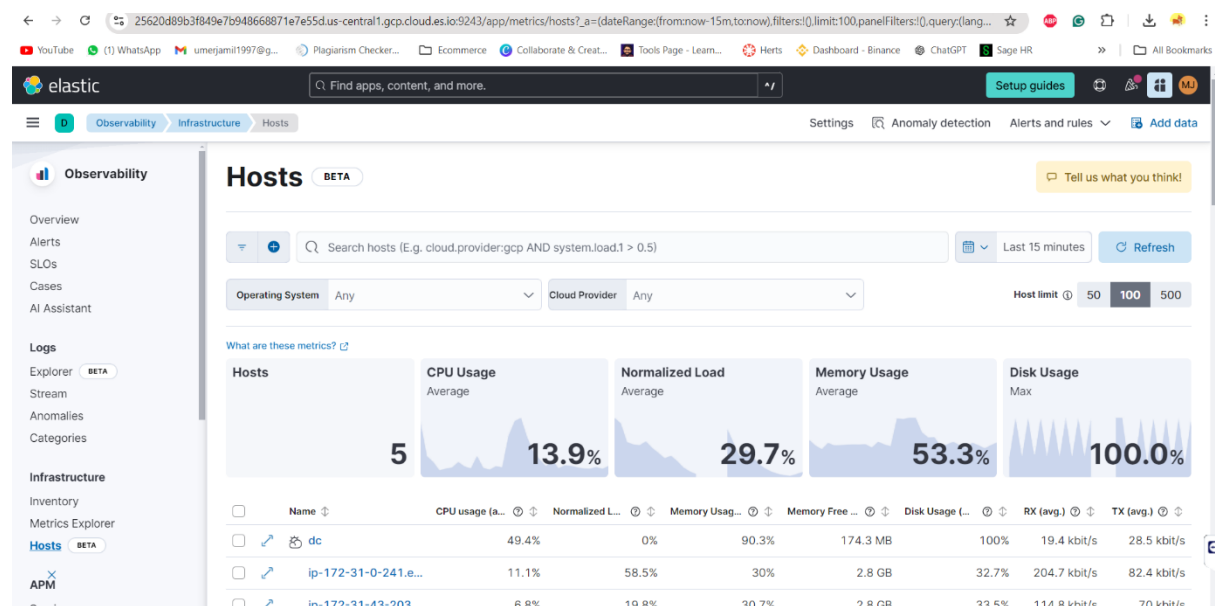
## SEIM Network Overview



This picture depicts the Elastic Security interface, with a focus on network activity monitoring. A globe map depicts the geographical distribution of network events, with clusters found in North America and Europe. Summary panels quantify network events, DNS queries, and unique private IP addresses (source and destination). The existence of a timeline indicates that network traffic patterns can be analysed over time.



## SIEM Host Overview



This picture depicts the Elastic Observability "Hosts" view, which provides a real-time snapshot of critical performance data across monitored hosts. The dashboard displays aggregated CPU consumption, normalised load, memory usage, and disc usage, providing information on overall system health and resource utilisation. A tabular list also includes individual host metrics, such as network throughput (RX/TX). This view allows administrators to proactively discover possible bottlenecks or performance concerns in their infrastructure.

### 4.12.3 Implementation of Two-factor Authentication (2FA)

Because 2FA is among the crucial key controls of SOC 2 compliance, that is required to add an extra layer of authentication, by providing “something you know” along with “something you have”. Okta is offering the best multi-factor authentication (MFA) solution in the market, since it has strong features, it works seamlessly and can integrate with entire organizations and their ecosystems.

It has different levels for the additional authentication evidence, from the basic security questions, One-time passwords (OTPs) text message service. To ensure the high assurance of security and balance with the ease of use, I enforced the Okta Verify Push on mobile application. In addition, employees' smartphones are normally protected by biometrics-based solutions (Apple Face ID, Windows Hello, Fingerprint), I would say that is the most secured MFA solution. I can name a list of HAL core service are now integrated with the OKTA MFA:

- Microsoft Active Directory
- Remote VPN (FortiClient)
- Amazon AWS

- Elastic(SIEM)

#### **4.12.4 Implementation of Disaster Recovery Plan**

I helped HAL to develop emergency procedures, which includes determining HAL's critical assets, tools & technologies should be used, a team who in charge of the event, which level of management need to be informed...as well as Recovery Time Objective (RTO), Recovery Point Objective (RPO) that need to bring operations back online.

For AWS, I found that HAL IT Department has been developing a highly available & scalable architecture, but still have minor errors and insufficient design in case of region outage, I helped them improve these and all seems great to us. HAL still has some services running on the headquarters site, but most of them were an on-going migration to AWS cloud. On Premises & Rackspace, as I recommended using Rackspace as offsite warm backup for the services hosting at headquarters. Both were designed with highly fault-tolerant on both network & systems.

Incremental & Weekly Full System Backups are scheduled to run daily and weekend respectively and are kept for 30 days. While Monthly Full System Backups are kept for a year, 7-10 years, depending on which types of data. There was a periodical test that restores backups and verifies them to make sure all data is being replicated correctly.

HAL's IT Department often has their training and practicing on Disaster Recovery that helps them lower their stress when disaster occurs and clearly understand what to do in case of disaster.

#### **4.12.5 Implementation of Monitoring & Logging Management**

I recommend HAL to extend their scope of monitoring: all components of the network & system must be monitored and tailored for security information and event management (SIEM) tool. All components of network & system must be configured to record logon & administrative activities, including servers, critical services, network devices, firewalls...on both on-premises and cloud.

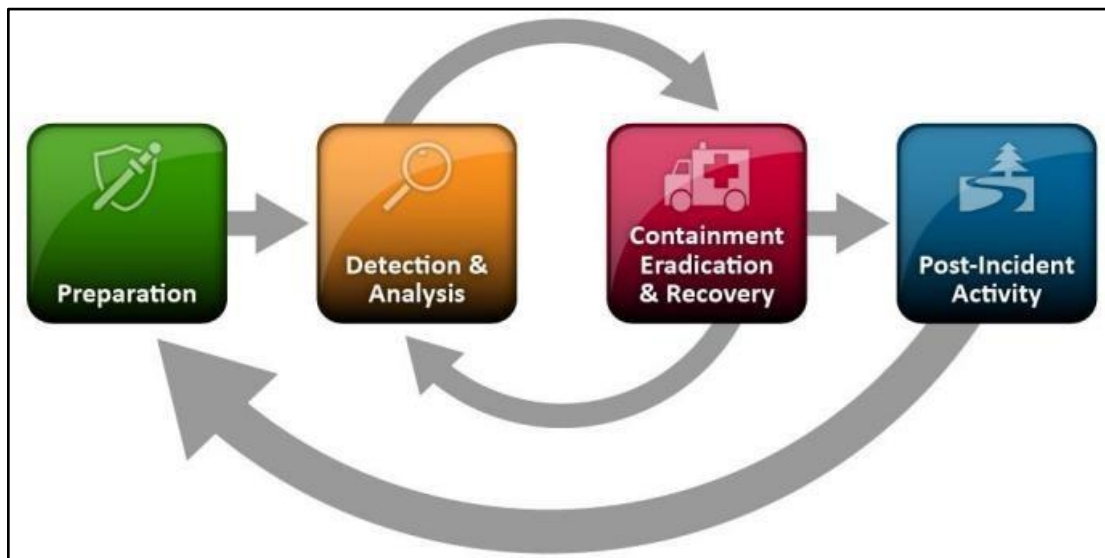
Logs & metrics data should be centralized for better management and retained for at least 30 days. Logs are considered confidential information and tampering is prohibited. I also recommended the use of AWS CloudWatch, Cloud Trails to collect and store the infrastructure metrics & logs on cloud, for the on-premises assets, it can be configured to push the data to cloud.

The IT Department should review logs and perform audits regularly, and it's important to have NTP for time synchronization.

#### **4.13 Incident Responses**

In the case of a cyberattack, HAL must have an incident response plan in place to mitigate the damage and ensure a quick recovery. The incident response plan should include steps for identifying and containing the attack, assessing damage, and restoring

systems and data. HAL should also have a team of professionals ready to respond promptly to an assault and reduce its effects. It is vital that HAL tests and updates its incident response plan on a regular basis to maintain its effectiveness in the face of changing cyber threats. Furthermore, HAL should maintain open channels of communication with all stakeholders, including consumers and regulators.



#### 4.13.1 Incident Responses Preparation

- Develop comprehensive incident response policies and procedures: Create and disseminate clear guidelines for handling various incidents.
- Ensure adequate resources for incident analysis: Verify access to necessary software, hardware, and data.
- Conduct a thorough risk assessment: Identify critical assets and assess their risks to prioritize response activities.
- Establish dedicated incident response teams: Form cross-functional teams with defined roles and responsibilities.
- Conduct training and awareness activities: Educate staff on recognizing and reporting security incidents.
- Develop effective communication plans: Outline communication strategies with stakeholders during an incident.
- Implement robust security controls: Deploy and maintain security measures to prevent or mitigate incidents.
- Conduct regular testing and exercises: Evaluate and improve incident response capabilities through simulations and exercises.

#### 4.13.2 Creation of Initial alert

If any of the following questions are answered as "yes," there should be an obligatory alert.:

1. Do the impacted systems store P3/P4 data locally?
2. Do impacted systems have access to network file shares that store P3/P4 data?

3. Are affected systems being accessed by users using P3/P4 access credentials?
4. Can affected systems programmatically access external P3/P4 data?
5. Do the impacted systems access programs that store/process P3/P4 data?

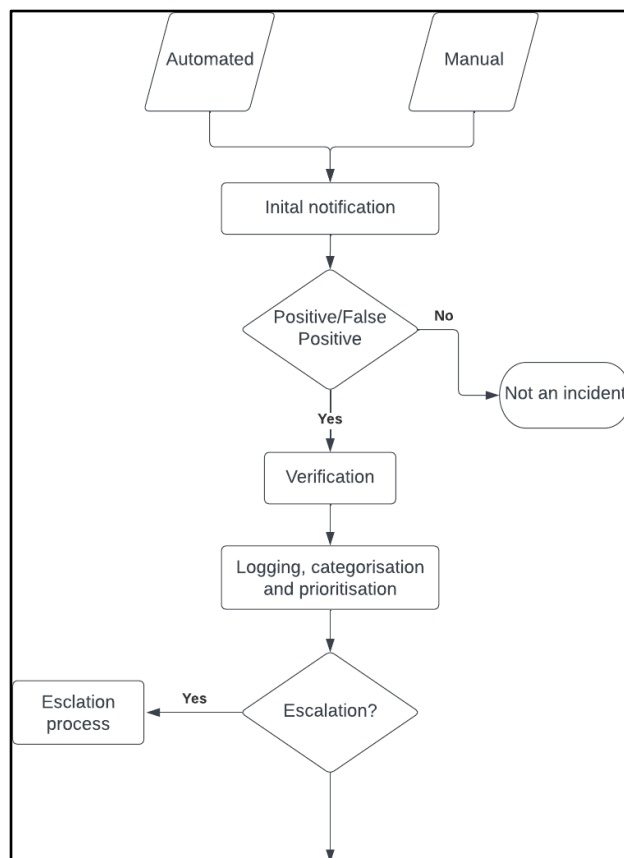
*Policy Example:*

- If a security event involves P3/P4 data, notify the Manager and IR team immediately by emailing [urgent@security.HAL.com](mailto:urgent@security.HAL.com) with the "Intake report" information.

#### 4.13.3 Incident Identification

- Implement comprehensive monitoring systems: Utilize IDPS, SIEM, and other tools to detect anomalies and potential threats.
- Review logs and alerts regularly: Analyse system and network logs to identify unusual activity.
- Conduct vulnerability scans: Perform routine scans to uncover and address potential weaknesses in systems.
- Monitor external sources: Stay informed about potential threats by monitoring security news and advisories.
- Conduct user awareness training: Educate employees on recognizing and reporting potential security incidents.

Once an incident has been identified we will follow the following stages:



1. Initial Alert: The monitoring team will receive an initial alert from an automated or manual source, which can be a user or an alert from SEIM software.
2. Alert Verification: The operator will review the alert to determine whether it is a real or false alert. To reduce alert fatigue, HAL will automate this process as much as possible, so only critical alerts will reach the operator.
3. Incident Triage: If the indicator is positive, the alert will be forwarded to the incident verification team for further investigation. The team consists of well-trained individuals who will conduct a triage to determine the scope and severity of the incident.
4. Logging and Classification: After verification, incidents are registered and classified according on their severity and impact on HAL operations. This information will be utilised to identify the right reaction and deploy the resources accordingly.
5. Based on *Data* involved (P3-P4) i will decide whether to escalate the Alert or not.
6. Incident Response: HAL will start its incident response plan dependent on the severity of the situation. This strategy comprises established measures to contain the incident, lessen its impact, and resume normal operations as soon as possible.

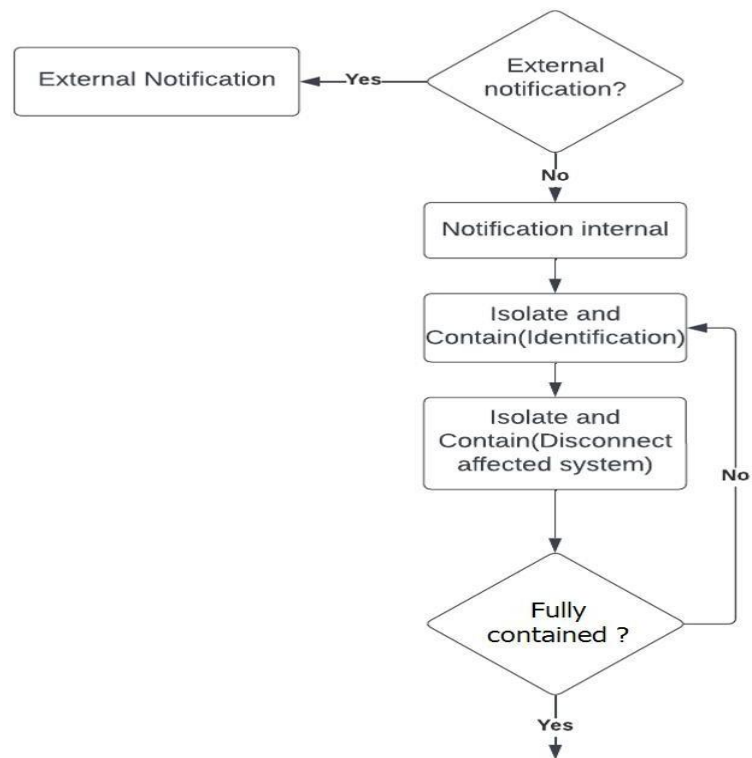
#### **4.13.4 Isolation and Containing**

The Incident Analysis and Containment phase is critical for HAL. During this phase, HAL must quickly determine the scope and impact of any security incidents that occur and take immediate steps to contain them to prevent further damage.

Here are some key activities that HAL typically undertakes during the Incident Analysis and Containment phase:

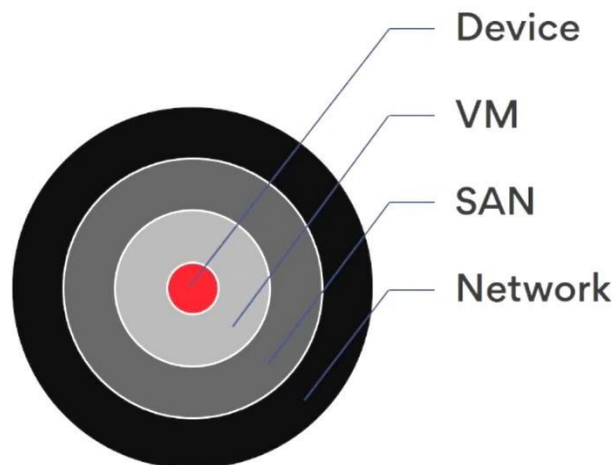
1. Collect evidence: Gather all relevant data including system logs, network traffic, and any other pertinent information.
2. Analyse evidence: Thoroughly examine collected data using forensic and network analysis tools to assess the incident's scope and impact.
3. Contain the incident: Take immediate action to limit the damage and prevent further harm by isolating affected systems or shutting down services.
4. Determine the cause: Investigate the root cause of the incident, identifying vulnerabilities or weaknesses that were exploited.
5. Develop a remediation plan: Create a comprehensive plan to address vulnerabilities and prevent similar incidents in the future.
6. Notify relevant stakeholders: Communicate with customers, regulatory agencies, and other relevant parties as necessary

By taking these steps during the Incident Analysis and Containment phase, HAL can minimize the impact of any security incidents and prevent further damage to its network and services. This phase is critical to the overall success of HAL's incident response plan, as it lays the groundwork for later phases such as recovery and lessons learned. The team must follow the following structure and improve them.



#### 4.13.5 Containing

Containing is one of the most curtail part of Isolation as it will define whether the whole system is compromise or only a particular device. we can further defy the Containment on the bases of



the scope of the attack, which can be at the device level, VM, SAN or Network level

- **Devices:** In the context of isolation a device is physical endpoint such as a desktop computer laptop or mobile device that may be exploited or potentially compromised.
- **Virtual Machines (VMs):** A virtual machine is a software-based representation of a physical computer capable of running an operating system and applications. Isolating VMs may be necessary to prevent the transmission of malware or to safeguard other VMs on the same host.
- **Storage Area Networks (SANs):** A SAN is a specialised, high-speed network that allows block-level access to data storage. Isolating a SAN may be necessary to prevent the spread of malware or to maintain the integrity of the data stored on the SAN.
- **Entire Networks:** An entire network is a collection of interconnected devices and resources that use the same communication protocol and network address. An entire network may need to be isolated in order to prevent the spread of malware or to protect other networks that are connected to it.

It's also worth noting that the effectiveness of the containment strategy will depend on the depth of isolation achieved. The deeper the isolation, the better it is for the organization as it minimizes the risk of the attack spreading further and causing more damage. However, deeper isolation may also have a greater impact on business operations, so it's important to balance the level of isolation with the needs of the organization.

#### 4.13.6 Recovery and Eradication

The Recovery and Eradication phase is the fourth phase of an incident response plan for HAL. The major purpose of this phase is to restore damaged systems to a known good

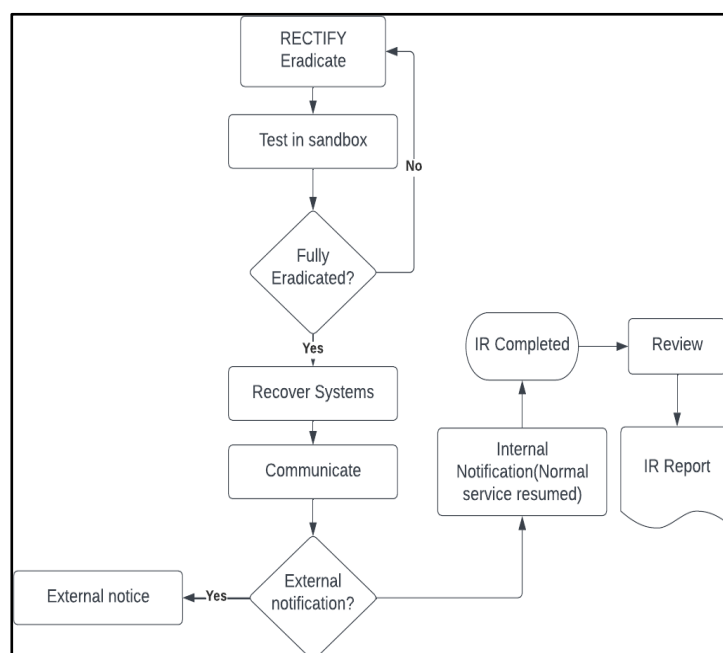
state and delete all evidence of the incident.

Here are some key activities that are typically undertaken during the Recovery and Eradication phase for HAL:

- Restore affected systems: Bring compromised systems back to a known good state by re-imaging or restoring from backups.
- Verify system integrity: Ensure restored systems are free of malware and other signs of compromise using security tools and manual review.
- Eliminate remaining traces: Remove any lingering evidence of the incident, such as backdoors or modified files.
- Verify remediation: Confirm that the remediation plan has been fully implemented and is effective in preventing future incidents.
- Resume normal operations: Once systems are fully restored and verified, gradually resume normal operations and services

Taking these procedures during the Recovery and Eradication phase allows HAL to remove any lingering traces of the incident and return affected systems to a known good condition. This reduces the risk of future disasters and guarantees that business operations continue without obstacles.

It's worth noting that the Recovery and Eradication phase is closely tied to the Incident Analysis and Containment phase, as the effectiveness of the remediation plan developed during the Incident Analysis and Containment phase will be evaluated during the Recovery and Eradication phase. This highlights the importance of thorough analysis and planning during the earlier stages of incident response for HAL's web hosting and internet access services.





This will be the final stage of the whole Incident Response strategy it means that the team is able to bring back the control and everything is recovered, now that we have overcome the incident, we have to focus on the post incident activities which are as follows.

#### **4.13.7 Post incident**

- Review service level agreements (SLAs): Evaluate and update SLAs as needed, incorporating lessons learned from the incident.
- Conduct a root cause analysis: Perform a thorough investigation to identify the underlying cause and contributing factors.
- Update incident response playbooks: Incorporate insights from the incident to improve and refine response procedures.
- Provide additional training for staff: Enhance staff knowledge and skills related to incident response.
- Conduct tabletop exercises: Test and validate updated playbooks and staff preparedness through simulated exercises.
- Continuous improvement: Maintain an ongoing commitment to enhancing incident response capabilities through lessons learned and feedback.

#### **4.14 What are the results of the audit you have done as blue team on your project?**

I have conducted a comprehensive blue team audit of HAL's security controls to identify potential vulnerabilities and assess the company's security posture. During the audit, I discovered several areas where HAL can improve its security posture and prevent potential security incidents. Our recommendations for remediation are outlined below.

Key Findings: During the blue team audit, our team identified the following key findings:

1. **Outdated software and systems:** HAL is using several outdated software and systems that are no longer supported by the vendor. These systems are vulnerable to cyberattacks, and HAL should consider upgrading or replacing them.
2. **Weak access controls:** The team identified several instances where access controls were not implemented or were implemented poorly. This can lead to unauthorized access to sensitive data and systems.
3. **Insufficient logging and monitoring:** HAL does not have a centralized logging and monitoring system, making it difficult to detect potential security incidents in a timely manner.
4. **Missing patches:** HAL has several systems that are missing critical security patches. These systems are vulnerable to known exploits and can be easily compromised by attackers.

Recommendations: To address these key findings and improve its security posture, we recommend HAL take the following remediation actions:

1. Upgrade or replace outdated software and systems to ensure they are fully

supported and free from known vulnerabilities.

2. Implement strong access controls, including the principle of least privilege, to ensure that only authorized personnel can access sensitive data and systems.
3. Implement a centralized logging and monitoring system to detect and respond to potential security incidents in a timely manner.
4. Prioritize and apply critical security patches to systems in a timely manner to reduce the risk of exploitation by attackers, also implement a patch management system

Overall, we recommend HAL implement these remediation actions to improve its security posture and reduce the risk of potential security incidents. We also recommend conducting regular security assessments to identify and address any potential vulnerabilities before they can be exploited by attackers.

#### 4.15 Detailed Findings

The version of Apache web server running on HAL's servers I found to be 2.4.29, which was released on November 29, 2017. The current version of Apache web server is [2.4.57](#), which was released on April 6, 2023. The outdated version of Apache web server is vulnerable to known security vulnerabilities, which could allow attackers to gain unauthorized access to HAL's systems, steal sensitive data, or disrupt its services.

```
root@3d69c5fc86bb:/usr/local/apache2/conf# ls
extra httpd.conf magic mime.types original
root@3d69c5fc86bb:/usr/local/apache2/conf# apachectl -v
Server version: Apache/2.4.29 (Unix)
Server built:   Mar 14 2018 05:15:10
root@3d69c5fc86bb:/usr/local/apache2/conf# |
```

I also found MySQL 5.7.5: HAL is still using MySQL 5.7.5 which was released in 2016 and is no longer supported. There have been several security vulnerabilities identified in this version of MySQL, and HAL should upgrade to a newer version to address these vulnerabilities.

```
root@274eda56c0a3:~# mysql -v
mysql Ver 5.7.5ubuntu0.20.04.3 for Linux on x86_64 ((Ubuntu))
root@274eda56c0a3:~#
```

- Cisco ASA 5505 firewall: This firewall has reached its end of life and is no

longer supported by Cisco. This means that any vulnerabilities found in this firewall will remain unpatched, leaving HAL's network open to attacks. Our audit has revealed that HAL has weak access controls in place that could potentially allow unauthorized users to access sensitive data or systems. Specifically, I found the following issues:

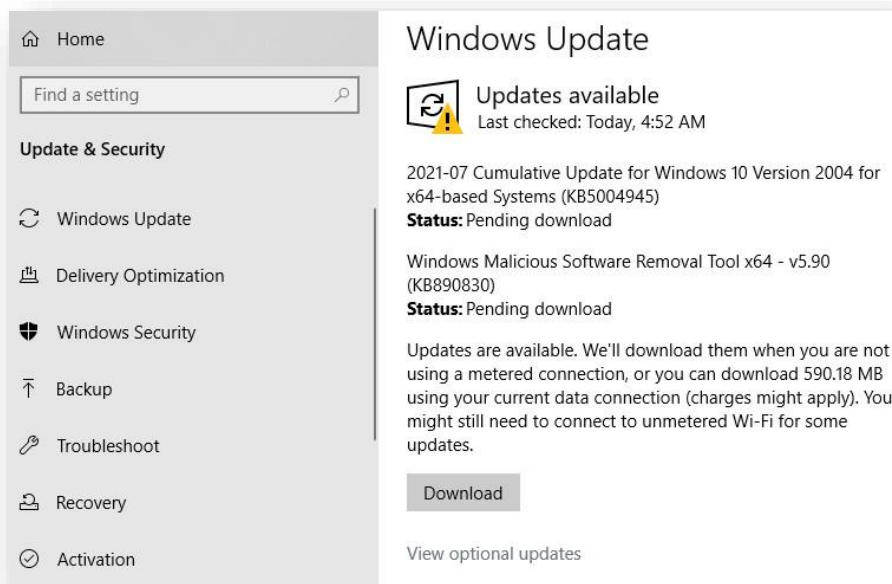
- Shared administrator accounts: There are several shared administrator accounts that are being used by multiple employees. This creates a risk of unauthorized access to sensitive systems and data, as it is difficult to track who has accessed what information.
- Many user accounts have weak passwords that are easily guessable, such as "password" or "123456". This makes it easy for attackers to gain access to HAL's systems and data.
- Inactive accounts: There are many inactive user accounts that have not been disabled or deleted. These accounts could be used by attackers to gain access to HAL's systems and data.

janedoe	pts/1	192.168.1.3	Fri Jan 13 10:57:35 2017
stevejohnson	pts/2	192.168.1.4	Wed Apr 26 09:15:21 2017
michaelgreen	pts/3	192.168.1.6	Sat Feb 18 11:57:42 2017
sarahjones	pts/4	192.168.1.7	Sun Mar 5 07:24:51 2017
peterlee	pts/5	192.168.1.8	Tue Apr 11 13:45:29 2017

- HAL's current logging system only captures a limited set of events, such as login attempts and system errors. This means that important security events, such as failed authentication attempts or changes to system settings, are not being logged.
- The monitoring system in place is not set up to alert the security team in real-time. Instead, security incidents are only discovered during routine reviews of the logs, which can take days or even weeks to complete. as we can see John Doe is logged in but there is no record saved for this event.

lp			**Never logged in**
mail			**Never logged in**
news			**Never logged in**
johndoe	pts/0	192.168.1.2	Tue Mar 7 18:09:23 2023

Another significant vulnerability identified during the audit is the presence of multiple outdated Windows systems running without any patches applied. This poses a serious security threat to the company's infrastructure as it makes it more susceptible to cyber-attacks such as malware infections, data breaches, and other forms of unauthorized access. It is imperative that HAL takes immediate action to address this issue by installing the necessary security updates and patches to the affected systems.



Considering these vulnerabilities, it is crucial that HAL takes immediate action to update and patch these systems to ensure the security of the company's infrastructure. It is recommended that the company implement a regular patching schedule to ensure that all systems receive the necessary security updates and patches in a timely manner. Additionally, HAL should consider upgrading these outdated systems to newer versions that are still supported and receive regular security updates. This will not only address the current vulnerabilities but also help prevent future security risks associated with outdated systems.

### Discussion and Evaluation

This thesis embarked on a journey to address the critical challenges faced by Small and Medium-sized Enterprises in achieving and maintaining SOC 2 compliance with a specific focus on enhancing the network infrastructure and security posture of Hierarchical Access Limited (HAL). This chapter provides a comprehensive discussion and evaluation of the research findings, reflecting on the achievements, challenges, and implications of the project.

#### 5.1 Summary of Findings

The project successfully delivered its core objectives, resulting in a strong and secure network infrastructure for HAL that meets the stringent SOC 2 standards. Key achievements include:

- **Implementation of SOC 2 Compliance:** HAL now has a SOC 2 compliant environment, promoting trust and confidence among its clients, particularly those in the big tech sector. This achievement opens doors to new business opportunities and strengthens HAL's market position.
- **Enhanced Network Security:** Through the deployment of AWS, IDS/IPS systems, and SIEM tools, HAL's network infrastructure has been secured against a wide array of cyber threats. The reduction in vulnerabilities and improved incident response capabilities demonstrate an immediate improvement in HAL's security posture.
- **Improved System Performance and Reliability:** The implementation of load balancing and cluster management has resulted in a more security and performance system. This translates to improved service availability and superior user experience for HAL's clients.
- **Establishment of a Secure Authentication and Authorization Framework:** A strong network infrastructure for authentication, authorization, and accounting of network assets now ensures controlled access and transparency, further strengthen HAL's security posture.

These accomplishments have been met with positive results highlighting the tangible benefits of the project.

#### 5.2 Evaluation of Achievements

The research questions posed at the beginning of this thesis have been comprehensively addressed. The project successfully demonstrated how a SOC 2 compliant network infrastructure can be designed and implemented for an organization like HAL, even with its specific constraints and requirements. The security posture of HAL has been significantly enhanced, mitigating risks associated with network vulnerabilities, resource strain, and compliance requirements.

The project's success is further underscored by the measurable improvements in system performance, reduction in security incidents, and positive results. These outcomes validate the effectiveness of the implemented solutions and their alignment with HAL's business objectives.

### **5.3 Reflection on Methodology**

The research methodology adopted for this project, encompassing a combination of literature review, case study analysis, and hands-on implementation, proved instrumental in achieving the desired outcomes. The literature review provided a solid theoretical foundation, while the case study approach allowed for a deep dive into HAL's specific context and challenges. The hands-on implementation ensured the practical applicability and effectiveness of the proposed solutions.

### **5.4 Challenges and Limitations**

The project was not without its challenges. Resource constraints, the complexities of integrating disparate security tools, and the ever-evolving threat landscape created significant hurdles. However, through careful planning, adaptability, and a commitment to continuous improvement, these challenges were successfully navigated.

While the project achieved its core objectives, certain limitations warrant acknowledgment. The scope of the project was confined to HAL's specific context, and further research is needed to explore the generalizability of the findings to other SMEs. Additionally, the long-term sustainability and adaptability of the implemented solutions in the face of emerging threats will require ongoing monitoring and evaluation.

### **5.5 Commercial and Economic Context**

The successful implementation of SOC 2 compliance and the enhanced security posture have a major impact on HAL's business prospects. The ability to demonstrate compliance with industry-recognized standards positions HAL as a trusted and reliable partner, particularly for clients in the big tech sector. This can lead to increased business opportunities, revenue growth, and a competitive advantage in the marketplace.

Beyond HAL, this project serves as a blueprint for other SMEs grappling with the complexities of SOC 2 compliance and network security. The insights and lessons learned can empower other organizations to embark on similar journeys, fostering a more secure and resilient business environment.

### **5.6 Project Management Reflection**

The project's initial plan underwent several adaptations in response to unforeseen challenges and evolving requirements. Resource constraints necessitated careful prioritization and a phased implementation approach. The complexities of integrating security tools required additional time and effort. However, through effective communication with experienced people, collaboration, and a focus on key deliverables, the project was successfully navigated to completion.

The experience underscores the importance of adaptability and proactive risk management in project execution. It also highlights the value of continuous learning and improvement in navigating the dynamic landscape of cybersecurity.

## 5.7 Future Work

While this project has significantly enhanced HAL's security posture and achieved SOC 2 compliance, the pursuit of cybersecurity is an ongoing journey. Several avenues for future work emerge from this research:

- **Continuous Monitoring and Improvement:** The threat landscape is constantly evolving, necessitating continuous monitoring and adaptation of security measures. Future work could involve implementing advanced threat detection and response capabilities, leveraging AI and machine learning to proactively identify and mitigate risks.
- **Expansion of Scope:** The current project focused on core network infrastructure and SOC 2 compliance. Future initiatives could explore extending security measures to other areas, such as endpoint security, cloud security, and data loss prevention.
- **User Awareness and Training:** While technological solutions are crucial, human factors remain a significant vulnerability. Future efforts could focus on enhancing user awareness and training programs to cultivate a security conscious culture within HAL.
- **Exploration of Emerging Technologies:** The fast pace of technological advancement presents both opportunities and challenges. Future research could investigate the potential of emerging technologies, such as blockchain and zero-trust architectures, in further bolstering HAL's security posture.

## 5.8 Conclusion

This project has successfully addressed the research questions and objectives, delivering a SOC 2 compliant and secure network infrastructure for HAL. The tangible improvements in security posture, system performance, and risk mitigation capabilities stand as a testament to the project's success.

While acknowledging the challenges and limitations encountered, the project outcomes offer valuable insights for both HAL and the broader SME community. The journey towards SOC 2 compliance and enhanced security is an ongoing one, but this project has laid a solid foundation for HAL's future growth and resilience in an increasingly interconnected and threat-prone digital landscape. The avenues for future work identified in this chapter present exciting opportunities to further strengthen HAL's security posture and maintain its competitive edge in the years to come.

## ➤ **References**

1. Alghamdi, F., Hamza, N., Tamimi, M., 2019. Factors that Influence the Adoption of Information Security on Requirement Phase for Custom-Made Software at SMEs, in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). Presented at the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), IEEE, Riyadh, Saudi Arabia, pp. 1–6. <https://doi.org/10.1109/CAIS.2019.8769519>
2. Arenda, L., Popov, O., 2019. A Conceptual Model of an Intelligent Platform for Security Risk Assessment in SMEs, in 2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT). Presented at the 2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT), IEEE, Baku, Azerbaijan, pp. 1–8. <https://doi.org/10.1109/AICT47866.2019.8981796>
3. Bundela, R., Dhanda, N., Verma, R., 2022. Load Balanced Web Server on AWS Cloud, in 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). Presented at the 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE, Greater Noida, India, pp. 114–118. <https://doi.org/10.1109/ICCCIS56430.2022.10037657>
4. Carias, J.F., Borges, M.R.S., Labaka, L., Arrizabalaga, S., Hernantes, J., 2020. Systematic Approach to Cyber Resilience Operationalization in SMEs. IEEE Access 8, 174200–174221. <https://doi.org/10.1109/ACCESS.2020.3026063>
5. Fleron, C.N., Jørgensen, J.K., Kulyk, O., Paja, E., 2023. Towards a Basic Security Framework for SMEs – Results from an Investigation of Cybersecurity Challenges in Denmark, in: 2023 IEEE 31st International Requirements Engineering Conference Workshops (REW). Presented at the 2023 IEEE 31st International Requirements Engineering Conference Workshops (REW), IEEE, Hannover, Germany, pp. 230–233. <https://doi.org/10.1109/REW57809.2023.00046>
6. Ganesh, A., Ramakrishnan, R., Sekar, A.K., Logeshwaran, J., 2023. A Load Balancing Architecture to Improve the Security of Cloud Computing in the Disease Management Centers, in 2023 Second International Conference on Smart Technologies For Smart Nation (SmartTechCon). Presented at the 2023 Second International Conference on Smart Technologies For Smart Nation (SmartTechCon), IEEE, Singapore, Singapore, pp. 1299–1305. <https://doi.org/10.1109/SmartTechCon57526.2023.10391528>
7. Henriques, J., Caldeira, F., Cruz, T., Simões, P., 2024. A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection. IEEE Access 12, 2409–2444. <https://doi.org/10.1109/ACCESS.2023.3348552>
8. Iyamuremye, B., Shima, H., 2018. Network security testing tools for SMEs (small and medium enterprises), in 2018 IEEE International Conference on Applied System Invention (ICASI). Presented at the 2018 IEEE International Conference on Applied System Innovation (ICASI), IEEE, Chiba, pp. 414–417. <https://doi.org/10.1109/ICASI.2018.8394272>
9. Johansen, G., 2023. Digital forensics and incident response: incident response tools and techniques for effective cyber threat response, Third edition. ed. Packet Publishing, Birmingham.
10. Kandpal, S., Bhatt, S., Mohan, L., Patwal, A., Kumar, P., 2023. Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis, in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Presented at the



- 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, Delhi, India, pp. 1–5. <https://doi.org/10.1109/ICCCNT56998.2023.10307363>
11. Kanpariyasontorn, J., Senivongse, T., 2017. Cloud service trustworthiness assessment based on cloud controls matrix, in 2017 19th International Conference on Advanced Communication Technology (ICACT). Presented at the 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE, Pyeongchang, Kwangwoon Do, South Korea, pp. 291–297. <https://doi.org/10.23919/ICACT.2017.7890100>
  12. Khande, R., Rajapurkar, S., Barde, P., Balsara, H., Datkhile, A., 2023. Data Security in AWS S3 Cloud Storage, in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Presented at the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, Delhi, India, pp. 1–6. <https://doi.org/10.1109/ICCCNT56998.2023.10306922>
  13. Kumar, S., Singh, B.P., Kumar, V., 2021. A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security, in 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). Presented at the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), IEEE, Greater Noida, India, pp. 1963–1967. <https://doi.org/10.1109/ICAC3N53548.2021.9725596>
  14. Mmango, N., Gundu, T., 2023. Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs, in 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). Presented at the 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), IEEE, Cape Town, South Africa, pp. 1–6. <https://doi.org/10.1109/ICECET58911.2023.10389226>
  15. Monev, V., 2020. Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002, in: 2020 International Conference on Information Technologies (InfoTech). Presented at the 2020 International Conference on Information Technologies (InfoTech), IEEE, Varna, Bulgaria, pp. 1–5. <https://doi.org/10.1109/InfoTech49733.2020.9211066>
  16. Muhammad Jamshid Khan, 2023. Securing network infrastructure with cyber security. World J. Adv. Res. Rev. 17, 803–813. <https://doi.org/10.30574/wjarr.2023.17.2.0308>
  17. Nadaf, S.M., Revoori, V., Rath, H.K., Simha, A., 2014. An Enterprise Data Center Network Design - Netdes, in 2014 Fourth International Conference on Communication Systems and Network Technologies. Presented at the 2014 International Conference on Communication Systems and Network Technologies (CSNT), IEEE, Bhopal, India, pp. 540–545. <https://doi.org/10.1109/CSNT.2014.114>
  18. Park, W., Ahn, G., 2021. A Study on the Next Generation Security Control Model for Cyber Threat Detection on the Internet of Things (IoT) Environment, in: 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter). Presented at the 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), IEEE, Ho Chi Minh City, Vietnam, pp. 213–217. <https://doi.org/10.1109/SNPDWinter52325.2021.00053>
  19. Roy, P.P., 2020. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard, in: 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTE). Presented at the 2020 National Conference on Emerging Trends on Sustainable Technology

- and Engineering Applications (NCETSTEA), IEEE, Durgapur, India, pp. 1–3. <https://doi.org/10.1109/NCETSTEA48365.2020.9119914>
20. Ryan, I., Roedig, U., Stol, K.-J., 2022. Insecure Software on a Fragmenting Internet, in 2022 Cyber Research Conference - Ireland (Cyber-RCI). Presented at the 2022 Cyber Research Conference - Ireland (Cyber-RCI), IEEE, Galway, Ireland, pp. 1–9. <https://doi.org/10.1109/Cyber-RCI55324.2022.10032675>
  21. Sun, Z., 2022. Hierarchical and Complex Parallel Network Security Threat Situation Quantitative Assessment Method, in 2022 6th International Conference on Computing Methodologies and Communication (ICCMC). Presented at the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), IEEE, Erode, India, pp. 276–279. <https://doi.org/10.1109/ICCMC53470.2022.9753819>
  22. Wang, W., Sadjadi, S.M., Rishe, N., 2024. A Survey of Major Cybersecurity Compliance Frameworks, in 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity). Presented at the 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity), IEEE, NYC, NY, USA, pp. 23–34. <https://doi.org/10.1109/BigDataSecurity62737.2024.00013>
  23. Yang, H., Hoang, C.-P., Kim, Y., 2018. Architecture for Virtual Network Function's High Availability in Hybrid Cloud Infrastructure, in 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). Presented at the 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE, Verona, Italy, pp. 1–5. <https://doi.org/10.1109/NFV-SDN.2018.8725784>

