Design and Implementation of a Secure and Compliant IT Infrastructure for a Healthcare SME under GDPR and NIS2

Uthman Oluwadamilare Ismail

January 9, 2026

Contents

Chapter 1

Introduction

The digitalisation of healthcare services has expanded the use of Electronic Health Record (EHR) systems, improving efficiency and continuity of care. At the same time, the sensitive nature of health data makes healthcare organisations attractive targets for cybercriminals, with ransomware and data breaches posing risks to patient safety and organisational resilience [1], [2].

Within the European Union, healthcare organisations operate under strict regulatory obligations imposed by the General Data Protection Regulation (GDPR) and the Network and Information Security Directive 2 (NIS2). GDPR establishes a comprehensive framework for the protection of personal data, with specific emphasis on special categories of data, including health-related information. Article 32 of GDPR requires data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including confidentiality, integrity, availability, and resilience of processing systems [3]. Additional principles such as data protection by design and by default (Article 25) further reinforce the need for integrated security controls throughout system lifecycles [3].

Complementing GDPR, NIS2 significantly strengthens cybersecurity requirements for entities operating in critical and important sectors, explicitly including healthcare providers. NIS2 mandates the adoption of risk management measures, security monitoring, incident handling capabilities, and formal incident reporting processes to national authorities [4].

Unlike its predecessor, NIS2 introduces stricter supervisory measures and enforcement mechanisms, making cybersecurity governance a strategic obligation rather than a voluntary best practice.

In this regulatory and threat landscape, effective cybersecurity governance must be supported by concrete and verifiable technical controls, such as network segmentation, intrusion detection systems, centralized logging and monitoring, vulnerability management, and structured incident response procedures. SMEs, however, often face financial, technical, and human resource constraints that limit their ability to deploy enterprise-grade security solutions [5]. This project addresses this challenge by designing and implementing a realistic, resource-efficient, and standards-aligned cybersecurity infrastructure tailored to the needs of a healthcare SME.

As shown in Figure 1.1, the typical cyber threat landscape targeting healthcare organisations.

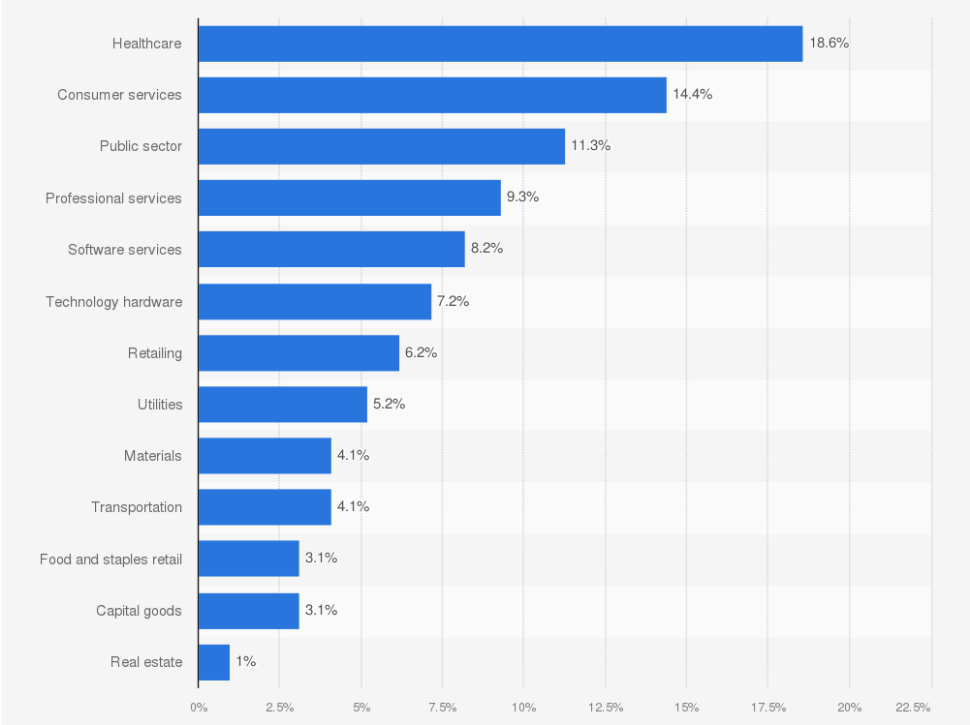

Figure 1.1: Typical cyber threat landscape targeting healthcare organisations

1.1 Project Objectives

The primary objective of this project is to design, deploy, and evaluate a secure IT infrastructure for a simulated healthcare SME, named *MediServ HealthTech Lda*, ensuring alignment with GDPR and NIS2 cybersecurity and data protection requirements. The project aims to bridge regulatory compliance and practical implementation by integrating governance, risk management, and technical security controls in a coherent and auditable manner.

The specific objectives of the project are:

- To design a segmented and monitored network architecture suitable for a healthcare environment.
- To implement centralized security monitoring through a Security Information and Event Management (SIEM) platform.
- To deploy an Intrusion Detection System (IDS) capable of identifying malicious or anomalous network activity.
- To establish a structured asset inventory and vulnerability management process.
- To conduct internal and external security audits within a clearly defined ethical and legal scope.
- To simulate and manage a cybersecurity incident using an incident response and digital forensics platform.
- To perform a structured risk analysis in accordance with ISO/IEC 27005.
- To demonstrate compliance with key GDPR and NIS2 security requirements through documented technical and procedural controls.

Table 1.1: Mapping of project objectives to GDPR and NIS2 requirements

Project Objective	**Regulatory Requirement**
Segmented network architecture	GDPR Art. 32, NIS2 Risk Management
SIEM monitoring	GDPR Art. 32, NIS2 Security Monitoring
IDS deployment	GDPR Art. 32, NIS2 Incident Detection
Vulnerability management	GDPR Art. 25, NIS2 Risk Treatment
Incident response simulation	GDPR Art. 32, NIS2 Incident Handling

1.2 Scope and Methodology

The scope of this project is limited to the design and implementation of a virtualised laboratory environment representing the core IT infrastructure of a healthcare SME. The environment consists of nine virtual machines, including an EHR application server, a database server, centralized security management platforms, administrative workstations, and a deliberately vulnerable legacy workstation system used for controlled testing and demonstration purposes.

The project adopts a structured methodology grounded in internationally recognised standards and cybersecurity frameworks. Risk management activities are conducted in accordance with ISO/IEC 27005 [6], which provides a systematic approach to asset identification, threat and vulnerability analysis, risk evaluation, and risk treatment selection. Information security management principles are aligned with ISO/IEC 27001 [7], particularly regarding continuous monitoring, access control, and incident management. Additionally, operational security practices are informed by the NIST Cybersecurity Framework [8], with emphasis on the Identify, Detect, Respond, and Recover functions.

To support secure and centralized management of the distributed laboratory environment, a Virtual Private Network (VPN) overlay using Tailscale is employed. This enables encrypted connectivity between virtual machines hosted across different physical systems while maintaining centralized visibility and control. This design reflects real-world hybrid

and geographically distributed infrastructures commonly used by SMEs.

The methodology combines theoretical analysis with hands-on implementation. Project outcomes are supported by verifiable evidence, including configuration screenshots, system logs, vulnerability scan reports, security alerts, and incident response documentation. This evidence-based approach ensures that the implemented controls are auditable and demonstrably aligned with regulatory and standards-based requirements.

As shown in Figure 1.2, the laboratory architecture illustrates the segmentation of network components and the isolation of critical assets.

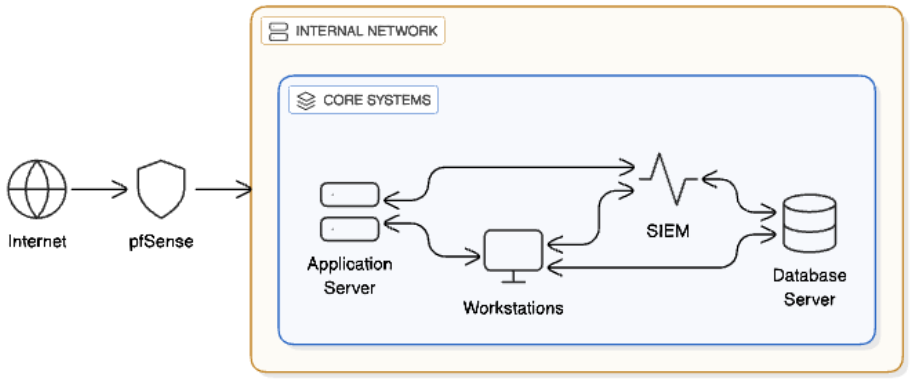

Figure 1.2: Laboratory architecture and network segmentation diagram

1.3 Document Structure

This report is structured as follows:

- Chapter 2 presents the state of the art, covering relevant regulatory frameworks and cybersecurity practices for SMEs.
- Chapter 3 describes the organisational scenario and the designed infrastructure architecture.
- Chapter 4 details the risk analysis conducted in accordance with ISO/IEC 27005.
- Chapter 5 addresses asset inventory and vulnerability management processes.

- Chapter 6 presents the auditing and security testing activities.
- Chapter 7 focuses on incident response and digital forensic analysis.
- Chapter 8 evaluates compliance with GDPR and NIS2 requirements.
- Chapter 9 concludes the report and outlines recommendations for future improvements.

Chapter 2

State of the Art

This chapter presents the state of the art in cybersecurity for healthcare small and medium-sized enterprises (SMEs), focusing on the threat landscape, regulatory obligations, and widely adopted security practices. It reviews the cybersecurity challenges specific to healthcare environments, examines relevant European regulatory and standards-based frameworks, and discusses key technical domains such as security monitoring, intrusion detection, vulnerability management, and incident response. The objective of this chapter is to establish the theoretical and regulatory foundation that informs the design and implementation decisions described in subsequent chapters.

2.1 Cybersecurity Challenges in Healthcare SMEs

Healthcare organisations are consistently identified as one of the most targeted sectors in cyberspace due to the sensitivity, richness, and long-term value of medical and personal data. Electronic Health Records (EHRs) typically contain personally identifiable information, medical histories, and financial data, making them particularly attractive targets for cybercriminals [1]. For healthcare SMEs, these risks are further amplified by limited financial, technical, and human resources, which often restrict the adoption of advanced security solutions and dedicated security teams.

Common cybersecurity threats affecting healthcare SMEs include ransomware attacks,

credential theft, unauthorised access to medical systems, and data breaches caused by misconfigurations or unpatched vulnerabilities. Industry reports and academic studies consistently identify inadequate security monitoring, weak authentication mechanisms, and insufficient incident response preparedness as primary contributors to successful attacks in healthcare environments [2], [9].

In addition to confidentiality concerns, healthcare systems are subject to stringent availability requirements. Disruptions to clinical systems may directly impact patient safety and service continuity. This constraint limits the ability to frequently interrupt systems for maintenance, testing, or upgrades, requiring security controls that are both robust and minimally disruptive. Consequently, healthcare SMEs must adopt cybersecurity solutions that balance security effectiveness, operational continuity, and regulatory compliance.

As shown in Figure 2.1, healthcare organisations face a wide range of cyber threats.

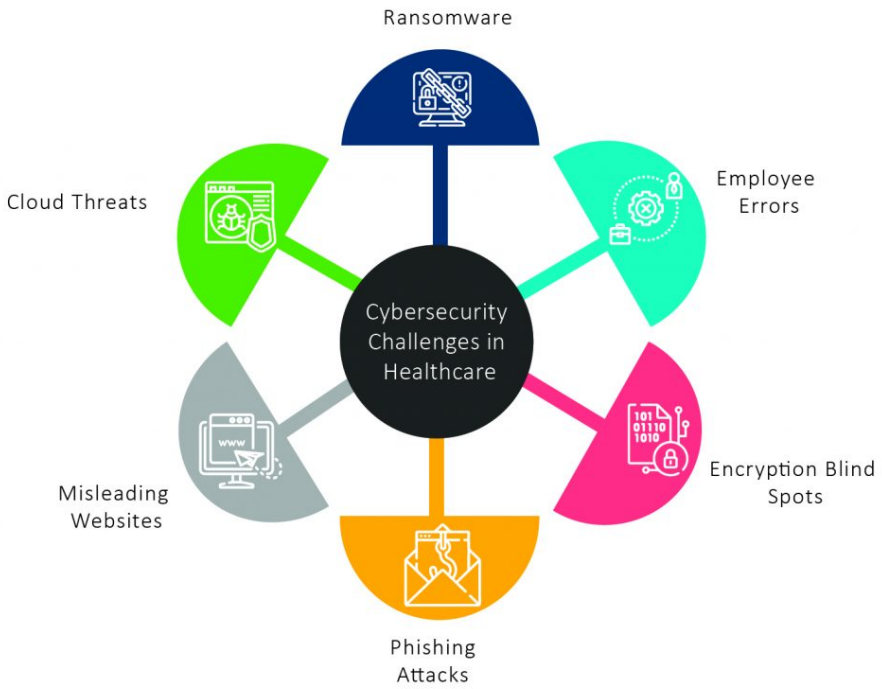

Figure 2.1: Common cyber threats targeting healthcare organisations

2.2 Regulatory and Standards Framework

2.2.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) establishes a comprehensive legal framework for the protection of personal data within the European Union. Health data is classified as a special category of personal data under Article 9, requiring enhanced protection measures due to its sensitivity and potential impact on data subjects' rights and freedoms [3].

Article 32 of GDPR mandates the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These measures explicitly include the ability to ensure the confidentiality, integrity, availability, and resilience of processing systems, as well as the capability to restore availability and access to personal data in a timely manner following an incident [3]. GDPR adopts a technology-neutral and risk-based approach, allowing organisations to select controls appropriate to their context, provided that risks are adequately mitigated.

Furthermore, the accountability principle (Article 5(2)) requires organisations to demonstrate compliance, making documentation, logging, auditing, and continuous monitoring essential components of a compliant cybersecurity strategy. As a result, technical controls such as access control, logging, intrusion detection, and incident detection play a central role in GDPR compliance.

2.2.2 NIS2 Directive

The NIS2 Directive significantly strengthens cybersecurity obligations across the European Union by expanding its scope and introducing stricter supervisory and enforcement mechanisms. Healthcare providers are explicitly classified as essential entities, reflecting the critical nature of healthcare services and their societal impact [4].

Article 21 of NIS2 requires essential and important entities to implement appropriate

technical, operational, and organisational measures. These measures include risk analysis, incident handling, business continuity and crisis management, supply chain security, vulnerability management, and the use of security monitoring and detection mechanisms [4]. In contrast to the original NIS Directive, NIS2 places greater emphasis on proactive and continuous risk management rather than reactive compliance.

NIS2 also introduces stricter incident reporting requirements, including early warning notifications and detailed incident reports within defined timeframes. This reinforces the need for centralised logging, real-time monitoring, and structured incident response capabilities. Overall, NIS2 elevates cybersecurity from a technical concern to a governance-level responsibility with direct management accountability.

2.2.3 ISO/IEC 27001 and ISO/IEC 27005

ISO/IEC 27001 defines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a comprehensive set of security controls across domains such as access control, operations security, communications security, logging and monitoring, and incident management [7].

ISO/IEC 27005 complements ISO/IEC 27001 by focusing specifically on information security risk management. It provides a structured methodology for identifying assets, threats, and vulnerabilities, assessing risk likelihood and impact, and selecting appropriate risk treatment options [6]. The continuous risk management lifecycle promoted by ISO/IEC 27005 aligns closely with GDPR's risk-based approach and NIS2's emphasis on ongoing risk assessment and resilience.

Together, these standards provide a practical and internationally recognised framework for translating regulatory requirements into measurable and auditable security controls.

Table 2.1: Mapping between GDPR, NIS2, and ISO/IEC 27001 controls

GDPR	**NIS2**	**ISO/IEC 27001**
Article 32	Article 21	Annex A Controls

2.3 Security Monitoring and Intrusion Detection

Security Information and Event Management (SIEM) systems are a cornerstone of modern cybersecurity operations. SIEM platforms aggregate logs from diverse sources, correlate events, and generate alerts that support both operational security and regulatory compliance. In healthcare environments, SIEM systems provide visibility into authentication events, system changes, network activity, and potential policy violations, enabling organisations to detect anomalies and security incidents in a timely manner [10].

Intrusion Detection Systems (IDS), particularly network-based IDS, complement SIEM platforms by analysing network traffic to identify malicious patterns, reconnaissance activities, and exploitation attempts. When IDS alerts are integrated into a SIEM, they can be correlated with host-based logs and authentication data, improving detection accuracy and contextual awareness.

The integration of centralised logging, intrusion detection, and alert correlation is widely recognised as a best practice for enhancing detection capabilities and reducing incident response times. This approach is especially relevant for healthcare SMEs, where limited resources necessitate efficient and automated security monitoring solutions.

2.4 Vulnerability Management and Incident Response

Vulnerability management is a critical element of cybersecurity governance and involves the continuous identification, assessment, prioritisation, and remediation of security weaknesses. Automated vulnerability scanning tools, such as OpenVAS, enable organisations to detect known vulnerabilities across systems and services and to prioritise remediation based on severity and potential impact [11].

Despite preventive measures, security incidents remain inevitable. Effective incident response therefore requires predefined procedures, clearly assigned roles and responsibilities, and tools that support evidence collection and forensic analysis. Digital Forensics

and Incident Response (DFIR) platforms, such as DFIR-IRIS, support structured incident management by enabling case creation, evidence tracking, timeline reconstruction, and reporting [12].

Both GDPR and NIS2 explicitly require organisations to detect, respond to, and report security incidents. GDPR mandates personal data breach notification under Articles 33 and 34, while NIS2 introduces mandatory incident reporting timelines for essential entities. Consequently, integrating vulnerability management and incident response into a unified security architecture is essential for ensuring operational resilience and regulatory compliance.

2.5 Summary

This chapter has reviewed the cybersecurity challenges faced by healthcare SMEs and examined the regulatory and standards-based frameworks governing their security obligations. It has highlighted the importance of risk-based security management, centralised monitoring, intrusion detection, vulnerability assessment, and incident response as foundational components of an effective and compliant cybersecurity strategy.

The concepts and best practices discussed in this chapter provide the theoretical and regulatory foundation for the system design, risk analysis, and implementation activities presented in the subsequent chapters of this report.

Chapter 3

Planning and Contextualisation

This chapter presents the organisational context and technical planning underpinning the project. It introduces the simulated healthcare SME scenario, identifies the resulting security and compliance requirements, and describes the design of the virtualised infrastructure used to meet these requirements. The chapter establishes how regulatory obligations derived from GDPR and NIS2 are translated into concrete architectural and technical decisions, forming the basis for the risk analysis, auditing, and incident response activities developed in later chapters.

3.1 Company Scenario

MediServ HealthTech Lda is a fictional small-to-medium-sized enterprise (SME) operating in the healthcare technology sector. The organisation provides digital healthcare services through an Electronic Health Record (EHR) platform used by medical professionals to manage patient data, including personal identification information, medical histories, and clinical records.

As a healthcare service provider, MediServ HealthTech Lda processes sensitive personal data classified as special category data under Article 9 of the General Data Protection Regulation (GDPR). Consequently, the organisation is subject to strict regulatory obligations concerning data protection, security of processing, and personal data breach

notification [3]. In addition, due to the essential nature of healthcare services, the company falls within the scope of the NIS2 Directive, which classifies healthcare providers as essential entities and mandates enhanced cybersecurity risk management and operational resilience measures [4].

The organisation's core business processes depend heavily on the availability, integrity, and confidentiality of its IT infrastructure. Any disruption, compromise, or unauthorised disclosure affecting the EHR system could result in operational downtime, regulatory sanctions, reputational damage, and potential risks to patient safety. For this reason, cybersecurity is treated as a critical business function and governance concern rather than a purely technical issue.

3.2 Security and Compliance Requirements

Based on the organisational context and applicable regulatory frameworks, a set of security and compliance requirements was identified to guide the design of the infrastructure and the selection of technical controls. These requirements include:

- Protection of sensitive healthcare data against unauthorised access and data breaches.
- Continuous monitoring of systems and network activity.
- Early detection of cyber threats and anomalous behaviour.
- Structured vulnerability management and periodic risk assessment.
- Defined incident response and reporting procedures aligned with NIS2 timelines.
- The ability to demonstrate compliance through logging, auditing, and documentation.

These requirements reflect the risk-based approach mandated by GDPR, particularly Article 32, as well as the operational security expectations outlined in Article 21 of the NIS2 Directive [3], [4]. They are further aligned with the principles of ISO/IEC 27005,

which emphasise systematic risk identification, evaluation, and treatment as the foundation of effective information security management [6].

3.3 Infrastructure Design Overview

To address the identified requirements, a virtualised infrastructure was designed to represent the core IT environment of MediServ HealthTech Lda. The architecture prioritises security monitoring, network segmentation, and auditability while remaining realistic and feasible within an SME context.

The infrastructure comprises nine virtual machines, each assigned a specific operational or security role. Network traffic is centrally controlled through a firewall, and security visibility is achieved through the integration of centralised logging, intrusion detection, vulnerability scanning, and incident response platforms. This layered approach supports defence-in-depth and facilitates compliance verification through technical evidence.

As shown in Figure 3.1, the infrastructure architecture of MediServ HealthTech Lda is illustrated.

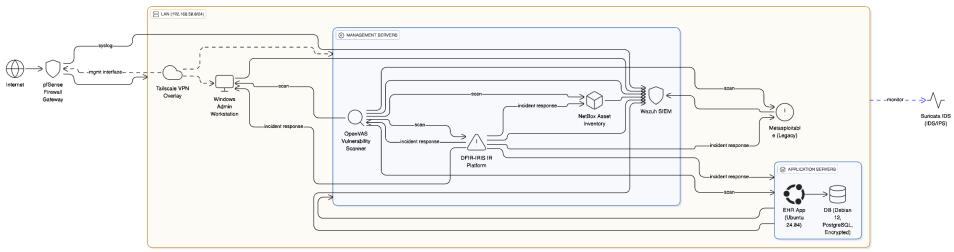

Figure 3.1: Infrastructure architecture of MediServ HealthTech Lda

3.4 Network Architecture and Connectivity

The network architecture is centred on a pfSense firewall acting as the primary gateway between internal systems and external networks. All internal systems operate within

the private address space `192.168.50.0/24`, which hosts application servers, security platforms, and administrative workstations.

The pfSense firewall enforces network access control and traffic filtering policies and hosts the Suricata Intrusion Detection System (IDS). Suricata inspects network traffic to detect malicious patterns, reconnaissance activities, and known attack signatures, thereby supporting early threat detection and compliance with NIS2 monitoring requirements [4].

Due to the distributed nature of the laboratory environment—where virtual machines are hosted on different physical systems—a secure VPN overlay using Tailscale was implemented. Tailscale provides encrypted connectivity between virtual machines and administrative systems without exposing internal services to the public internet. The pfSense firewall is optionally connected to the Tailscale network exclusively for management and log forwarding purposes, ensuring that operational traffic remains confined to the internal LAN.

3.5 Virtual Machines and System Roles

The virtual infrastructure deployed in this project includes the following systems:

- **pfSense Firewall with Suricata IDS**: Acts as the network gateway, enforces firewall rules, and monitors traffic using Suricata.
- **EHR Application Server (Ubuntu 24.04 LTS)**: Hosts the electronic health record application accessed by authorised users.
- **Database Server (Debian GNU/Linux 12)**: Stores sensitive healthcare data using PostgreSQL with encryption enabled.
- **Wazuh SIEM Manager**: Collects, correlates, and analyses logs from servers, workstations, and network devices.
- **OpenVAS (Greenbone)**: Performs vulnerability scanning across internal systems.

- **NetBox Asset Inventory Platform**: Maintains a structured inventory of assets, IP addresses, and system roles.
- **DFIR-IRIS Incident Response Platform**: Supports structured incident handling, evidence collection, and forensic analysis.
- **Windows Administrative Workstation**: Used for system administration and management tasks.
- **Vulnerable Linux System (Metasploitable)**: Represents a legacy system used for security testing, auditing, and incident simulation.

This separation of system roles supports the principle of least privilege and facilitates effective monitoring, auditing, and incident response.

All virtual machines were deployed as part of the project. The detailed installation and configuration steps for each VM are documented in Appendix A.

3.6 Security Monitoring and Logging Architecture

Centralised security monitoring is implemented using the Wazuh SIEM platform. Wazuh agents are deployed on all supported systems, including the EHR server, database server, and Windows administrative workstation. Systems that do not support native agents, such as pfSense, forward logs via syslog.

Wazuh aggregates logs related to authentication events, system configuration changes, and security-relevant activity. This architecture supports early threat detection, incident investigation, and compliance verification through auditable logs.

3.7 Summary

This chapter presented the planning and contextualisation of the project, including the organisational scenario, security and compliance requirements, and the design of the virtualised infrastructure. The proposed architecture reflects a realistic and resource-efficient

approach to securing a healthcare SME while addressing the obligations imposed by GDPR and NIS2. The integration of network security, centralised monitoring, vulnerability management, and incident response platforms establishes a solid foundation for the risk analysis, auditing, and incident simulation activities described in the subsequent chapters.

Chapter 4

Risk Analysis

This chapter delineates the information security risk analysis undertaken for MediServ HealthTech Lda. The assessment employs a structured, risk-based methodology consistent with ISO/IEC 27005 and ensures alignment with the risk management obligations stipulated by the General Data Protection Regulation (GDPR) and the NIS2 Directive. Its purpose is to identify critical assets, examine pertinent threats and vulnerabilities, appraise the associated risks, and establish mitigation measures that inform the design and implementation of security controls within the project.

4.1 Risk Management Methodology

The risk analysis undertaken in this project adheres to the principles and guidelines of ISO/IEC 27005, which establishes a structured framework for information security risk management [6]. Its primary aim is to identify, analyse, and evaluate risks to the confidentiality, integrity, and availability (CIA) of MediServ HealthTech Lda's information assets, thereby supporting the selection of appropriate technical and organisational security controls. In accordance with ISO/IEC 27005 recommendations for small-to-medium-sized enterprises (SMEs), a qualitative risk assessment approach was adopted to balance methodological rigour with practical feasibility. The methodology encompasses the following stages:

- Identification and classification of information assets
- Identification of relevant threats and vulnerabilities
- Risk estimation based on likelihood and impact
- Risk evaluation and prioritisation
- Definition of risk treatment decisions

This risk-based approach directly supports GDPR Article 32, which requires security measures proportionate to identified risks [3], as well as NIS2 Article 21, which mandates continuous risk analysis and the implementation of appropriate mitigation measures [4].

4.2 Scope of the Risk Analysis

The scope of the risk analysis includes all systems forming the project infrastructure, encompassing application servers, databases, network devices, security platforms, and administrative endpoints. Asset identification and documentation were performed using NetBox [13], ensuring consistency, traceability, and alignment between the technical infrastructure and the risk assessment process.

Particular emphasis was placed on systems processing personal and health-related data, which constitute special category personal data under GDPR Article 9 [3]. Supporting systems critical to detection, monitoring, and incident response were also included, as their compromise could indirectly impact the organisation's ability to maintain security and compliance.

4.3 Asset Identification and Classification

Assets were identified and classified according to their role within the infrastructure, the sensitivity of the data processed, and their importance to business continuity. Assets

handling electronic health records and patient data were classified as critical, reflecting their high regulatory and operational impact.

The complete asset inventory, including asset roles, IP addresses, and criticality levels, is documented in Appendix B. This inventory forms the foundation for all subsequent risk identification and evaluation activities.

4.4 Threat and Vulnerability Identification

Threat identification considered common threat sources relevant to healthcare environments, including external attackers, insider threats, malware, misconfiguration, and exploitation of known software vulnerabilities. These threat sources reflect realistic attack scenarios observed in healthcare organisations and documented by regulatory and security bodies [1].

Vulnerability identification was conducted using a combination of automated vulnerability scanning and security monitoring. OpenVAS scans [11] were performed against selected systems to identify known vulnerabilities and configuration weaknesses, providing evidence-based input into the risk analysis. The results revealed multiple high- and medium-severity vulnerabilities, particularly on the intentionally vulnerable Linux system deployed for testing and validation purposes (see Appendix F).

In addition, the Wazuh SIEM identified suspicious authentication-related activity, such as SSH events, contributing to the assessment of attack likelihood for externally accessible or privileged systems.

4.5 Risk Evaluation

Risk evaluation was performed by combining the likelihood of exploitation with the potential impact on the organisation. Likelihood was assessed based on factors such as exposure of services, presence of known vulnerabilities, threat attractiveness, and existing

security controls. Impact was evaluated in the context of healthcare operations, considering potential consequences including:

- Breach of personal and health data
- Service disruption or unavailability
- Regulatory non-compliance and sanctions
- Loss of monitoring or incident response capability

A qualitative risk matrix was used to classify risks as low, medium, high, or critical, ensuring alignment with ISO/IEC 27005 while remaining suitable for an SME context. The detailed risk register, including asset–threat–vulnerability mappings, likelihood and impact ratings, and resulting risk levels, is provided in Appendix F.

4.6 Risk Treatment Decisions

Risk treatment decisions were defined based on the evaluated risk levels, organisational risk tolerance, and available resources. High and critical risks, particularly those affecting systems processing healthcare data or administrative access, were prioritised for mitigation through technical and organisational controls. These controls include network segmentation, intrusion detection, centralised logging, access control, and system hardening.

Medium risks were addressed through a combination of mitigation and acceptance, depending on feasibility and residual risk. Certain risks associated with intentionally vulnerable systems were formally accepted, as these systems are isolated, do not process real data, and are deployed exclusively for testing, detection validation, and educational purposes. This risk acceptance decision is supported by compensating controls such as network isolation and enhanced monitoring.

A complete overview of risk treatment decisions, including mitigated and accepted risks, is documented in Appendix F.

4.7 Compliance Alignment

The documented risk management process directly supports regulatory compliance by demonstrating:

- GDPR Article 32: Risk-based selection of appropriate technical and organisational security measures
- GDPR Article 5(2): Accountability through documented and justifiable security decisions
- NIS2 Article 21: Continuous risk analysis, monitoring capabilities, and incident preparedness

By formally documenting risks, vulnerabilities, and treatment decisions, the organisation demonstrates its ability to justify security measures to supervisory authorities and auditors.

4.8 Summary

This chapter presented a structured information security risk analysis conducted in accordance with ISO/IEC 27005. Critical assets were identified and classified, relevant threats and vulnerabilities were analysed using evidence from OpenVAS and SIEM monitoring, and risks were evaluated using a qualitative risk matrix. High-risk scenarios, particularly those affecting healthcare data and administrative access, were prioritised and addressed through appropriate mitigation strategies, while controlled risk acceptance was applied where justified. This risk-driven approach provides a solid foundation for the vulnerability management, auditing, and incident response activities presented in the subsequent chapters.

Chapter 5

Asset Inventory and Vulnerability Management

Effective asset inventory and vulnerability management are foundational elements of an organisation's cybersecurity governance. Without accurate knowledge of existing systems, their roles, and the data they process, it is not possible to perform meaningful risk assessments or to implement proportionate security controls.

Both GDPR and NIS2 establish the necessity of maintaining visibility over information systems. The GDPR accountability principle (Article 5(2)) requires organisations to demonstrate compliance, while Article 32 mandates the implementation of appropriate technical and organisational measures based on risk [3]. Similarly, NIS2 Article 21 requires essential entities to implement continuous risk management, including asset awareness and vulnerability handling processes [4].

In this project, asset inventory and vulnerability management were implemented as integrated and continuous processes, enabling the identification of critical systems, the assessment of their exposure to known vulnerabilities, and the prioritisation of remediation actions in line with a risk-based security strategy.

5.1 Asset Inventory with NetBox

5.1.1 Asset Identification and Documentation

To maintain a structured and centralised asset inventory, the NetBox platform was deployed. NetBox functions as an authoritative source of truth for infrastructure components, supporting accurate documentation and traceability of systems.

For each asset, the following attributes were documented:

- Device name and type
- IP address and associated network segment
- Assigned functional role (e.g. firewall, application server, SIEM)
- Operating system
- Business criticality

Maintaining this level of documentation supports operational management, facilitates auditing activities, and enables organisations to demonstrate control over their infrastructure, as required by GDPR and NIS2.

As shown in Figure 5.1, below is an image from the NetBox dashboard illustrating the asset inventory and assigned roles.

5.1.2 Asset Classification

Assets documented in NetBox were classified according to:

- Business criticality, reflecting their impact on core operations
- Data sensitivity, based on the type of data processed

This classification directly aligns with the asset identification and criticality assessment performed during the risk analysis phase described in Chapter **??**. Systems processing

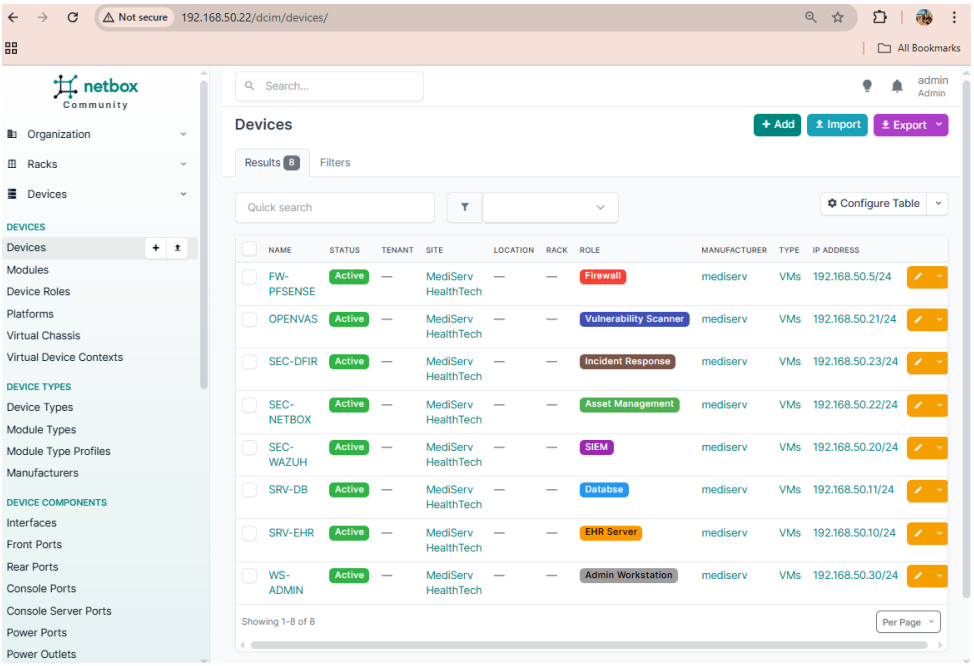

Figure 5.1: NetBox asset inventory showing devices and assigned roles

healthcare data—such as the EHR application server and the database server—were classified as critical assets due to the sensitivity of personal and medical data under GDPR Article 9 [3].

The use of NetBox ensured consistency between asset inventory, risk analysis, and vulnerability management, reinforcing a structured and auditable approach to security governance.

Additional screenshots and detailed evidence of the NetBox asset inventory, including device classifications, IP assignments, and role definitions, are provided in Appendix B.

5.2 Vulnerability Management Methodology

Vulnerability management was conducted using a combination of automated scanning and contextual risk assessment. Automated vulnerability scanning was performed using OpenVAS (Greenbone Vulnerability Management), complemented by network reconnaissance and security monitoring outputs.

The vulnerability management process followed these steps:

- Identification of scan targets based on asset criticality
- Execution of vulnerability scans
- Analysis and classification of identified vulnerabilities
- Prioritisation based on risk and business impact
- Definition of remediation or risk acceptance strategies

This methodology aligns with ISO/IEC 27001 and ISO/IEC 27005 recommendations for continuous vulnerability assessment and treatment, and supports the risk-based approach required by both GDPR and NIS2 [6], [7].

5.3 Vulnerability Scanning and Results

5.3.1 Scan Scope

Vulnerability scans were conducted against the following systems:

- EHR Application Server
- Windows Administrative Workstation
- Vulnerable Linux System (legacy platform)

These targets were selected to represent a mix of critical production systems and an intentionally vulnerable legacy system, allowing both realistic risk assessment and validation of detection and monitoring capabilities.

5.3.2 Scan Execution

OpenVAS was configured to perform authenticated and unauthenticated scans where applicable. Identified vulnerabilities were mapped to known Common Vulnerabilities and

Exposures (CVE) entries and assigned severity levels using the Common Vulnerability Scoring System (CVSS). This approach enables objective vulnerability classification and supports prioritisation decisions based on standardised severity metrics. Further detailed evidence and vulnerability listings are provided in Appendix C.

As shown in Figure 5.2, below is an image summarising the OpenVAS vulnerability scan targets and severity distribution.

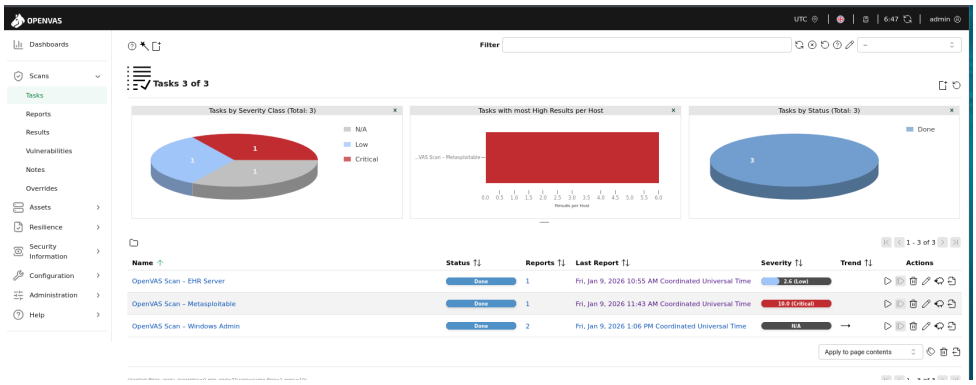

Figure 5.2: OpenVAS vulnerability scan summary and severity distribution

5.3.3 Key Findings

The vulnerability scans revealed a clear distinction between production systems and the legacy vulnerable system:

- **EHR Servers**: Limited number of low-severity findings, primarily related to service configuration and version exposure. No critical unpatched vulnerabilities identified.
- **Windows Administrative Workstation**: No vulnerabilities detected.
- **Legacy Vulnerable System**: Multiple critical and high-severity vulnerabilities, including remote code execution flaws and outdated services. Intended outcome to support security testing and incident simulation.

These findings validate the risk assessment presented in Chapter 4, where legacy systems were identified as high-risk assets requiring compensating controls [1].

5.4 Vulnerability Prioritisation and Treatment

Vulnerabilities were prioritised based on:

- CVSS severity score
- Asset criticality
- Potential impact on confidentiality, integrity, and availability

Table 5.1: Vulnerability Treatment Strategy

Asset	**Vulnerability Severity**	**Treatment Decision**
EHR Server	Low	Mitigate
Windows Admin	None	No treatment required
Legacy System	Critical	Accept with compensating controls

For production systems, mitigation strategies included:

- Service hardening
- Secure configuration adjustments
- Access control enforcement
- Continuous monitoring through SIEM

For the legacy system, vulnerabilities were formally accepted as residual risk, justified by its isolation and exclusive use for security testing. Compensating controls—including network segmentation and enhanced monitoring—were implemented to reduce exposure, consistent with ISO/IEC 27005 risk treatment guidance [6].

5.5 Integration with Risk Analysis and Monitoring

Vulnerability management results were integrated into the broader security and risk management framework:

- High-risk vulnerabilities informed prioritisation in the ISO/IEC 27005 risk matrix
- OpenVAS findings supported audit conclusions and remediation planning
- Vulnerability-related exploitation attempts were detectable via Wazuh SIEM and Suricata IDS

This integration demonstrates a mature security lifecycle approach, where vulnerability management directly supports detection, auditing, and incident response activities.

5.6 Compliance Alignment

The asset inventory and vulnerability management activities directly support regulatory compliance:

- GDPR Article 32: Demonstrates implementation of appropriate technical measures based on risk
- GDPR Accountability Principle: Enables evidence-based compliance demonstration
- NIS2 Article 21: Addresses vulnerability handling, risk management, and monitoring obligations

Maintaining an up-to-date asset inventory and performing regular vulnerability assessments enhances the organisation's ability to prevent, detect, and respond to cybersecurity incidents, as required for essential entities under NIS2.

5.7 Summary

This chapter presented the implementation of asset inventory and vulnerability management processes within the project infrastructure. The deployment of NetBox enabled structured asset documentation and classification, while OpenVAS provided visibility into

known security weaknesses across systems. By linking vulnerability findings to asset criticality and risk analysis, the project demonstrates a risk-based, auditable, and regulation-aligned approach to cybersecurity management suitable for healthcare SMEs.

Chapter 6

Auditing and Security Testing

Auditing and security testing are fundamental components of an effective information security management system, providing assurance that implemented technical and organisational controls operate as intended. While vulnerability management focuses on identifying exploitable weaknesses, auditing evaluates whether systems are securely configured, monitored, and governed in accordance with defined policies, recognised standards, and regulatory obligations.

Both the General Data Protection Regulation (GDPR) and the NIS2 Directive explicitly require continuous evaluation of security controls. GDPR Article 32 mandates "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures" [3]. Similarly, NIS2 Article 21 obliges essential entities to implement ongoing risk analysis, monitoring, and security assessment practices to ensure resilience against cyber threats [4].

In this project, auditing and security testing were conducted using a dual assurance approach:

- **Internal security audits**, focusing on systems under direct organisational control
- **Controlled external security audits**, simulating attacker visibility from an authorised VPN perimeter

This approach aligns with ISO/IEC 27001 control validation practices and ISO/IEC

27005 risk verification principles, ensuring that security measures are proportionate, auditable, and risk-driven [6], [7].

6.1 Internal Security Audit

Scope and Objectives

The internal security audit assessed the effectiveness of security controls implemented within MediServ HealthTech Lda's internal infrastructure. The primary objectives were to:

- Verify firewall enforcement and internal network segmentation
- Assess host-level exposure and service hardening
- Validate centralised logging, alerting, and monitoring capabilities
- Identify misconfigurations or deviations from defined security policies

The audit scope included the following assets:

- pfSense security gateway and IDS/IPS configuration
- Electronic Health Record (EHR) application server
- Database server storing healthcare data
- Windows administrative workstation
- Centralised logging and monitoring infrastructure (Wazuh SIEM)

Internal Audit Methodology

The internal audit followed a structured methodology aligned with ISO/IEC 27001 Annex A controls and ISO/IEC 27005 guidance. The applied techniques included:

- Network discovery and port scanning using Nmap

- Service exposure validation through SYN scans and host discovery
- Review of firewall rules and IDS policies
- Log analysis and alert correlation using the Wazuh SIEM platform
- Targeted service assessment for critical systems

All activities were conducted in a controlled environment to avoid disruption to services processing healthcare data.

```
└─$ sudo nmap -sS -Pn 192.168.50.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-08 10:20 EST
Nmap scan report for 192.168.50.1
Host is up (0.0035s latency).
All 1000 scanned ports on 192.168.50.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:03 (VMware)

Nmap scan report for 192.168.50.5
Host is up (0.0032s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:51:E5:86 (VMware)

Nmap scan report for 192.168.50.11
Host is up (0.0079s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
5432/tcp open  postgresql
MAC Address: 00:0C:29:08:9C:31 (VMware)

Nmap scan report for 192.168.50.20
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  closed http
443/tcp open   https
MAC Address: 00:0C:29:21:5E:03 (VMware)

Nmap scan report for 192.168.50.133
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
```

Figure 6.1: Internal network reconnaissance results

Internal Audit Findings

The internal audit identified the following key observations:

- **Firewall Enforcement and Service Exposure**: The pfSense firewall regulated traffic, ensuring that production systems exposed only essential services in line with the principle of least privilege.
- **Service Exposure Control**: Critical servers, including the EHR and database systems, exposed only required services (e.g., HTTPS and PostgreSQL). Intentionally vulnerable systems exposed additional services for testing purposes, consistent with their documented risk acceptance status.
- **Detection and Monitoring Effectiveness**: Suricata successfully detected reconnaissance activity such as port scanning. Authentication failures and system events were centrally logged, providing complete audit trails.
- **Administrative Endpoint Risk**: The Windows administrative workstation represented a higher-risk asset due to its privileged access, reinforcing the need for continuous monitoring and strict access control.

6.2 External Security Audit

Scope and Ethical Considerations

The external security audit was conducted within a strictly authorised and ethically approved scope. The assessment targeted a VPN-accessible subnet (`192.168.11.0/24`) provided exclusively for educational and testing purposes.

Explicit authorisation was obtained prior to testing, and all activities complied with professional security assessment ethics. No exploitation, denial-of-service, or destructive techniques were employed. The audit focused on exposure and configuration analysis rather than penetration testing, in line with legal and ethical standards governing security assessments [7], [14].

External Audit Methodology

The external audit simulated the perspective of an authenticated but untrusted VPN peer. The following techniques were employed:

- **Network Discovery:** Nmap scan of VPN subnet hosts and ports.
- **Cryptographic Assessment:** OpenSSL check of TLS cipher strength and certificate validity.
- **Service Fingerprinting:** Banner and protocol analysis to detect vulnerable software versions.
- **Automated Vulnerability Scanning:** OpenVAS mapping of services against known CVEs.
- **Lateral Movement Testing:** Evaluation of VPN peer access to restricted subnets.

Testing focused on identifying architectural and configuration weaknesses rather than exploiting vulnerabilities.

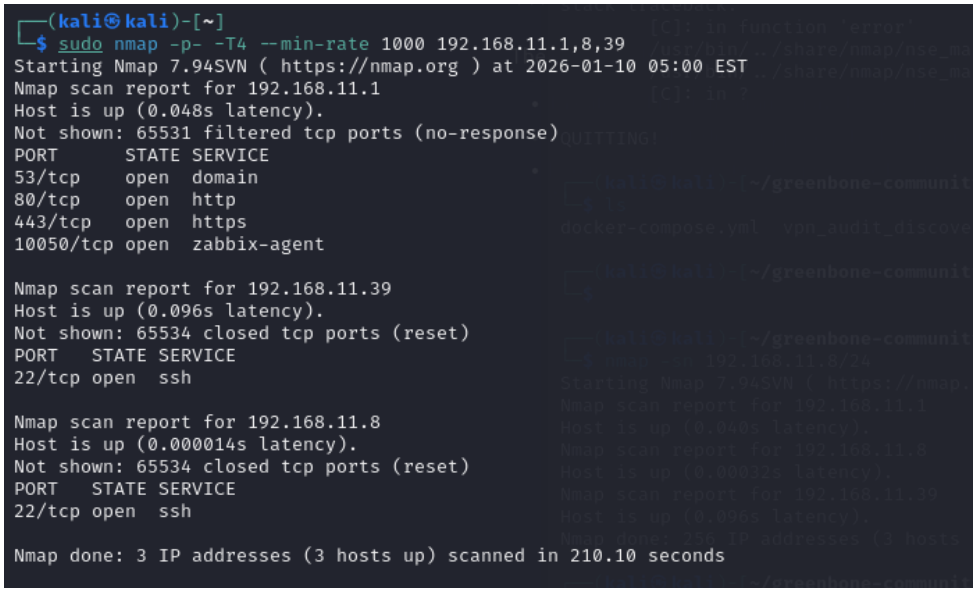

Figure 6.2: External audit scan results within authorised VPN scope

External Audit Findings

The external audit identified several significant findings:

- **Lack of Network Segmentation**: The VPN subnet exhibited a flat topology, allowing unrestricted peer-to-peer communication. Security management services were accessible from any VPN peer, increasing the risk of lateral movement [4].
- **Cryptographic Weaknesses**: Self-signed certificates were used for management interfaces, reducing assurance of confidentiality and integrity and exposing the infrastructure to potential man-in-the-middle attacks [3].
- **Information Disclosure via Service Banners**: Service banners disclosed operating system and software versions, increasing the feasibility of targeted attacks [3].
- **Infrastructure Resilience Observations**: NTP and DNS services were active on the gateway. While time synchronisation supports audit trail integrity, unencrypted DNS traffic within a flat network introduces spoofing risks.

A detailed technical breakdown of external audit findings, evidence, and compliance mapping is provided in Appendix H.

6.3 Risk Evaluation and Remediation Alignment

External audit findings were evaluated against regulatory requirements and security best practices. Recommended remediation measures included:

- Implementation of VPN peer isolation following Zero Trust principles
- Deployment of an internal Public Key Infrastructure (PKI)
- Restriction of management services to dedicated administrative hosts
- Hardening of service banners and reduction of unnecessary protocol exposure

All remediation decisions were evaluated using the risk management methodology defined in Chapter **??** and documented in the risk register presented in Appendix F. These measures align with ISO/IEC 27001 control objectives and NIS2 resilience requirements [4], [7].

6.4 Validation of Detection Capabilities

A key objective of the auditing phase was to validate detection and monitoring capabilities. During both internal and external audits:

- Reconnaissance activity triggered Suricata IDS alerts
- Host-level events generated Wazuh SIEM alerts
- Alerts were timestamped and correlated, enabling forensic traceability

This demonstrates compliance with monitoring and detection obligations under NIS2 and supports incident readiness requirements [4], [15].

6.5 Audit Findings and Recommendations

Based on the combined audit results, the following recommendations were formulated:

- Continued hardening of administrative endpoints
- Periodic review and tuning of IDS detection rules
- Regular internal audits to detect configuration drift
- Segmentation of security management infrastructure
- Continuous improvement of cryptographic controls

6.6 Compliance Alignment

The auditing and security testing activities directly support regulatory compliance by demonstrating:

- GDPR Article 32: Regular testing and evaluation of security measures
- NIS2 Article 21: Risk management, monitoring, and security assessment

By documenting audit scope, methodology, findings, and remediation decisions, the organisation demonstrates accountability and audit readiness to supervisory authorities.

6.7 Summary

This chapter demonstrated how structured auditing and security testing were used to validate the effectiveness of implemented security controls. Through internal audits and ethically scoped external assessments, the project verified firewall enforcement, intrusion detection, and centralised monitoring. The results confirmed the organisation's ability to detect and assess security threats while identifying architectural improvements necessary to meet GDPR and NIS2 obligations.

Chapter 7

Incident Response and Forensic Analysis

7.1 Role of Incident Response in Healthcare Cybersecurity

In contemporary healthcare environments, cybersecurity incidents must be treated as an inevitability rather than an exception. The increasing digitalisation of clinical services, combined with the high value of health data, has positioned healthcare organisations among the most frequently targeted sectors by ransomware and data exfiltration campaigns [1]. Consequently, the ability to detect, contain, and respond effectively to incidents is a critical determinant of organisational resilience.

From a regulatory perspective, incident response is no longer optional. GDPR Articles 33 and 34 impose strict obligations on organisations to detect personal data breaches, assess their impact, and notify supervisory authorities and affected data subjects within defined timeframes [3]. In parallel, NIS2 Article 23 introduces mandatory incident reporting timelines for essential entities, while Article 21 requires the implementation of risk management measures that explicitly include incident detection and response capabilities [4].

Within this context, incident response must be embedded as an operational process supported by technical controls, documented procedures, and forensic readiness. This chapter evaluates the incident response and forensic analysis capabilities implemented in this project through a controlled but realistic ransomware and data exfiltration simulation targeting critical healthcare systems.

7.2 Incident Response Policy and Framework

7.2.1 Adopted Incident Response Lifecycle

An incident response policy was defined in accordance with established international standards, primarily NIST SP 800-61 (Computer Security Incident Handling Guide) and ISO/IEC 27035 [16], [17]. These standards provide a structured and widely accepted framework for handling cybersecurity incidents in regulated environments.

The adopted lifecycle consists of the following phases:

- Preparation
- Detection and Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

This lifecycle ensures a systematic approach to incident handling, enabling consistent decision-making, traceable actions, and post-incident learning. Importantly, it also supports the GDPR accountability principle and NIS2 governance requirements by ensuring that incidents are documented, reviewed, and used to improve future security posture [3], [4].

7.2.2 Organisational Roles and Responsibilities

Effective incident response requires clear role definition and separation of responsibilities. The following roles were defined for the project environment:

- **Security Analyst**: Responsible for continuous monitoring, alert triage, and initial technical analysis
- **System Administrator**: Executes containment, eradication, and recovery actions on affected systems
- **Incident Response Coordinator**: Oversees the incident lifecycle, ensures documentation completeness, and coordinates reporting obligations
- **Management**: Provides strategic oversight and approves external communications

Although implemented within a laboratory environment, this role model reflects realistic practices suitable for small and medium-sized healthcare organisations and aligns with recommendations from ENISA and ISO standards [1], [7].

Documentary evidence supporting the incident response policy described in this section is provided in Appendix G.

7.3 Incident Detection and Alerting Architecture

Incident detection in this project is based on a defence-in-depth monitoring architecture, integrating host-based, network-based, and centralised correlation mechanisms:

- Wazuh SIEM for host-level telemetry, log aggregation, and correlation
- Suricata IDS for network traffic inspection and threat detection
- pfSense firewall for traffic monitoring and enforcement of containment actions

Security-relevant events—including abnormal file modifications, suspicious outbound connections, and anomalous network patterns—were centrally correlated within the SIEM.

Alerts were classified by severity and mapped to incident categories, supporting prioritisation and escalation in line with NIST guidance [16].

As shown in Figure 7.1, below is an image from wazuh dashboard illustrating wazuh alerts.

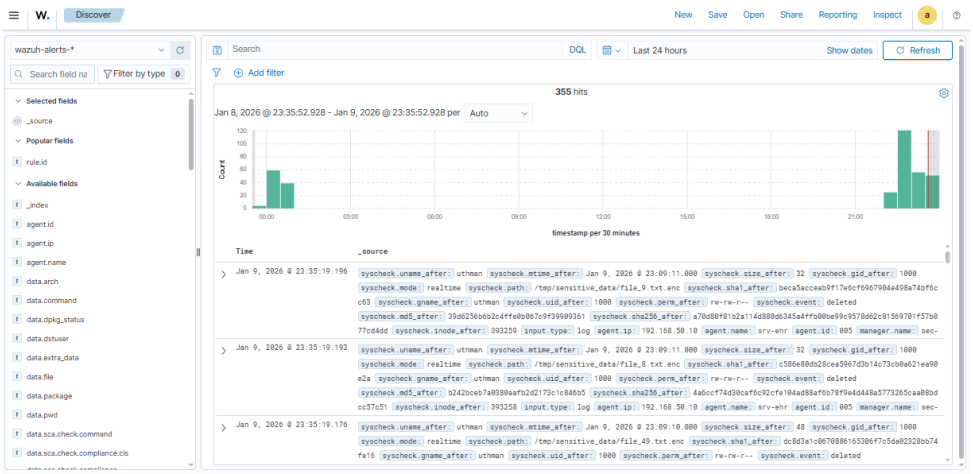

Figure 7.1: Wazuh SIEM alerts triggered during ransomware simulation

Security-relevant events—including abnormal file modifications, suspicious outbound connections, and anomalous network patterns—were centrally correlated within the SIEM. Alerts were classified by severity and mapped to incident categories, supporting prioritisation and escalation in line with NIST guidance [15]. Further illustrative evidence of Wazuh alerts, including agent activity, security events, and detailed drill-downs, is provided in Appendix D.

7.4 Incident Simulation Design

7.4.1 Scenario Definition

To validate the effectiveness of the incident response framework, a multi-stage ransomware and data exfiltration simulation was conducted. The scenario targeted two critical healthcare assets:

- Electronic Health Record (EHR) Server

- Database (DB) Server

The simulated attack followed a realistic threat progression commonly observed in healthcare breaches:

- Execution of a ransomware-like encryption process on the EHR server
- Mass file modification indicative of data encryption
- Subsequent unauthorised data exfiltration from the database server

Such combined ransomware-and-exfiltration attacks have been identified by ENISA as a dominant threat pattern in the healthcare sector [1]. All actions were performed using dummy data in an isolated laboratory environment. Further illustrative evidence of this incident, including DFIR-IRIS case screenshots and timeline reconstruction, is provided in Appendix E.

7.4.2 Detection and Initial Analysis

During the simulation:

- Wazuh File Integrity Monitoring (FIM) detected high-frequency file changes within seconds
- SIEM correlation rules escalated the event severity to critical

The correlation of host-based and network-based telemetry enabled rapid identification of the affected systems and the attack stages, demonstrating the value of integrated monitoring architectures recommended by ISO/IEC 27002 and NIST [15], [18].

7.5 Incident Handling and Forensic Case Management

7.5.1 DFIR-IRIS Case Creation and Evidence Preservation

Once the incident was confirmed, a formal case was created in the DFIR-IRIS incident response platform. DFIR-IRIS was used to:

- Register the incident and assign severity and status
- Attach SIEM alerts, firewall logs, and screenshots
- Maintain a structured and auditable incident timeline
- Preserve evidence in accordance with forensic best practices

This approach supports forensic readiness, ensuring that evidence is preserved in a manner suitable for regulatory review and potential legal proceedings [19].

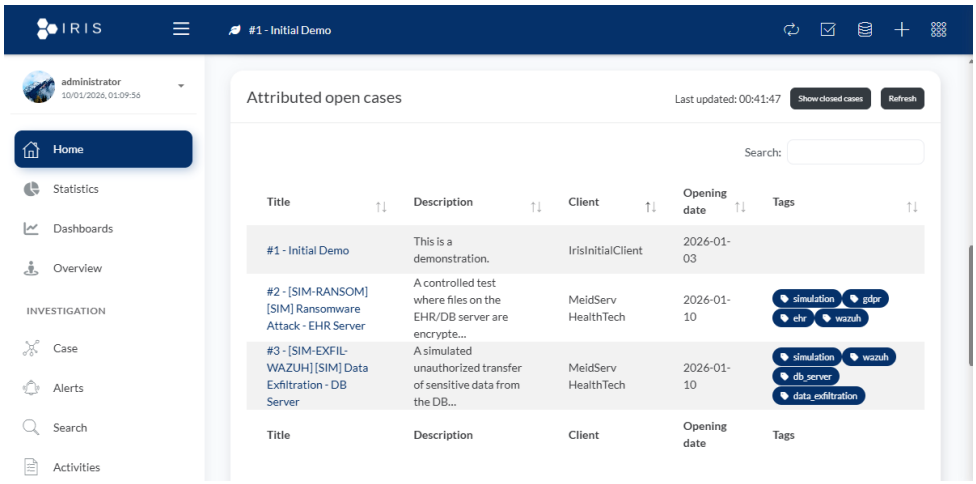

Figure 7.2: DFIR-IRIS incident case overview and evidence repository

7.5.2 Timeline Reconstruction

DFIR-IRIS was further used to reconstruct a chronological timeline of the incident, including:

- Initial detection timestamp
- Alert correlation and escalation events
- Containment and remediation actions
- Recovery and monitoring restoration

Timeline reconstruction is essential for root-cause analysis, regulatory reporting, and post-incident evaluation, as recommended by both GDPR supervisory authorities and NIST [3], [16].

Evidence of incident documentation, evidence preservation, and timeline reconstruction is provided in Appendix E.

7.6 Forensic Artefacts Acquisition and Management

During the incident response simulation for the SRV-EHR virtual machine, two types of forensic artefacts were captured to support investigation:

- **Disk Image** – A bit-for-bit copy of the SRV-EHR VM storage.
- **Process Memory Dump** – Memory of a specific running process.

These artefacts were handled according to standard digital forensic principles to ensure integrity, traceability, and reproducibility. Due to DFIR-IRIS storage limitations, the raw files were stored securely offline, while their metadata and hash values were registered in DFIR-IRIS.

7.6.1 Disk Image

A full disk image of SRV-EHR was acquired and verified. While the raw image remains offline, it is linked to the corresponding incident in DFIR-IRIS to ensure traceability and chain of custody. Preliminary analysis of the image was conducted to inspect key system directories and logs.

7.6.2 Process Memory Dump

Memory of a single running process from SRV-EHR was captured as a proof-of-concept for live memory analysis. Like the disk image, the memory dump is stored offline with corresponding metadata and hash values recorded in DFIR-IRIS.

7.6.3 Evidence Integration in DFIR-IRIS

Both artefacts are represented in DFIR-IRIS through metadata entries, which include:

- Evidence type (Disk Image / Memory Capture)
- Acquisition method
- Hash values (SHA256)
- Source system and acquisition timestamp

This approach demonstrates incident-driven forensic practice while accommodating system storage limitations.

All acquisition commands, hash values, and DFIR-IRIS evidence registration details are documented in Appendix I – Forensic Artefacts. Screenshots of DFIR-IRIS entries can also be included there.

7.7 Containment, Eradication, and Recovery Actions

Containment measures were implemented to limit further damage and prevent ongoing data loss:

- Immediate network isolation of the compromised EHR server via firewall rules
- Temporary restriction of database network access
- Blocking of suspicious outbound connections

Eradication involved identifying and removing the malicious script and auditing system privileges, revealing excessive permissions on a service account. Recovery focused on restoring normal monitoring coverage and verifying system integrity.

Although simulated, these actions reflect realistic response procedures applicable to operational healthcare environments and align with ISO/IEC 27035 recommendations.

7.8 Post-Incident Evaluation and Lessons Learned

Post-incident activities were conducted to critically assess the effectiveness of the response and identify improvement opportunities.

Strengths identified include:

- Near real-time detection through host-based monitoring
- Effective containment via centralised firewall enforcement
- Comprehensive forensic documentation using DFIR-IRIS

Identified weaknesses include:

- Dependence on manual intervention for containment actions
- Excessive service account privileges
- Limited visibility into database-level file access events

Based on these findings, the following improvements are recommended:

- Automation of containment through SIEM-to-firewall integration
- Enforcement of least-privilege access controls
- Regular vulnerability scanning and proactive ingestion of findings into incident management workflows [6], [7]

7.9 Regulatory Compliance Alignment

The incident response and forensic analysis activities implemented in this project directly support compliance with applicable regulations:

- GDPR Articles 33 and 34: Breach detection, documentation, and notification readiness
- GDPR Article 5(2): Accountability through structured incident documentation
- NIS2 Articles 21 and 23: Risk management, incident handling, and reporting obligations

The structured documentation and traceability provided by DFIR-IRIS enable the organisation to demonstrate due diligence, accountability, and preparedness during regulatory audits or supervisory authority investigations. This evidential approach ensures that incident response is not only operationally effective but also legally defensible.

Technical and documentary evidence supporting GDPR and NIS2 compliance claims related to incident response is consolidated in Appendix G.

7.10 Chapter Summary

This chapter demonstrated the design, implementation, and validation of an incident response and forensic analysis framework suitable for healthcare SMEs operating under GDPR and NIS2 obligations. Through a realistic multi-stage ransomware, data exfiltration simulation and Forensic Artefacts Acquisition, the project validated its detection, containment, and documentation capabilities while also identifying critical areas for improvement.

Overall, the results confirm that while the implemented monitoring and forensic documentation mechanisms are mature and compliant, further automation is required to reduce response times and enhance resilience. This evaluation reinforces the importance of continuous improvement and operational readiness in healthcare cybersecurity.

Chapter 8

GDPR and NIS2 Compliance Mapping

8.1 Importance of Regulatory Compliance in Healthcare Cybersecurity

In healthcare environments, cybersecurity is not solely a technical concern but a binding legal obligation. Organisations that process personal and health-related data must comply with sector-specific regulatory frameworks, most notably the General Data Protection Regulation (GDPR) and the NIS2 Directive. Both frameworks adopt a risk-based and accountability-driven approach, requiring organisations to implement appropriate security measures and to demonstrate their effectiveness through documentation and evidence [3], [4].

Failure to comply with these obligations may result in significant administrative fines, reputational damage, and operational disruption. Consequently, regulatory compliance must be embedded into the design of information systems and security processes rather than treated as an afterthought.

This chapter provides a structured mapping between the technical and organisational controls implemented in this project and the relevant GDPR and NIS2 requirements. The

objective is to demonstrate that compliance is not claimed abstractly, but supported by concrete, auditable technical evidence.

8.2 GDPR Compliance Mapping

8.2.1 GDPR Article 32 – Security of Processing

Article 32 of the GDPR requires data controllers and processors to implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risk, taking into account the nature of the data processed and the likelihood and severity of potential impacts [3].

In this project, Article 32 compliance is addressed through a combination of preventive, detective, and responsive controls selected based on the risk analysis conducted in Chapter 4.

Table 8.1: GDPR Article 32 Compliance Mapping

GDPR Requirement	**Implemented Measure**	**Supporting Evidence**
Confidentiality	Network segmentation, access control, firewall enforcement	pfSense configuration files, audit screenshots
Integrity	Centralised log collection and correlation	Wazuh SIEM alerts and dashboards
Availability	Continuous monitoring and incident response readiness	SIEM availability views, IR documentation
Resilience	Network-based intrusion detection	Suricata IDS alerts
Risk-based security	ISO/IEC 27005-aligned risk analysis	Risk matrix (Chapter 4)
Regular testing	Security auditing and vulnerability assessments	OpenVAS reports, audit results

The implemented measures were selected based on a documented risk assessment and tailored to the sensitivity of healthcare data. This demonstrates adherence to the GDPR requirement that security controls must be proportionate to risk rather than generic or

ad hoc [1], [7].

8.2.2 GDPR Articles 33 and 34 – Personal Data Breach Notification

Articles 33 and 34 of the GDPR require organisations to detect personal data breaches, notify the competent supervisory authority within 72 hours, and—where applicable—inform affected data subjects without undue delay [3].

The project infrastructure supports breach notification readiness through integrated detection, documentation, and forensic capabilities.

Table 8.2: GDPR Breach Notification Readiness

Requirement	**Implementation**
Breach detection	SIEM and IDS correlation (Wazuh + Suricata)
Incident documentation	DFIR-IRIS case management
Evidence preservation	Centralised log retention and timeline reconstruction
Reporting readiness	Defined incident response policy and procedures

By combining real-time monitoring with structured incident documentation, the organisation is capable of identifying, analysing, and reporting personal data breaches within regulatory timeframes. The use of DFIR-IRIS further supports the GDPR accountability principle by ensuring traceability and completeness of incident records.

8.3 NIS2 Compliance Mapping

8.3.1 NIS2 Article 21 – Cybersecurity Risk Management Measures

Article 21 of the NIS2 Directive mandates that essential and important entities implement appropriate technical, operational, and organisational measures to manage cybersecurity

risks, including prevention, detection, response, and recovery capabilities [4].

Table 8.3: NIS2 Article 21 Compliance Mapping

NIS2 Requirement	**Implemented Measure**	**Evidence**
Risk analysis	ISO/IEC 27005-based risk assessment	Chapter 4
Incident handling	Structured incident response lifecycle	Chapter 7
Business continuity	Monitoring and recovery preparedness	SIEM dashboards, IR documentation
Asset management	Centralised asset inventory	NetBox screenshots
Security monitoring	Host- and network-based monitoring	Wazuh & Suricata alerts
Vulnerability management	Regular vulnerability scanning	OpenVAS reports

These measures reflect a continuous risk management approach rather than isolated security controls. This aligns with NIS2's emphasis on organisational maturity and ongoing risk governance rather than point-in-time compliance [20].

8.3.2 NIS2 Article 23 – Incident Reporting Obligations

Article 23 of the NIS2 Directive introduces strict incident reporting obligations, including early warnings, incident notifications, and final reports within defined timelines [4].

Table 8.4: NIS2 Incident Reporting Support

Requirement	**Supporting Mechanism**
Early detection	Real-time IDS and SIEM alerts
Incident classification	Severity-based alert correlation
Documentation	DFIR-IRIS incident cases
Timeline reconstruction	Forensic timeline features
Post-incident analysis	Lessons learned documentation

The ability to rapidly detect incidents, reconstruct timelines, and maintain structured documentation enables compliance with NIS2 reporting obligations and supports communication with national competent authorities.

8.4 Accountability and Demonstrability of Compliance

A central principle shared by GDPR and NIS2 is accountability, which requires organisations not only to implement security measures but also to demonstrate their effectiveness upon request by supervisory or competent authorities [3], [4].

In this project, demonstrability is achieved through:

- Documented risk analysis and treatment decisions
- Centralised logging and monitoring evidence
- Vulnerability scan reports and audit findings
- Incident response records and forensic timelines

Together, these elements provide a coherent compliance narrative supported by verifiable technical evidence. This approach reflects best practices recommended by ISO standards and ENISA for regulated sectors such as healthcare.

8.5 Chapter Summary

This chapter mapped the technical and organisational controls implemented in the project to the core requirements of the GDPR and the NIS2 Directive. By adopting a risk-based approach, implementing continuous monitoring, performing vulnerability management, and validating incident response capabilities, the infrastructure demonstrates both operational resilience and regulatory compliance.

Most importantly, the explicit linkage between controls, evidence, and legal obligations illustrates the organisation's ability to demonstrate accountability, a critical requirement for healthcare entities operating under modern European cybersecurity and data protection regulations.

Chapter 9

Conclusions and Future Work

This project addressed the design, implementation, and evaluation of a secure and compliant IT infrastructure for a healthcare small-to-medium-sized enterprise (SME), MediServ HealthTech Lda, with specific alignment to the requirements of the General Data Protection Regulation (GDPR) and the NIS2 Directive. Given the sensitivity of health data and the essential nature of healthcare services, the project adopted a risk-based, standards-aligned, and evidence-driven approach to cybersecurity governance and operations [3], [4].

A virtualised multi-host infrastructure was successfully deployed and secured, integrating network protection, centralised logging, vulnerability management, and incident response capabilities. Network perimeter security was enforced through a pfSense firewall, while the integration of the Suricata Intrusion Detection System (IDS) enabled real-time inspection and detection of suspicious traffic patterns, supporting early threat identification and containment [1], [4]. Centralised security monitoring was achieved through the Wazuh Security Information and Event Management (SIEM) platform, which provided host-based intrusion detection, log correlation, and alerting across critical systems, thereby supporting continuous monitoring and operational awareness [7], [15].

Asset visibility and vulnerability management were addressed through the deployment of NetBox and OpenVAS. NetBox enabled structured documentation of assets, roles, and network topology, supporting both risk assessment and accountability requirements [3],

[4]. OpenVAS facilitated systematic vulnerability scanning, enabling the identification, prioritisation, and mitigation of technical weaknesses in accordance with recognised vulnerability management practices [18], [21].

The project further validated the organisation's detection and response capabilities through internal and external security audits, as well as a controlled incident simulation. The integration of DFIR-IRIS provided a structured framework for incident handling, evidence collection, and forensic timeline reconstruction, demonstrating preparedness to manage security incidents in compliance with GDPR breach notification obligations and NIS2 incident reporting requirements [3], [4]. The use of DFIR-IRIS also reinforced the principles of traceability, evidential integrity, and post-incident analysis, which are essential for regulatory inspections and continuous improvement [17].

The risk analysis conducted in alignment with ISO/IEC 27005 served as the foundation for control selection and prioritisation. By explicitly linking identified assets, threats, vulnerabilities, and risks to implemented technical and organisational measures, the project ensured that security controls were proportionate, justified, and auditable, in line with both GDPR and NIS2 expectations [3], [4], [6].

Overall, the results demonstrate that a healthcare SME can achieve a robust cybersecurity posture and demonstrable regulatory compliance using open-source and resource-efficient tools, provided that security initiatives are driven by structured risk management, continuous monitoring, and formalised incident response processes [1].

9.1 Limitations of the Project

Despite meeting its primary objectives, several limitations must be acknowledged. The infrastructure was implemented within a controlled laboratory environment, which does not fully replicate the operational complexity, scale, and threat exposure of a real-world healthcare production network. As such, certain factors—such as high availability constraints, legacy system integration, and large-scale user behaviour—were not fully represented [1].

Additionally, some organisational and governance controls, including staff security awareness training, supplier and third-party risk management, and formal business continuity exercises, were discussed conceptually but not fully implemented or tested. These controls are explicitly referenced within both GDPR and NIS2 as critical components of organisational security and resilience [3], [4].

Furthermore, incident response activities were based on simulated attack scenarios rather than real security incidents. While these simulations effectively validated detection, escalation, and documentation workflows, real-world incidents may involve greater uncertainty, time pressure, and cross-organisational coordination challenges [16], [17].

9.2 Future Work and Improvements

Several improvements could be implemented to further enhance the organisation's cybersecurity maturity and compliance posture:

- **Multi-Factor Authentication (MFA)**: Enforcing MFA for administrative and user access would significantly reduce the risk of credential-based attacks [1], [22].
- **Endpoint Detection and Response (EDR)**: Deploying EDR solutions on critical systems would improve visibility into advanced and persistent threats beyond traditional log-based detection [23].
- **Advanced Network Segmentation**: Further segmentation of internal networks could limit lateral movement and reduce the impact of potential compromises [24], [25].
- **Automated Backup and Recovery**: Implementing automated, encrypted, and regularly tested backups would enhance service availability and resilience against ransomware and data loss incidents [3], [4].
- **Security Awareness Training**: Regular training programmes would address human-factor risks, such as phishing and social engineering [1], [18].

- **SIEM Rule Optimisation**: Continuous tuning of detection and correlation rules would reduce false positives and improve alert fidelity [15].
- **Formal Compliance Audits**: Periodic internal and external compliance audits would support sustained alignment with evolving regulatory and threat landscapes [3], [4].

These enhancements represent realistic and incremental next steps for a growing healthcare SME seeking to strengthen its security posture while maintaining operational feasibility.

9.3 Final Remarks

This project underscores the importance of aligning technical cybersecurity controls with legal, regulatory, and organisational requirements, particularly in critical sectors such as healthcare. By adopting a structured, risk-based methodology and leveraging integrated security tools, organisations can enhance resilience to cyber threats while fulfilling GDPR and NIS2 obligations in a demonstrable and auditable manner [3], [4].

The architectures, methodologies, and practices presented in this report provide a practical and scalable foundation for real-world healthcare environments. They illustrate how compliance, security, and operational effectiveness can be balanced, even within the constraints typically faced by SMEs. As regulatory scrutiny and cyber threats continue to evolve, such integrated and evidence-driven approaches will remain essential for sustainable cybersecurity governance.

Bibliography

[1] ENISA, "Threat landscape for the healthcare sector," European Union Agency for Cybersecurity, Tech. Rep., 2023.

[2] I. Security, "Cost of a data breach report 2023," IBM Corporation, Tech. Rep., 2023.

[3] E. Union, *Regulation (eu) 2016/679 (general data protection regulation)*, Official Journal of the European Union, Apr. 2016.

[4] E. Union, *Directive (eu) 2022/2555 (nis2 directive)*, Official Journal of the European Union, Dec. 2022.

[5] ENISA, "Cybersecurity for smes – challenges and recommendations," European Union Agency for Cybersecurity, Tech. Rep., 2022.

[6] ISO/IEC, *ISO/IEC 27005:2018 – Information Security Risk Management*. International Organization for Standardization, 2018.

[7] ISO/IEC, *ISO/IEC 27001:2022 – Information Security Management Systems*. International Organization for Standardization, 2022.

[8] NIST, "Framework for improving critical infrastructure cybersecurity, version 1.1," National Institute of Standards and Technology, Tech. Rep., 2018.

[9] Verizon, "2023 data breach investigations report," Verizon Enterprise, Tech. Rep., 2023.

[10] A. Behl and K. Behl, *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford University Press, 2017.

[11] G. Networks, "Openvas vulnerability scanning – technical documentation," Greenbone Networks, Tech. Rep., 2023.

[12] DFIR-IRIS, "Incident response platform documentation," DFIR-IRIS Project, Tech. Rep., 2024.

[13] J. Stretch, *Netbox: Infrastructure resource modeling*, `https://github.com/netbox-community/netbox`, Accessed: 2026-01-10, 2016.

[14] K. Scarfone and P. Mell, "Guide to penetration testing (nist sp 800-115)," National Institute of Standards and Technology, Tech. Rep., 2008.

[15] K. Kent, M. Souppaya, and R. Chandramouli, "Guide to computer security log management (nist sp 800-92)," National Institute of Standards and Technology, Tech. Rep., 2006.

[16] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide (nist sp 800-61 revision 2)," National Institute of Standards and Technology, Tech. Rep., 2012.

[17] ISO/IEC, *ISO/IEC 27035:2016 – Information Security Incident Management*. International Organization for Standardization, 2016.

[18] ISO/IEC, *ISO/IEC 27002:2022 – Information Security Controls*. International Organization for Standardization, 2022.

[19] ISO/IEC, *ISO/IEC 27037:2012 – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. International Organization for Standardization, 2012.

[20] ENISA, "Guidelines on security measures for healthcare providers," European Union Agency for Cybersecurity, Tech. Rep., 2023.

[21] J. T. F. T. Initiative, "Security and privacy controls for federal information systems and organizations (nist sp 800-53 rev. 5)," National Institute of Standards and Technology, Tech. Rep., 2020.

[22] P. Grassi, M. Garcia, and J. Fenton, "Digital identity guidelines (nist sp 800-63-3)," National Institute of Standards and Technology, Tech. Rep., 2017.

[23] N. I. of Standards and Technology, *Nist cybersecurity framework*, `https://www.nist.gov/cyberframework`, Accessed: 2026-01-10, 2018.

[24] M. Carpenter, M. Barrett, and W. Burr, "Guidelines on firewalls and firewall policy (nist sp 800-41 rev. 1)," National Institute of Standards and Technology, Tech. Rep., 2009.

[25] ISO/IEC, *ISO/IEC 27033:2015 – Network Security*. International Organization for Standardization, 2015.

Appendix A

Installation Process

pfSense, Suricata, and Tailscale Installation & Configuration

A.1 pfSense Installation

A.1.1 Virtual Machine Preparation

* pfSense deployed as a virtual firewall appliance using VMware Workstation * VM configuration: - OS type: FreeBSD (64-bit) - CPU: 2 vCPUs - Memory: 2–4 GB RAM - Storage: 20 GB * Network adapters: - WAN → Bridged / NAT (Internet access) - LAN → Host-Only Network (VMnet3) - TAILSCALE → Assigned later via virtual interface

A.1.2 Installation Steps

* Boot from pfSense ISO * Select Install pfSense * Use default keymap and partitioning (Auto ZFS/UFS) * Complete installation and reboot * Remove ISO after installation

A.1.3 Initial Configuration (Setup Wizard)

* WAN interface → Internet-facing adapter, IPv4 via DHCP (later static if required) * LAN interface → VMnet3, Static IPv4: 192.168.50.5/24 * DHCP server on LAN disabled

(all machines use static IPs)

A.1.4 LAN Network Design

* LAN subnet: 192.168.50.0/24 * Default gateway: 192.168.50.5 * VMware Host Adapter (VMnet3): 192.168.50.1

A.1.5 Firewall Rules

* Allow internal traffic for testing * Permit ICMP (ping) * Allow outbound traffic to WAN * Example LAN rule: Pass, Interface LAN, Protocol Any, Source LAN subnet, Destination Any

A.1.6 NAT Configuration

* Outbound NAT set to Automatic * WAN performs NAT for LAN traffic * Internet access enabled for internal VMs

A.1.7 Tailscale Integration

* Install via System → Package Manager * Enable Tailscale service * Add interface linked to tailscale0 (no manual IP) * Firewall rules allow traffic from Tailscale interface

A.1.8 Suricata Integration

* Install via System → Package Manager * Enable on LAN interface (WAN/Tailscale excluded during testing) * Ruleset: Emerging Threats Open, auto-updates enabled, IDS mode only * Alerts generated via Nmap, port sweeps, attack simulations * Verified in Suricata and pfSense logs

A.1.9 Syslog Forwarding

* Forward logs to Wazuh server (UDP, port 514) * Log types: firewall, system * Logs received at OS level but not fully parsed in dashboard

A.1.10 Limitations

* pfSense hardened appliance, extra agents caused instability * Suricata alerts remained local (no Wazuh correlation) * Tailscale service occasionally stopped after reboot * DNS resolution issues fixed by explicit DNS/gateway settings

A.1.11 Architectural Justification

* pfSense + Suricata → Network intrusion detection/auditing * Wazuh → Host-based monitoring/SIEM * Tailscale → Secure overlay network * Design aligns with NIS2 defense-in-depth principles

A.1.12 Conclusion

* Deployment demonstrated firewall enforcement, IDS, logging, secure remote access * Implementation meets functional and academic requirements

A.2 EHR Application Server Installation (SRV-EHR)

VM Name: SRV-EHR OS: Ubuntu Server 24.04 LTS IP: 192.168.50.10 (static)

A.2.1 Base System Configuration

* Set hostname:

```
sudo hostnamectl set-hostname srv-ehr
```

* Configure static IP (Netplan):

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    ens33:
```

```
      dhcp4: no
      addresses:
        - 192.168.50.10/24
      gateway4: 192.168.50.5
      nameservers:
        addresses:
          - 192.168.50.5
          - 1.1.1.1
```

```
sudo netplan apply
```

* Enable time sync:

```
sudo timedatectl set-timezone UTC
sudo systemctl enable systemd-timesyncd
sudo systemctl restart systemd-timesyncd
```

A.2.2 Secure Remote Access (SSH)

* Install and enable SSH:

```
sudo apt update
sudo apt install openssh-server -y
sudo systemctl enable ssh
```

* Harden SSH:

```
sudo nano /etc/ssh/sshd_config
```

```
PermitRootLogin no
PasswordAuthentication no
```

```
sudo systemctl restart ssh
```

A.2.3 Firewall Configuration

```
sudo apt install ufw -y
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw enable
sudo ufw status verbose
```

A.2.4 Wazuh Agent Installation

```
curl -sO https://packages.wazuh.com/4.x/wazuh-agent_4.7.3-1_amd64
   .deb
sudo dpkg -i wazuh-agent_4.7.3-1_amd64.deb
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

A.2.5 Intrusion Prevention (Fail2Ban)

```
sudo apt install fail2ban -y
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local

[sshd]
enabled = true

sudo systemctl enable fail2ban
sudo systemctl restart fail2ban
fail2ban-client status
```

A.2.6 Web Server Installation

```
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
```

A.2.7 EHR Application Deployment

```
sudo apt install python3-pip python3-venv -y
mkdir /opt/ehr-app
cd /opt/ehr-app
python3 -m venv venv
source venv/bin/activate
pip install flask
python app.py
```

A.2.8 Reverse Proxy Configuration

```
sudo nano /etc/nginx/sites-available/ehr

server {
    listen 80;
    server_name srv-ehr;

    location / {
        proxy_pass http://127.0.0.1:5000;
    }
}

sudo ln -s /etc/nginx/sites-available/ehr /etc/nginx/sites-
   enabled/
sudo nginx -t
```

```
sudo systemctl reload nginx
```

A.2.9 HTTPS Configuration

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/ehr.key \
-out /etc/ssl/certs/ehr.crt

listen 443 ssl;
ssl_certificate /etc/ssl/certs/ehr.crt;
ssl_certificate_key /etc/ssl/private/ehr.key;

sudo systemctl reload nginx
```

A.2.10 Result

* Secure remote administration * Centralized monitoring via Wazuh * Intrusion prevention with Fail2Ban * Encrypted web access (HTTPS) * Functional healthcare-style application for compliance validation

A.3 Database Server (SRV-DB) Installation

VM Name: SRV-DB OS: Debian 12 (Bookworm) IP: 192.168.50.11 (static) Disk Encryption: LUKS enabled during installation Installation type: Minimal system (no GUI)

A.3.1 Initial System Setup

```
apt update && apt upgrade -y
apt install vim curl wget ufw gnupg -y

nano /etc/network/interfaces
```

```
auto eth0
iface eth0 inet static
    address 192.168.50.11
    netmask 255.255.255.0
    gateway 192.168.50.5

systemctl restart networking
```

A.3.2 PostgreSQL Installation and Configuration

```
apt install postgresql postgresql-contrib -y

nano /etc/postgresql/15/main/postgresql.conf
listen_addresses = '192.168.50.11'

nano /etc/postgresql/15/main/pg_hba.conf
hostssl    all    all    192.168.50.10/32    md5
```

A.3.3 PostgreSQL SSL Configuration

```
mkdir /etc/postgresql/ssl
chown postgres:postgres /etc/postgresql/ssl
chmod 700 /etc/postgresql/ssl

sudo -u postgres openssl req -new -x509 -days 365 -nodes \
-out /etc/postgresql/ssl/server.crt \
-keyout /etc/postgresql/ssl/server.key
chmod 600 /etc/postgresql/ssl/server.key

nano /etc/postgresql/15/main/postgresql.conf
ssl = on
```

```
ssl_cert_file = '/etc/postgresql/ssl/server.crt'
ssl_key_file = '/etc/postgresql/ssl/server.key'

systemctl restart postgresql
```

A.3.4 Firewall Configuration

```
ufw default deny incoming
ufw default allow outgoing
ufw allow from 192.168.50.10 to any port 5432
ufw allow 1514/tcp   # Wazuh agent communication
ufw enable
ufw status
```

A.3.5 Wazuh Agent Installation

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | \
gpg --dearmor -o /usr/share/keyrings/wazuh-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/wazuh-archive-keyring.
   gpg] \
https://packages.wazuh.com/4.x/apt/ stable main" \
> /etc/apt/sources.list.d/wazuh.list

apt update
apt install wazuh-agent -y

nano /var/ossec/etc/ossec.conf
<address>192.168.50.20</address>

systemctl enable wazuh-agent
```

```
systemctl start wazuh-agent
```

A.3.6 Validation

```
ss -tulnp | grep 5432
ufw status
systemctl status postgresql
systemctl status wazuh-agent
```

A.3 Wazuh SIEM Installation (SEC-WAZUH)

VM Name: SEC-WAZUH OS: Ubuntu Server 22.04 LTS IP: 192.168.50.20

A.3.1 Base System Preparation

```
sudo hostnamectl set-hostname sec-wazuh
sudo apt update && sudo apt upgrade -y
sudo apt install -y curl unzip gnupg apt-transport-https chrony
   ufw
sudo systemctl enable chrony --now
```

A.3.2 Static Network Configuration

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 192.168.50.20/24
```

```
      gateway4: 192.168.50.5
      nameservers:
        addresses: [192.168.50.5, 1.1.1.1]
```

```
sudo netplan apply
```

A.3.3 Firewall Configuration

```
sudo ufw allow 22/tcp
sudo ufw allow 443/tcp
sudo ufw allow 1514/tcp
sudo ufw allow 1515/tcp
sudo ufw allow 55000/tcp
sudo ufw allow 514/udp
sudo ufw enable
```

A.3.4 Wazuh All-in-One Installation

```
cd /tmp
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
chmod +x wazuh-install.sh
sudo ./wazuh-install.sh -a
```

This installs: * Wazuh Manager * OpenSearch * Wazuh Dashboard

A.3.5 Credential Retrieval

```
sudo cat /usr/share/wazuh-dashboard/data/wazuh-install-files/
   wazuh-passwords.txt
```

A.3.6 Service Verification

```
sudo systemctl status wazuh-manager
sudo systemctl status opensearch
sudo systemctl status wazuh-dashboard
```

A.3.7 Enable Syslog for pfSense

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>192.168.50.1</allowed-ips>
</remote>
```

```
sudo systemctl restart wazuh-manager
```

A.3.8 Dashboard Access

Web interface:

```
https://192.168.50.20
```

Login using credentials generated during installation.

A.3.9 Installation Validation

```
sudo /var/ossec/bin/agent_control -l
sudo tail -f /var/ossec/logs/alerts/alerts.json
```

A.4 Wazuh SIEM Installation (SEC-WAZUH)

VM Name: SEC-WAZUH OS: Ubuntu Server 22.04 LTS IP: 192.168.50.20

A.4.1 Base System Preparation

```
sudo hostnamectl set-hostname sec-wazuh
sudo apt update && sudo apt upgrade -y
sudo apt install -y curl unzip gnupg apt-transport-https chrony
   ufw
sudo systemctl enable chrony --now
```

A.4.2 Static Network Configuration

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 192.168.50.20/24
      gateway4: 192.168.50.5
      nameservers:
        addresses: [192.168.50.5, 1.1.1.1]
```

```
sudo netplan apply
```

A.4.3 Firewall Configuration

```
sudo ufw allow 22/tcp
sudo ufw allow 443/tcp
sudo ufw allow 1514/tcp
sudo ufw allow 1515/tcp
sudo ufw allow 55000/tcp
```

```
sudo ufw allow 514/udp
sudo ufw enable
```

A.4.4 Wazuh All-in-One Installation

```
cd /tmp
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
chmod +x wazuh-install.sh
sudo ./wazuh-install.sh -a
```

Installs: * Wazuh Manager * OpenSearch * Wazuh Dashboard

A.4.5 Credential Retrieval

```
sudo cat /usr/share/wazuh-dashboard/data/wazuh-install-files/
   wazuh-passwords.txt
```

A.4.6 Service Verification

```
sudo systemctl status wazuh-manager
sudo systemctl status opensearch
sudo systemctl status wazuh-dashboard
```

A.4.7 Enable Syslog for pfSense

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>192.168.50.1</allowed-ips>
```

```
</remote>
```

```
sudo systemctl restart wazuh-manager
```

A.4.8 Dashboard Access

Web interface:

`https://192.168.50.20`

Login using credentials generated during installation.

A.4.9 Installation Validation

```
sudo /var/ossec/bin/agent_control -l
sudo tail -f /var/ossec/logs/alerts/alerts.json
```

A.5 NetBox (Asset Inventory) Installation

VM: SEC-NETBOX OS: Ubuntu Server IP: 192.168.50.22

A.5.1 System Preparation

```
sudo apt update && sudo apt upgrade -y
sudo hostnamectl set-hostname sec-netbox
sudo apt install -y git curl python3 python3-venv python3-pip \
postgresql postgresql-contrib redis-server \
build-essential libpq-dev nginx ufw
```

A.5.2 Firewall Configuration

```
sudo ufw allow OpenSSH
sudo ufw allow 80/tcp
sudo ufw enable
```

A.5.3 PostgreSQL & Redis

```
sudo -u postgres psql
CREATE DATABASE netbox;
CREATE USER netbox WITH PASSWORD 'StrongPasswordHere';
GRANT ALL PRIVILEGES ON DATABASE netbox TO netbox;
\q

sudo systemctl enable redis-server --now
```

A.5.4 NetBox Installation

```
sudo mkdir -p /opt/netbox
sudo adduser --system --group netbox
sudo chown netbox:netbox /opt/netbox
cd /opt/netbox
sudo -u netbox git clone https://github.com/netbox-community/
   netbox.git .
```

A.5.5 Python Environment

```
sudo -u netbox python3 -m venv /opt/netbox/venv
sudo -u netbox /opt/netbox/venv/bin/pip install --upgrade pip
sudo -u netbox /opt/netbox/venv/bin/pip install -r requirements.
   txt
```

A.5.6 Configuration

```
sudo -u netbox cp netbox/netbox/configuration.example.py \
netbox/netbox/configuration.py
sudo -u netbox nano netbox/netbox/configuration.py
```

```
# Key settings:
DATABASE = { 'NAME':'netbox','USER':'netbox','PASSWORD':'
    StrongPasswordHere','HOST':'localhost' }
STATIC_ROOT = '/opt/netbox/netbox/static/'
SECRET_KEY = 'generated-secret-key'

python3 -c 'from secrets import token_urlsafe; print(
    token_urlsafe(50))'
```

A.5.7 Database & Static Files

```
sudo -u netbox /opt/netbox/venv/bin/python3 netbox/manage.py
    migrate
sudo -u netbox /opt/netbox/venv/bin/python3 netbox/manage.py
    createsuperuser
sudo -u netbox /opt/netbox/venv/bin/python3 netbox/manage.py
    collectstatic
```

A.5.8 Service (Gunicorn)

```
sudo nano /etc/systemd/system/netbox.service
# Gunicorn service definition
sudo systemctl daemon-reload
sudo systemctl enable netbox
sudo systemctl start netbox
```

A.5.9 Nginx Reverse Proxy

```
sudo nano /etc/nginx/sites-available/netbox
# Proxy to 127.0.0.1:8001
sudo ln -s /etc/nginx/sites-available/netbox /etc/nginx/sites-
    enabled/
```

```
sudo rm /etc/nginx/sites-enabled/default
sudo nginx -t
sudo systemctl restart nginx
```

A.5.10 Verification

Access NetBox:

`http://192.168.50.22`

Web interface accessible Static files loaded Asset inventory operational

Appendix A.6 – DFIR-IRIS Installation

A.6.1 System Preparation

The DFIR-IRIS platform was deployed on a dedicated virtual machine (`SEC-DFIR`) running Ubuntu Server with a static IP address.

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y curl git ca-certificates gnupg lsb-release
sudo hostnamectl set-hostname sec-dfir
```

—

A.6.2 Firewall Configuration

The Uncomplicated Firewall (UFW) was enabled to restrict access to essential services only.

```
sudo ufw allow 22
sudo ufw allow 443
sudo ufw enable
sudo ufw status
```

—

A.6.3 Docker Installation

Docker and Docker Compose were installed to support the containerized deployment of DFIR-IRIS.

```
curl -fsSL https://get.docker.com | sudo sh
sudo systemctl enable docker
sudo systemctl start docker
sudo usermod -aG docker $USER
newgrp docker
sudo apt install -y docker-compose-plugin
docker compose version
```

—

A.6.4 DFIR-IRIS Deployment

The DFIR-IRIS source code was obtained from the official repository and configured using environment variables.

```
cd /opt
git clone https://github.com/dfir-iris/iris-web.git
cd iris-web
cp .env.example .env
```

Key parameters configured in `.env` include database credentials, secret keys, and HTTPS binding.

—

A.6.5 Evidence Storage Configuration

A persistent directory was created to securely store digital evidence.

```
sudo mkdir -p /srv/dfir-iris/evidence
sudo chown -R 1000:1000 /srv/dfir-iris
sudo chmod 750 /srv/dfir-iris/evidence
```

This directory was mapped into the DFIR-IRIS container to ensure evidence persistence.

—

A.6.6 Service Startup and Access

The DFIR-IRIS services were started using Docker Compose.

```
docker compose up -d
docker ps
```

The web interface was accessed securely via HTTPS:

```
https://192.168.50.23
```

—

A.6.7 Post-Installation Verification

Evidence storage accessibility and firewall status were verified.

```
docker exec -it iriswebapp_app ls /opt/iris/web/static/evidence
sudo ufw status
```

—

A.6.8 Outcome

DFIR-IRIS was successfully deployed as a secure, containerized incident response platform with persistent evidence storage and restricted network access, ready for SOC operations and GDPR/NIS2 incident handling.

A.7 Greenbone (OpenVAS) Docker Installation

VM: SEC-GREENBONE OS: Ubuntu Server IP: 192.168.50.23

A.7.1 Preparation and Cleanup

```
# Stop and disable native GVM services
sudo systemctl stop gsad gvmd ospd-openvas postgresql redis-
   server
sudo systemctl disable gsad gvmd ospd-openvas postgresql redis-
   server
```

A.7.2 Install Docker Dependencies

```
sudo apt update
sudo apt install docker.io docker-compose-v2 -y
sudo systemctl start docker
sudo systemctl enable docker
```

A.7.3 Deploy Greenbone Community Edition

```
mkdir ~/greenbone-community-container && cd ~/greenbone-community
   -container
curl -fL https://greenbone.github.io/docs/latest/_static/docker-
   compose-22.4.yml -o docker-compose.yml
sudo docker compose -p greenbone-community-edition pull
sudo docker compose -p greenbone-community-edition up -d
```

A.7.4 Feed Synchronization

```
sudo docker compose -p greenbone-community-edition logs -f gvmd
```

Note: Sync of NVTs and SCAP/CERT data may take hours. Minimum: 4GB RAM, 4 CPU cores.

A.7.5 Accessing the Interface

Web dashboard:

`http://127.0.0.1:9392`

Default credentials: `admin / admin`

A.7.6 Management Commands

```
# Stop GVM
sudo docker compose -p greenbone-community-edition stop

# Start GVM
sudo docker compose -p greenbone-community-edition up -d

# Check container stats
sudo docker stats
```

Feed status available via Dashboard → Administration → Feed Status.

A.8 Metasploitable (Vulnerable Test VM)

VM: SEC-META OS: Metasploitable 2 (Linux-based) IP: 192.168.50.21

A.8.1 Purpose

Metasploitable was deployed as a deliberately vulnerable virtual machine to serve as a target for penetration testing, IDS/IPS validation, and security monitoring exercises.

A.8.2 Configuration

No additional configuration or hardening was performed. The VM was used in its default vulnerable state to generate alerts and validate detection capabilities across the security stack.

A.8.3 Role in Project

* Provided attack surface for Suricata IDS testing * Used to validate Wazuh alert correlation * Served as a controlled environment for security demonstrations

A.9 Windows 10 Wazuh Agent Installation (ws-admin)

System: Windows 10 VM Name: ws-admin IP: 192.168.50.24 Gateway: 192.168.50.5

A.9.1 Network Configuration

* Static IP set via Windows Network Adapter settings: - IP: 192.168.50.24 - Subnet: 255.255.255.0 - Gateway: 192.168.50.5 - DNS: 192.168.50.5, 1.1.1.1

A.9.2 Wazuh Agent Download

```
# From PowerShell (run as Administrator)
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/
   wazuh-agent-4.7.3-1.msi -OutFile C:\wazuh-agent.msi
```

A.9.3 Installation

```
msiexec /i C:\wazuh-agent.msi /q WAZUH_MANAGER="192.168.50.20"
   WAZUH_AGENT_NAME="ws-admin"
```

A.9.4 Service Management

```
# Start agent service
net start wazuh-agent

# Stop agent service
net stop wazuh-agent
```

```
# Set service to auto-start
sc config wazuh-agent start= auto
```

A.9.5 Verification

```
# Check agent status
sc query wazuh-agent

# Confirm connectivity to Wazuh Manager
type "C:\Program Files (x86)\ossec-agent\logs\ossec.log"
```

A.9.6 Result

* Windows 10 endpoint (ws-admin) integrated with Wazuh SIEM * Logs forwarded to Wazuh Manager (192.168.50.20) * Agent configured for persistence and auto-start

Appendix B

Asset Inventory (NetBox)

Purpose

Demonstrate asset identification and classification, supporting risk analysis and compliance.

Contents

The NetBox deployment provides a centralized inventory of project assets. Screenshots below illustrate sites, devices, roles, IP assignments, and criticality levels.

B.1 Sites

The site entry represents the organizational scope for all registered devices.

B.2 Devices

Devices include firewalls, SIEM, database servers, application servers, and endpoints.

B.3 Device Classification

Each device is classified by role and assigned a criticality level to support risk analysis.

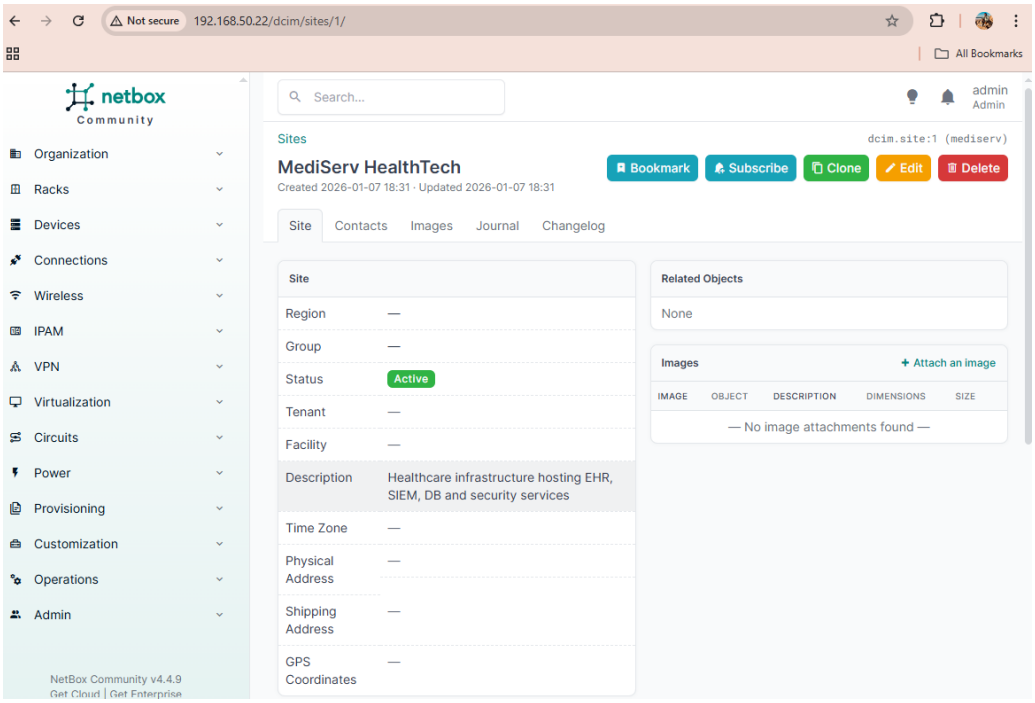

Figure B.1: NetBox site details – MediServ HealthTech

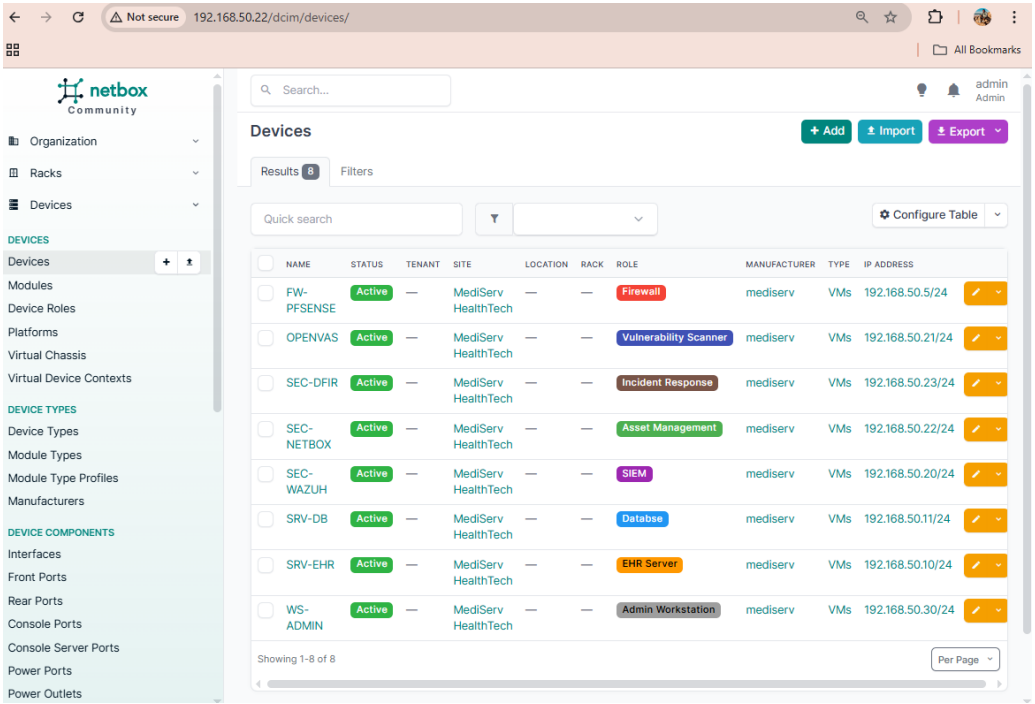

Figure B.2: List of registered devices in NetBox

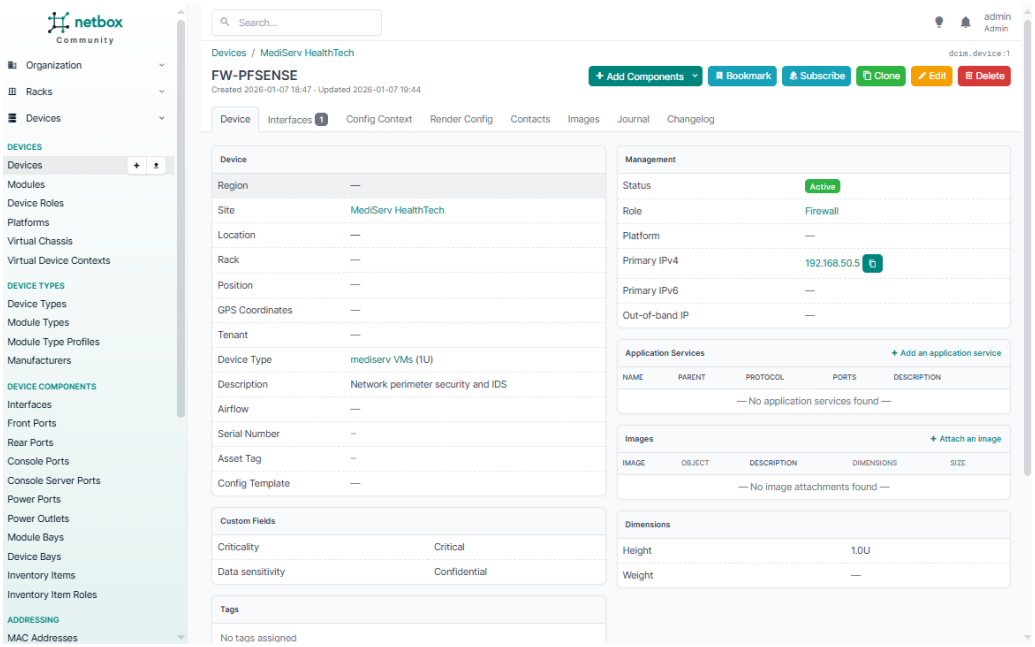

Figure B.3: Device detail view showing classification and criticality

B.4 Roles

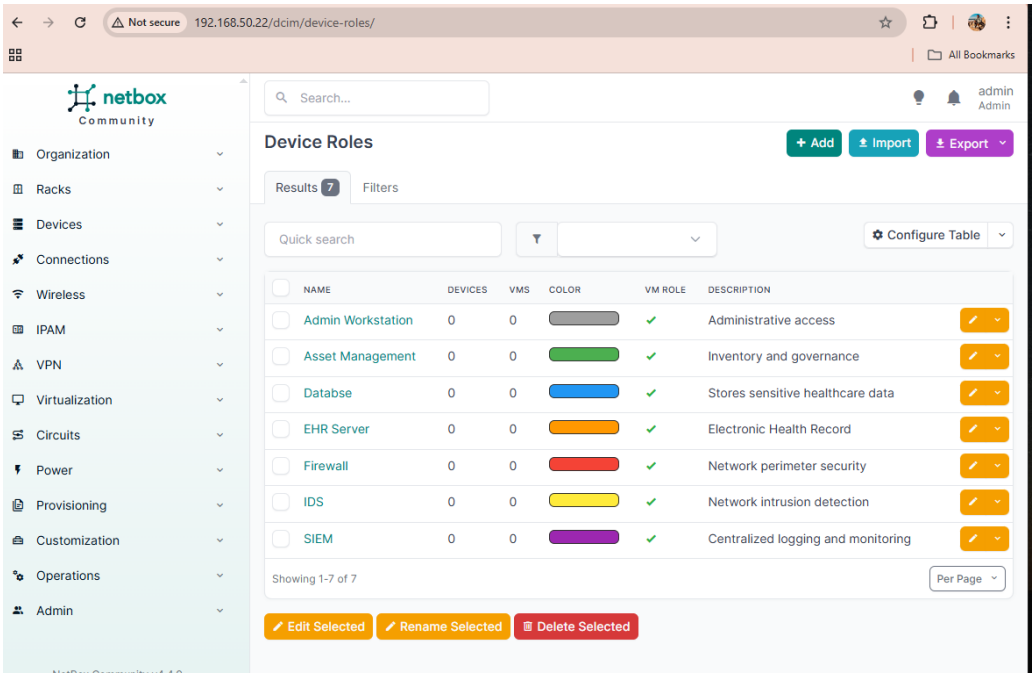

Figure B.4: Device roles – Firewall, SIEM, DB, Application, Endpoint

Roles ensure consistent categorization of assets across the environment.

B.5 IP Address Assignments

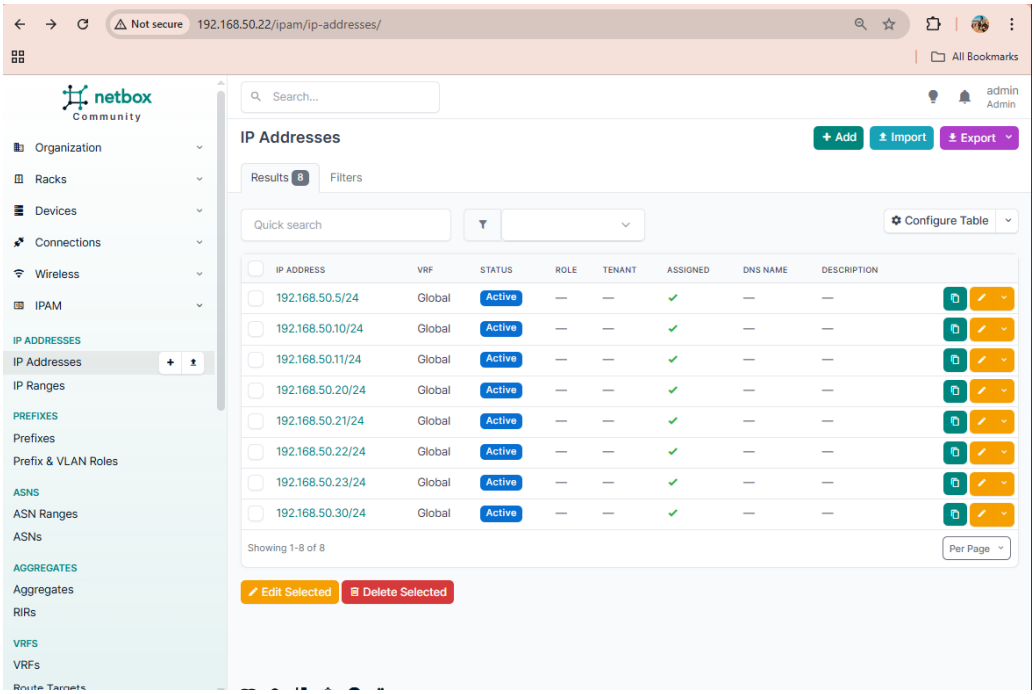

Figure B.5: IP address assignments in NetBox

IPAM records provide visibility into static addressing and network allocation.

Outcome

NetBox successfully supports asset inventory and classification. The system enables clear visibility of sites, devices, roles, IP addresses, and criticality levels, forming the basis for compliance validation and risk analysis.

Appendix C

Wazuh SIEM Alerts

Purpose

Demonstrate centralized logging, monitoring, and detection capability.

Contents

The following screenshots illustrate Wazuh's alerting and monitoring features, including agent status, security events, authentication alerts, and detailed drill-downs.

D.1 Active Agents

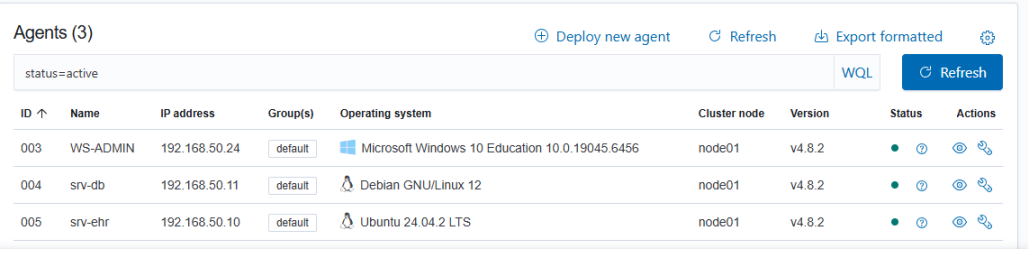

Figure C.1: Active Wazuh agents – EHR, DB, and Windows Admin endpoints

This confirms that all critical systems are registered and reporting to the Wazuh Manager.

D.2 Security Events

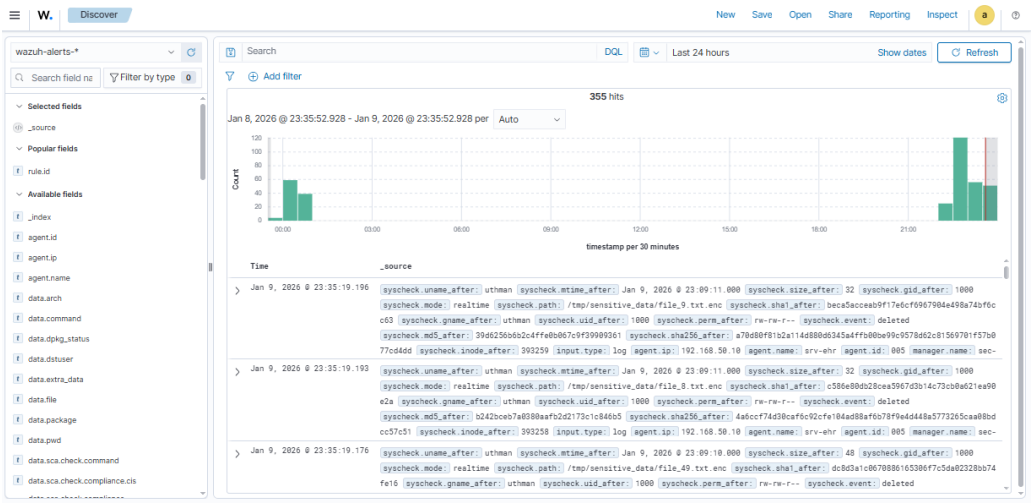

Figure C.2: Security event – ransomware-related file change detected on EHR server

Wazuh detected suspicious file modifications consistent with ransomware activity.

D.3 Alert Drill-Down

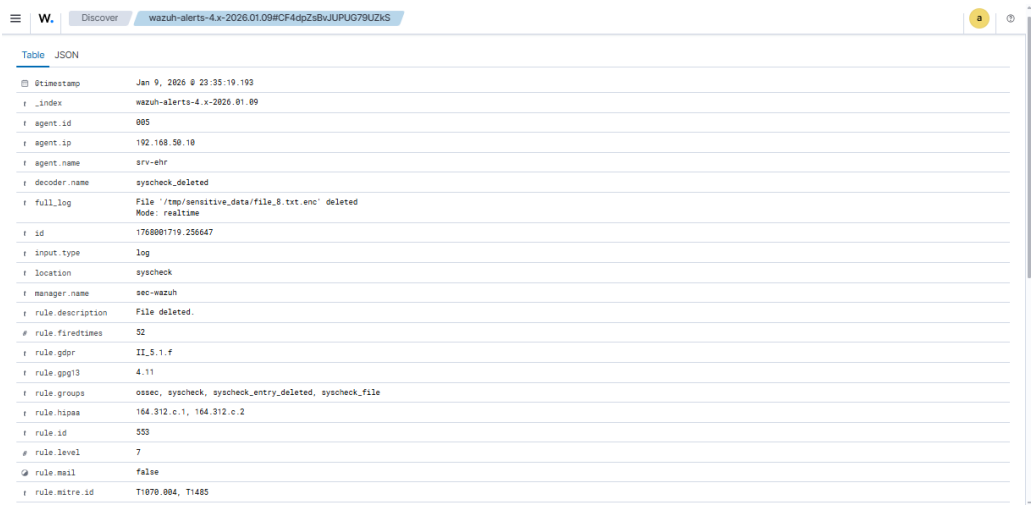

Figure C.3: Detailed drill-down of ransomware file change alert on EHR server

The drill-down provides context, affected files, and rule triggers for forensic analysis.

D.4 Authentication Alerts

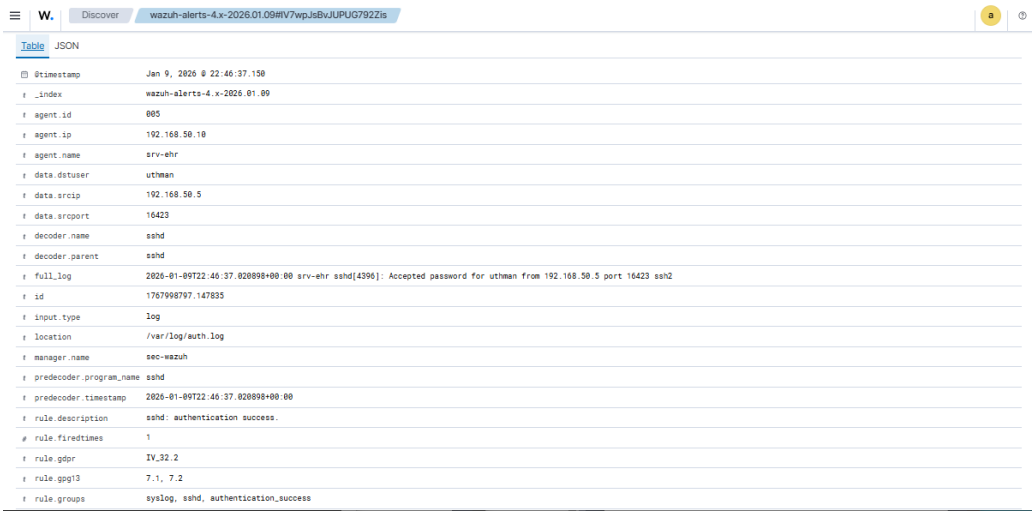

Figure C.4: Authentication alert – SSH login events on EHR server

Authentication logs highlight login attempts and potential brute-force activity.

D.5 Database Alerts

Wazuh flagged malicious file activity on the database server, demonstrating detection of integrity violations.

D.6 Agent Configuration

The figure illustrates the agent configuration in Wazuh, which was subsequently expanded to incorporate further directives enhancing monitoring and control.

D.7 pfSense Log Integration

This screenshot demonstrates integration of firewall telemetry into Wazuh, confirming that pfSense events are collected centrally for correlation and alerting.

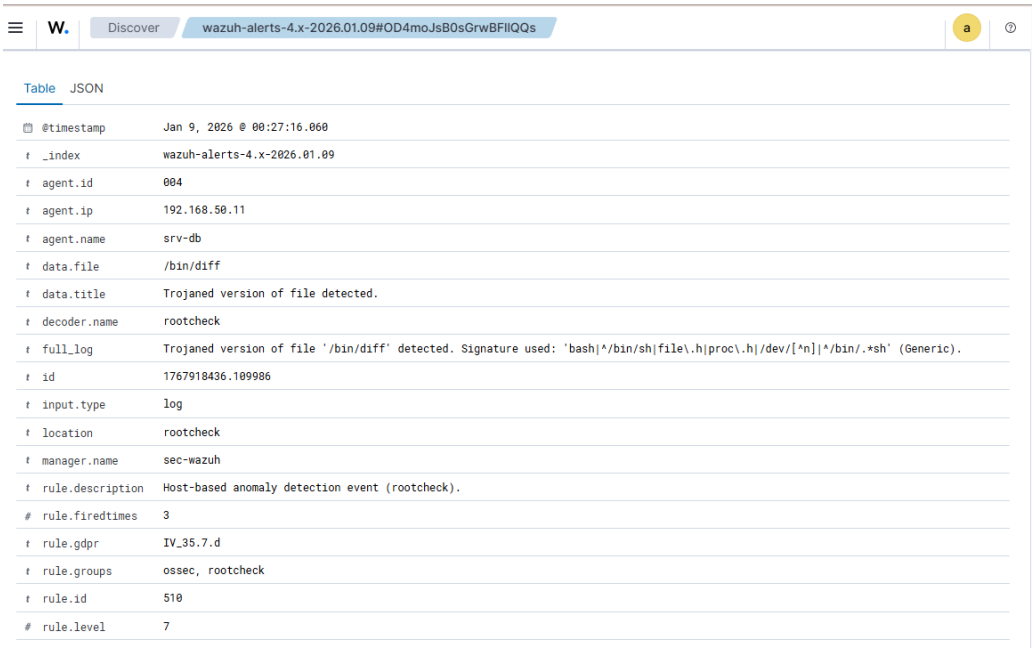

Figure C.5: Database alert – trojaned version of file detected on DB server

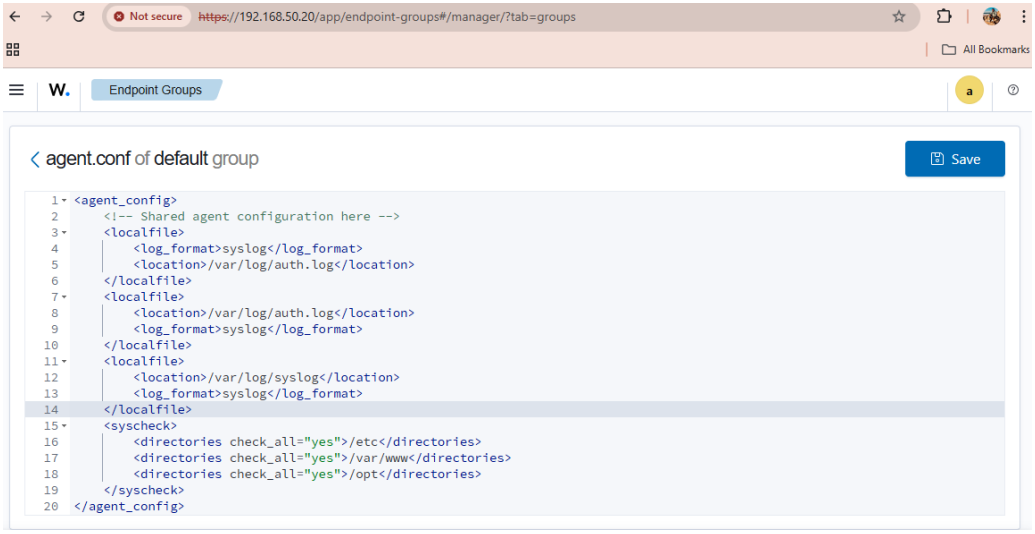

Figure C.6: Initial `agent.conf` configuration in Wazuh.

Outcome

Wazuh SIEM successfully aggregates logs and generates actionable alerts across all monitored systems. Evidence includes active agent registration, detection of ransomware

Figure C.7: Wazuh receiving and parsing logs from pfSense in `/var/log`

activity, authentication monitoring, database integrity alerts, and pfSense firewall log ingestion. This validates centralized monitoring and supports compliance, incident response, and risk management.

Appendix D

Vulnerability Assessment (OpenVAS)

Purpose

Provide evidence of vulnerability identification and risk prioritisation.

Contents

OpenVAS (Greenbone Community Edition) was used to assess project assets, focusing on deliberately vulnerable machines such as Metasploitable. This appendix presents scan configuration, results, and detailed vulnerability findings with severity, risk, and recommended solutions.

C.1 Scan Configuration

Scans were executed against Metasploitable and other Linux hosts.

C.2 Feed Status

Feed synchronization ensures the latest NVTs, SCAP, and CERT data are available.

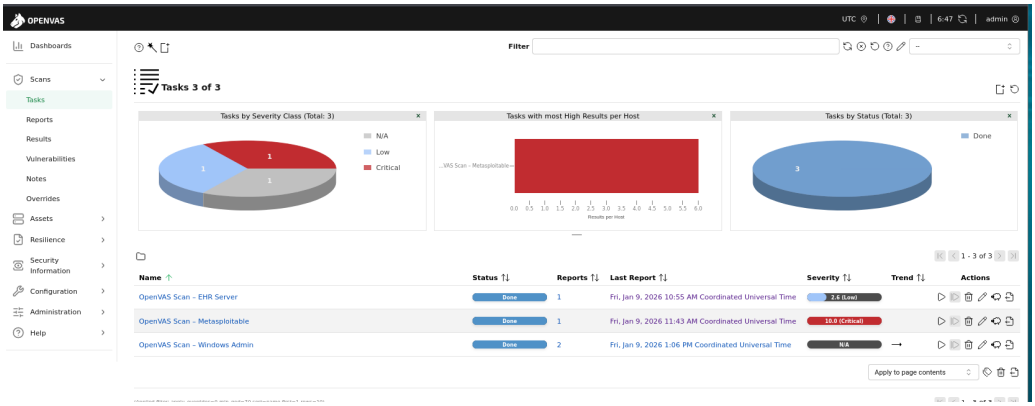

Figure D.1: OpenVAS task overview showing completed scans against multiple targets

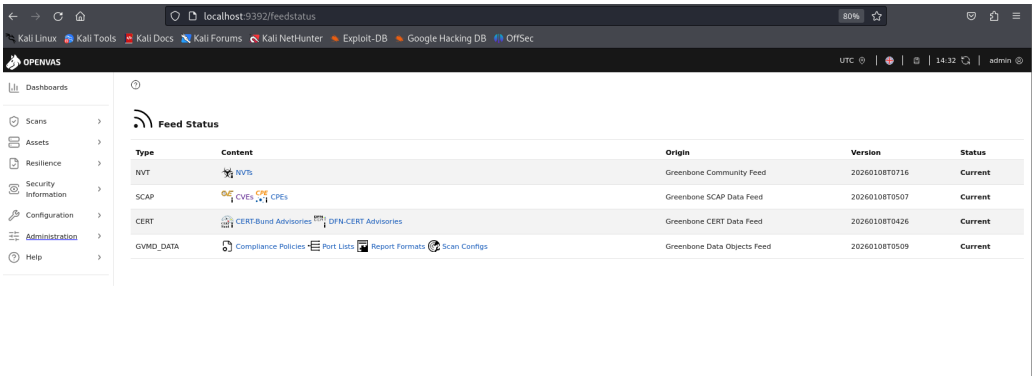

Figure D.2: OpenVAS feed status confirming vulnerability database synchronization

C.3 Target Details

The target configuration specifies IP ranges and host details for vulnerability scanning.

C.4 Key Vulnerability Findings

1. Outdated OpenSSH Service - **Severity:** High - **Risk:** Older OpenSSH versions are vulnerable to multiple exploits, including privilege escalation and information disclosure. - **Solution:** Upgrade OpenSSH to the latest stable release and disable weak ciphers.

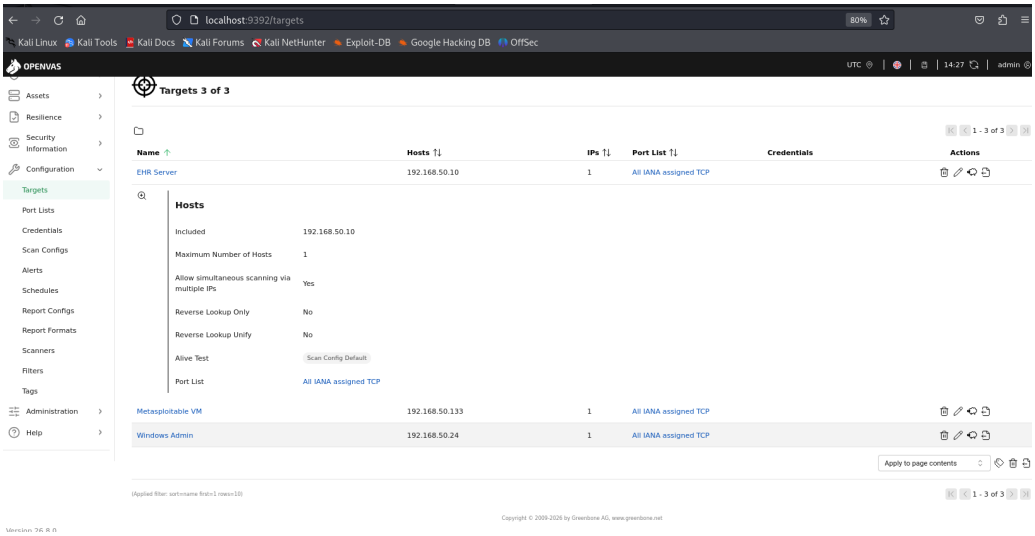

Figure D.3: Target configuration details for Metasploitable host

2. Apache HTTP Server Information Disclosure - **Severity:** Medium - **Risk:** The server banner reveals version details, aiding attackers in targeted exploitation. - **Solution:** Disable server signature and update Apache to a supported version.

3. Weak MySQL Authentication - **Severity:** Critical - **Risk:** Default or weak credentials allow attackers to gain full database access. - **Solution:** Enforce strong password policies, disable remote root login, and update MySQL.

4. Samba NetBIOS Exposure - **Severity:** High - **Risk:** Samba service exposes shares without proper authentication, enabling lateral movement. - **Solution:** Restrict access to trusted IPs, enforce authentication, and patch Samba.

5. Unpatched vsFTPd Service - **Severity:** Critical - **Risk:** Known backdoor vulnerability in vsFTPd allows remote code execution. - **Solution:** Remove vsFTPd or update to a secure FTP service.

C.5 Risk Classification

OpenVAS categorised vulnerabilities by CVSS score: - **Critical (CVSS $\geq$ 9.0):** vsFTPd backdoor, weak MySQL authentication - **High (CVSS 7.0–8.9):** Outdated OpenSSH, Samba exposure - **Medium (CVSS 4.0–6.9):** Apache information disclosure - **Low (CVSS $<$ 4.0):** Minor misconfigurations and banner exposures

C.6 Exported Report

The full PDF report (`metas_report_openvas.pdf`) contains detailed vulnerability listings, CVSS scores, and references to advisories.

Outcome

OpenVAS successfully identified critical and high-risk vulnerabilities in Metasploitable and other Linux targets. Findings demonstrate the importance of patch management, strong authentication, and service hardening. This evidence supports risk prioritisation and remediation planning in line with best practices.

Appendix E

Incident Response and DFIR-IRIS Case

Purpose

Demonstrate incident handling and forensic readiness.

Contents

Incident description, DFIR-IRIS case screenshots, and timeline reconstruction.

E.1 Incident Case Overview

E.2 Evidence Attachments

E.3 Timeline Reconstruction

The DFIR-IRIS case timeline reconstructs the incident flow: - Initial ransomware execution on EHR server - Mass file modification detected - Subsequent unauthorised data exfiltration from DB server

Investigation Report:

Customer: MeidServ HealthTech **Classification:** {'name': 'malicious-code:ransomware', 'name_expanded': 'Malicious-Code: Ransomware', 'description': "Ransomware is a type of malicious software from cryptovirology that blocks access to the victim's data or threatens to publish it until a ransom is paid.", 'id': 6, 'creation_date': '2026-01-03T13:23:44.928019'} **Date Generated:** 2026-01-10

1. Executive Summary

2. Evidence Collected

Filename	Hash (SHA256)	Added By
wazuh ransom file change ehr.png	1599c87477ba10d22d4861df4969fc85	administrator
wazuh ransom file change ehr datail.png	af56c1bf034c54c1576a8cea4cca7ac4	administrator

3. Incident Timeline

Timestamp	Event	Details
2026-01-09 23:40:00	**Wazuh Alert: Mass File Change Detected.**	"Wazuh FIM module triggered alerts for 50+ file modifications in /tmp/sensitive_data.
2026-01-09 23:50:00	**Network Isolation**	pfSense firewall rule applied to block all traffic for EHR-Server.

4. Compliance Check (GDPR/NIS2)

No immediate GDPR reporting tags found.

Report generated by IRIS-DFIR

Figure E.1: DFIR-IRIS case overview – ransomware attack on EHR server

Investigation Report:

Customer: MeidServ HealthTech **Classification:** {'name': 'information-content-security:Unauthorised-information-access', 'name_expanded': 'Information-Content-Security: Unauthorised access to information', 'description': 'Any access to unauthorized data. It may be access of data on improperly restricted server share or database exfiltered by using a SQLi.', 'id': 26, 'creation_date': '2026-01-03T13:23:45.042392'} **Date Generated:** 2026-01-10

1. Executive Summary

2. Evidence Collected

Filename	Hash (SHA256)	Added By
wazuh alert curl db file.png	f225fd62456871a82f9fbb7402e20148	administrator

3. Incident Timeline

Timestamp	Event	Details
2026-01-08 22:00:00	**[SIM-EXFIL-WAZUH] Data Exfiltration Simulation**	A simulated unauthorized transfer of sensitive database records was performed from the DB server to an external IP. Wazuh generated alerts indicating abnormal outbound traffic and suspicious file access, confirming detection of potential data theft activity.
2026-01-08 22:30:00	**Manual verification of db_dump.tar.gz presence in /tmp**	Manual verification of db_dump.tar.gz presence in /tmp.

4. Compliance Check (GDPR/NIS2)

No immediate GDPR reporting tags found.

Report generated by IRIS-DFIR

Figure E.2: DFIR-IRIS evidence attachment – data exfiltration from DB server

Appendix F

Risk Analysis and Risk Matrix (ISO/IEC 27005 Aligned)

F.1 Asset–Threat–Vulnerability Mapping

Purpose: Identify risks based on real assets (NetBox), real threats, and real vulnerabilities (OpenVAS, Wazuh).

F.2 Risk Register (ISO/IEC 27005)

Likelihood: Low / Medium / High

Impact: Low / Medium / High / Critical

F.3 Likelihood × Impact Risk Matrix

F.4 OpenVAS Findings → Risk Mapping

Purpose: Demonstrate evidence-based risk identification.

Asset (NetBox)	Threat Source	Vulnerability	Evidence Source
EHR Application Server (Ubuntu 24.04)	External attacker	Exposed web services and authentication surface	OpenVAS scan results
Database Server (Debian 12, PostgreSQL)	Insider misuse / lateral movement	Privileged access and potential misconfiguration	Risk assessment + architecture review
pfSense Firewall	External attacker	Risk of misconfiguration impacting traffic filtering	Configuration review
Windows Admin Workstation	Credential attacker	SSH / authentication abuse attempts	Wazuh SIEM SSH alerts
Vulnerable Linux / Metasploitable	External attacker	Multiple known critical vulnerabilities	OpenVAS scan results
Wazuh SIEM Manager	Targeted attack	Log integrity and availability risks	Architectural risk analysis
OpenVAS Scanner	Insider misuse	Credential exposure risk	Risk assessment
NetBox	Insider misuse	Unauthorized asset data access	Risk assessment
DFIR-IRIS	Data integrity threat	Incident evidence tampering	Risk assessment

Table F.1: Asset–Threat–Vulnerability Mapping

Risk ID	Asset	Likelihood	Impact	Risk Level	Treatment
R1	EHR Application Server	Medium	High	High	Mitigate
R2	Database Server	Low	Critical	High	Mitigate
R3	pfSense Firewall	Low	High	Medium	Mitigate
R4	Windows Admin Workstation	Medium	Medium	Medium	Mitigate
R5	Vulnerable Linux / Metasploitable	High	Medium	High	Accept
R6	Wazuh SIEM	Low	High	Medium	Mitigate
R7	OpenVAS	Low	Medium	Low	Accept
R8	NetBox	Low	Medium	Low	Accept
R9	DFIR-IRIS	Low	High	Medium	Mitigate

Table F.2: Risk Register (ISO/IEC 27005)

F.5 Risk Treatment Decisions and Justification

Mitigated Risks

- **R1 – EHR compromise:** Mitigate – Processes sensitive health data; high regulatory impact

Impact ↓ / Likelihood →	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical
Critical	High	Critical	Critical

Figure F.1: Figure F.1 – Qualitative Risk Matrix (ISO/IEC 27005)

OpenVAS Finding Category	Affected Asset	Risk ID
Critical vulnerabilities detected	Vulnerable Linux / Metasploitable	R5
High severity service exposure	EHR Application Server	R1
Medium severity configuration weaknesses	Windows Admin Workstation	R4
Informational findings	Infrastructure services	R7, R8

Table F.3: OpenVAS Findings Mapped to Risks

- **R2 – Database breach:** Mitigate – Critical GDPR and NIS2 implications
- **R3 – Firewall failure:** Mitigate – Single point of network security enforcement
- **R4 – Admin compromise:** Mitigate – Elevated privileges pose systemic risk
- **R6 – SIEM compromise:** Mitigate – Monitoring loss reduces detection capability
- **R9 – DFIR-IRIS compromise:** Mitigate – Incident integrity must be preserved

Accepted Risks (Academic Justification)

- **R5 – Vulnerable Linux:** Accept – The system is intentionally vulnerable, isolated, does not process real data, and is deployed exclusively for testing, detection validation, and educational purposes. Residual risk is controlled and documented.
- **R7 – OpenVAS:** Accept – Scanner exposure is limited, monitored, and does not affect core business processes.
- **R8 – NetBox:** Accept – Asset data is non-sensitive and access-restricted.

Appendix G

GDPR and NIS2 Compliance Evidence

Purpose

This appendix provides documentary and technical evidence supporting the GDPR and NIS2 compliance claims made throughout this report. It consolidates extracts from the risk management and incident response processes, together with operational logging and incident documentation, to demonstrate accountability, traceability, and regulatory preparedness.

The evidence presented herein supports the compliance mappings discussed in Chapter 8 and is derived directly from the implemented controls and procedures described in Chapters 4 and 7.

G.1 Control-to-Article Mapping Evidence

This section demonstrates how implemented security measures align with specific GDPR and NIS2 legal obligations.

GDPR Article	Requirement	Implemented Measure	Evidence Source
Art. 5(1)(f)	Integrity and confidentiality	Network segmentation, access control, monitoring	Chapters 3, 5; Wazuh logs
Art. 5(2)	Accountability	Documented risk analysis and IR processes	Chapters 4 and 7
Art. 32	Security of processing	IDS, SIEM, logging, access controls	Chapters 5 and 6
Art. 33	Breach notification	Incident detection and documentation	Chapter 7; DFIR-IRIS
Art. 34	Communication to data subjects	Incident assessment procedures	Chapter 7

Table G.1: GDPR Compliance Evidence

NIS2 Article	Requirement	Implemented Measure	Evidence Source
Art. 21	Risk management measures	Risk analysis and mitigation	Chapter 4; Appendix F
Art. 21(2)(b)	Incident handling	Incident response lifecycle	Chapter 7
Art. 21(2)(e)	Monitoring and detection	IDS and SIEM integration	Chapters 5 and 6
Art. 23	Incident reporting	Incident documentation and timelines	Chapter 7; DFIR-IRIS

Table G.2: NIS2 Compliance Evidence

G.2 Incident Response Policy (Extract)

MediServ HealthTech Lda maintains a structured incident response capability to ensure the timely detection, analysis, containment, and resolution of cybersecurity incidents. Incident handling follows a lifecycle aligned with ISO/IEC 27035 and NIST SP 800-61, comprising preparation, detection and analysis, containment, eradication, recovery, and post-incident review.

Incidents are detected through centralized monitoring mechanisms, including intrusion detection systems and SIEM correlation. Confirmed incidents are documented using a case management platform, with relevant logs and evidence preserved to support forensic

analysis and regulatory accountability.

Incidents involving personal data are assessed to determine notification obligations under GDPR Articles 33 and 34. Post-incident reviews are conducted to identify lessons learned and improvement opportunities.

G.3 Risk Analysis Summary Evidence

This section provides a compliance-oriented extract of the risk analysis, highlighting high-risk scenarios and treatment decisions relevant to GDPR and NIS2 obligations.

Risk ID	Asset	Risk Description	Risk Level	Treatment
R1	EHR Application Server	Unauthorised access to health data	High	Mitigate
R2	Database Server	Data breach affecting patient records	High	Mitigate
R3	pfSense Firewall	Failure to detect or block attacks	High	Mitigate
R4	Windows Admin Workstation	Credential compromise	High	Mitigate
R5	Vulnerable Linux System	Remote exploitation of known vulnerabilities	High	Accept

Table G.3: High-Risk Register Extract

Accepted risks relate exclusively to intentionally vulnerable and isolated systems deployed for testing and validation purposes. The full risk register and treatment rationale are provided in Appendix F.

G.4 Logging and Monitoring Evidence

Evidence of security monitoring and event detection capabilities includes:

- Wazuh SIEM dashboard screenshots;
- Example SSH authentication alert;

- Timestamped log entries showing affected assets;
- The evidence are shown in Appendix C.

These artefacts support compliance with GDPR Article 32 and NIS2 Article 21 by demonstrating continuous monitoring and traceability.

G.5 Incident Documentation Evidence

This section demonstrates the organisation's capability to document and manage security incidents.

Included evidence:

- DFIR-IRIS incident case overview
- Timeline reconstruction showing detection, analysis, and response
- Attached evidence (alerts, logs, screenshots)
- The evidence are show in Appendix E

This documentation supports breach notification and reporting obligations under GDPR Articles 33–34 and NIS2 Article 23.

G.6 Summary

This appendix demonstrates that MediServ HealthTech Lda has implemented and documented appropriate technical and organisational measures to support compliance with GDPR and NIS2. By combining structured risk analysis, centralized monitoring, and documented incident response procedures, the organisation can demonstrate accountability and preparedness during audits or regulatory inspections.

Appendix H

Auditing and Security Testing

Purpose

This appendix provides evidence of auditing and security testing activities conducted to validate the effectiveness of technical and organisational security controls within the MediServ HealthTech Lda infrastructure. The activities support internal assurance, external audit readiness, and compliance with GDPR Article 32 and NIS2 Article 21.

Auditing was performed from two perspectives: - Internal audit, focusing on systems within the trusted network - External audit, simulating third-party assessment through controlled VPN-based access

H.1 Audit Scope Definition

Internal Audit: Evaluated the security posture of systems inside the network boundary, including the EHR Application Server, Database Server, Windows Administrative Workstation, Wazuh SIEM Manager, DFIR-IRIS platform, and pfSense/OPNsense gateway. The deliberately vulnerable Linux system was included to validate detection and incident handling workflows.

External Audit: Conducted via WireGuard VPN (`192.168.11.0/24`), simulating a

third-party assessment. Objectives included identifying exposed services, assessing segmentation, evaluating cryptographic protections, and validating compliance with GDPR/-NIS2 principles. Two audits were performed at different project stages to reflect remediation progress.

H.2 Audit Tools and Techniques

Tools: Kali Linux, OpenVAS/Greenbone, Nmap, OpenSSL, Netcat, Wazuh SIEM. Approach: Automated scanning combined with manual validation, protocol-level verification, and risk-oriented interpretation aligned with ISO/IEC 27005.

H.3 Internal Audit Summary

Checklist Extract

Control Area	**Audit Activity**	**Result**
Asset management	Verification of NetBox inventory	Compliant
Vulnerability management	Internal OpenVAS scans	Issues identified
Access control	Administrative privilege review	Compliant
Network security	Firewall rules and segmentation	Compliant
Monitoring	SIEM alert generation and correlation	Compliant
Incident response	DFIR-IRIS case handling	Compliant

Table H.1: Internal Audit Checklist (Extract)

Findings Summary

Accepted risks are documented in the risk register (Appendix F).

Finding	Affected Asset	Severity	Treatment
Outdated services	Vulnerable Linux system	High	Accepted
Weak SSH configuration	Test system	Medium	Accepted
Missing hardening	Non-production services	Medium	Accepted

Table H.2: Internal Audit Findings Summary

H.4 External Audit Evidence

Audit 1 – Flat Network and Segmentation (Jan 10, 2026) Findings: Flat VPN topology, exposure of management services, self-signed certificates, and information disclosure via banners/TLS metadata. Compliance Impact: NIS2 segmentation and cryptographic safeguards; GDPR confidentiality.

Audit 2 – Gateway Hardening and Information Disclosure Platform: OPNsense Security Gateway. Findings: WPAD exposure, timestamp responses, HTTP banner leakage, continued use of self-signed certificates. Compliance Impact: NIS2 discovery and information disclosure; GDPR secure administrative sessions.

H.5 External Audit Risk Summary

Risk ID	Finding	Severity	Regulatory Impact
HIGH-01	Flat VPN topology	High	NIS2 (Segmentation)
HIGH-02	Self-signed certificates	High	GDPR (Confidentiality)
MED-01	WPAD disclosure	Medium	NIS2 / GDPR
MED-02	Service banner leakage	Medium	NIS2
LOW-01	Timestamp disclosure	Low	NIS2

Table H.3: External Audit Risk Summary

H.6 Remediation and Improvement Actions

Finding	**Action**
Flat VPN topology	Implement peer isolation via WireGuard ACLs
Self-signed certificates	Deploy internal PKI or trusted CA
WPAD exposure	Disable WPAD discovery
Banner leakage	Suppress service headers
Timestamp disclosure	Disable TCP/ICMP timestamps

Table H.4: Remediation and Improvement Actions

H.7 Summary

This appendix demonstrates that MediServ HealthTech Lda conducted structured internal and external auditing activities aligned with regulatory requirements. The external audits highlighted realistic weaknesses, while the remediation roadmap supports continuous improvement and accountability.

Appendix I

Forensic Artefacts

I.1 Disk Image Acquisition

Target: SRV-EHR VM

Acquisition tool: `dd` (bit-for-bit copy)

Storage location: */mnt/forensics/sda_image.dd*

Integrity verification: SHA256 / SHA1 hashes

Commands executed

```
sudo dd if=/dev/sda of=/mnt/forensics/sda_image.dd bs=4M status=
   progress
sha256sum /mnt/forensics/sda_image.dd
```

Mount for analysis

```
sudo mkdir /mnt/disk_image
sudo mount -o loop,ro /mnt/forensics/sda_image.dd /mnt/disk_image
ls /mnt/disk_image/var/log
sudo umount /mnt/disk_image
```

—

I.2 Process Memory Dump

Target: Single running process `<process_name>` on SRV-EHR

Acquisition tool: `gcore`

Storage location: `/mnt/forensics/<process_name>_mem.raw`

Integrity verification: SHA256 / SHA1 hashes

Commands executed

```
sudo gcore -o /mnt/forensics/<process_name>_mem.raw $(pidof <
   process_name>)
sha256sum /mnt/forensics/<process_name>_mem.raw
```

—

I.3 Notes

This appendix demonstrates proper forensic handling despite storage limitations.

Optional future work includes:

- Full VM memory capture
- Network traffic capture
- Multi-VM disk imaging

Investigation Report:

Customer: MeidServ HealthTech **Classification:** {'name': 'information-content-security:Unauthorised-information-access', 'name_expanded': 'Information-Content-Security: Unauthorised access to information', 'description': 'Any access to unauthorized data. It may be access of data on improperly restricted server share or database exfiltered by using a SQLi.', 'id': 26, 'creation_date': '2026-01-03T13:23:45.042392'} **Date Generated:** 2026-01-11

1. Executive Summary

2. Evidence Collected

Filename	Hash (SHA256)	Added By
sda_image.dd	64778b0a7e7695e147336b453f698149e3412be2d70fb07872737ae2a7b05bd7	administrator

3. Incident Timeline

Timestamp	Event	Details
2026-01-10 18:00:00	**Initial Detection**	Wazuh alerted on multiple failed SSH attempts followed by a successful login from an unknown IP.
2026-01-10 18:15:00	**System Isolation**	Host isolated via pfSense to preserve disk state.
2026-01-10 18:30:00	**Acquisition Start**	Disk image acquisition initiated using dd over the network to a forensic workstation.
2026-01-10 19:45:00	**Verification**	SHA256 hash generated for sda_image.dd to ensure integrity.
2026-01-10 20:30:00	**Artifact Found**	Identified hidden directory .hidden_exfil in /var/www/html/ containing database dumps.

4. Compliance Check (GDPR/NIS2)

No immediate GDPR reporting tags found.

Report generated by IRIS-DFIR

Figure I.1: DFIR-IRIS evidence entry – Unauthorized access on SRV-EHR

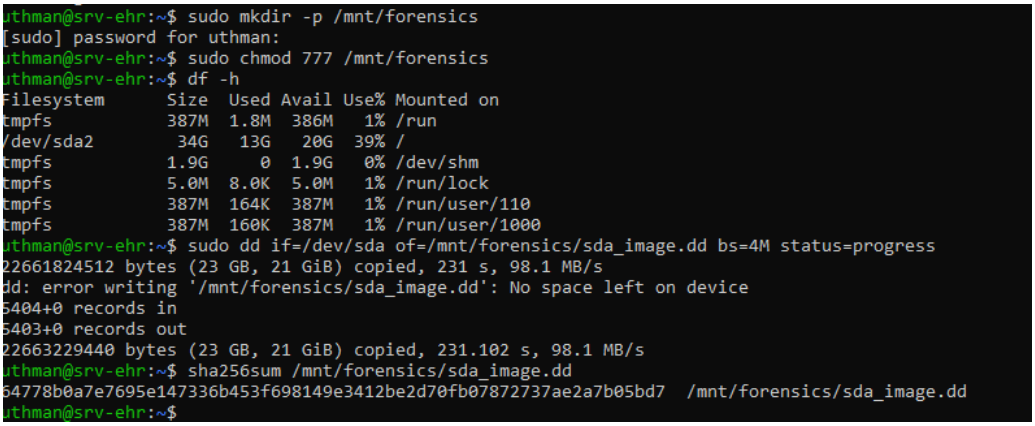

Figure I.2: Terminal capture showing disk image acquisition commands and output

Investigation Report:

Customer: MeidServ HealthTech **Classification:** {'name': 'other:other', 'name_expanded': 'Other: other', 'description': 'All incidents that do not fit in one of the given categories should be put into this class. If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.', 'id': 36, 'creation_date': '2026-01-03T13:23:45.095863'} **Date Generated:** 2026-01-11

1. Executive Summary

2. Evidence Collected

Filename	Hash (SHA256)	Added By
srv_ehr_pid_2296.raw	8757af8132eb09a033ba6ede117978a7edf41126dd3a2fc8d24d2cd4cea6ec26	administrator

3. Incident Timeline

Timestamp	Event	Details
2026-01-10 18:40:00	**Process Triage**	Identified suspicious process /tmp/system_update running with PID 2296.
2026-01-11 18:45:00	**Memory Capture**	Executed gcore to dump process memory before the process could be killed or terminated.
2026-01-11 19:10:00	**String Analysis**	Found plain-text C2 (Command & Control) IP address 91.23.45.67 inside the memory strings.
2026-01-11 19:30:00	**IOC Extraction**	Extracted encoded base64 script from memory used for data exfiltration.

4. Compliance Check (GDPR/NIS2)

No immediate GDPR reporting tags found.

Report generated by IRIS-DFIR

Figure I.3: DFIR-IRIS evidence entry – Suspicious process memory dump