



INSTITUTO POLITÉCNICO  
DE VIANA DO CASTELO

---

# ANALYSIS OF IMPLEMENTATION OF A SECURITY INFORMATION AND EVENTS MANAGEMENT (SIEM) SYSTEM IN PUBLIC BUSINESS ENTITIES (PBE) HOSPITALS

Emanuel de Araújo Gonçalves

---

---

Escola Superior de Tecnologia e Gestão

---



Instituto Politécnico  
de Viana do Castelo

Analysis of Implementation of a  
Security Information and Event Management  
(SIEM) System in Public Business Entities (PBE)  
Hospitals

Autor(a)

Emanuel de Araújo Gonçalves

Trabalho efetuado sob a supervisão de

Professor Vítor Júlio da Silva e Sá

Professor Pedro Miguel Simões Pinto Carneiro

Mestrado em Cibersegurança

14 de Dezembro de 2023



Mestrado em  
Cibersegurança  
Master in  
Cybersecurity

Analysis of Implementation of a Security  
Information and Event Management (SIEM)  
System in Public Business Entities (PBE)  
Hospitals

a master's thesis authored by

Emanuel de Araújo Gonçalves

and supervised by

Vítor Júlio da Silva e Sá

Assistant Professor, IPVC

Pedro Miguel Simões Pinto Carneiro

Assistant Professor, IPVC

This thesis was submitted in partial fulfillment of the requirements for the  
Masters degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo



14 December, 2023



## Abstract

In a general context, IT systems are vulnerable to attacks due to increasing digitalization, especially in the health sector. Therefore, the need to protect these systems is extremely urgent. Organizations are increasingly turning to Security Information and Event Management (SIEM) systems to protect the data they manage through a strategy of centralized analysis of multiple security events originating from different security components.

The purpose of this work is to analyze and implement a SIEM system in a hospital environment. To achieve this objective, an exploration of the current state of SIEM systems and their main functions was conducted. An analysis of security needs and specific requirements in the hospital context was also performed. Based on this analysis, an architectural model for implementing the SIEM system in the hospital is proposed. The proposed model was implemented and tested in a laboratory environment, revealing that the SIEM system is capable of identifying and reporting relevant security incidents in a hospital context [27]. Some limitations in the tested system were also identified, along with suggestions for future improvements.

Taking into account the recent cyberattacks that have targeted public hospitals in Portugal, hospitals must be prepared to face these threats. Implementing a SIEM system can play a key role in mitigating these attacks and safeguarding sensitive patient and employee information.

**Keywords:** cyber security, siem, hospital, threats, resilience

## Resumo

Num contexto geral, os sistemas informáticos encontram-se vulneráveis a ataques, devido à crescente digitalização, sobretudo no setor da saúde. Por isso, a necessidade de proteger esses sistemas é extremamente urgente. As organizações estão a recorrer cada vez mais a sistemas SIEM (Gestão de Informação e Eventos de Segurança) para proteger os dados que gerem, através de uma estratégia de análise centralizada de múltiplos eventos de segurança originados por diversos componentes de segurança.

O propósito deste trabalho é analisar e implementar um sistema SIEM num ambiente hospitalar. Para atingir este objetivo, foi realizada uma exploração do estado atual dos sistemas SIEM e das suas principais funções. Foi também conduzida uma análise das necessidades de segurança e dos requisitos específicos no contexto hospitalar. Com base nesta análise, é proposto um modelo arquitetural para a implementação do sistema SIEM no hospital. O modelo proposto foi implementado e testado em ambiente laboratorial, revelando que o sistema SIEM é capaz de identificar e reportar incidentes de segurança relevantes num contexto hospitalar. Foram também identificadas algumas limitações no sistema testado, juntamente com sugestões para melhorias futuras.

Tendo em conta os recentes ataques cibernéticos que têm visado hospitais públicos em Portugal, torna-se crucial que os hospitais estejam preparados para enfrentar estas ameaças. A implementação de um sistema SIEM pode desempenhar um papel fundamental na mitigação destes ataques e na salvaguarda de informações sensíveis de pacientes e colaboradores.

**Palavras-chave:** cibersegurança, siem, hospital, ameaças, resiliência

# Acknowledgements

I want to express my sincere gratitude to my supervisors, Prof. Vítor Sá and Prof. Pedro Carneiro, for all the support they provided during my study and research. Their commitment to assisting me has been invaluable. I am truly grateful for the guidance, suggestions, constructive criticism, and teachings they offered, which have helped me clarify my doubts and grow personally and academically.

I would like to express my appreciation to all hospital administrators, Chief Information Security Officer (CISO), system administrators, and other experts who contributed to this study. Your openness to share your knowledge and insight as well as your readiness to answer the provided questionnaire were both very beneficial. Your input has enriched my investigation and enhanced my understanding of the topic. Many thanks to Fabio for technical support and troubleshooting in English.

Finally, I would like to thank my family for their endless support and love. In particular, I would like to thank my wife, Cláudia, for her trust and patience during my graduate studies. She took time for herself and his family for me to focus on this important phase of my educational journey. I am very grateful to my parents, Manuel and Gracinda, and my younger brother, Victor, for their unwavering faith in me over the years.

# Contents

<b>List of Figures</b>	<b>vii</b>
<b>List of Tables</b>	<b>x</b>
<b>List of Listings</b>	<b>xi</b>
<b>List of Abbreviations</b>	<b>xii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Context . . . . .	1
1.2 Problem Statement and Motivation . . . . .	2
1.3 Objectives . . . . .	3
1.4 Contributions . . . . .	4
1.5 Organization . . . . .	5
<b>2 Related Work</b>	<b>7</b>
2.1 Cybersecurity, Threats, Risks, and Resilience . . . . .	7
2.1.1 Confidentiality, Integrity, and Availability . . . . .	11
2.1.2 Data Protection and Privacy . . . . .	11
2.1.3 Threats . . . . .	12
2.1.4 Risks . . . . .	12
2.1.5 Resilience . . . . .	17
2.2 Security Information and Event Management (SIEM) Systems . . . . .	19
2.2.1 Definition and Components (SIM and SEM) . . . . .	20
2.2.2 Objectives, Advantages, and Disadvantages . . . . .	20

2.2.3	Architecture and Components . . . . .	22
2.2.4	Workflow Processes . . . . .	24
2.2.5	Examples of Vendors and Products . . . . .	25
2.3	EDR vs. SIEM . . . . .	31
2.4	Security Operations Center (SOC) . . . . .	32
2.4.1	Definition and Functions . . . . .	32
2.4.2	Open-source Examples of SOC tools . . . . .	34
<b>3</b>	<b>Organization of the Healthcare Sector in Portugal</b>	<b>37</b>
3.1	History of the Healthcare System . . . . .	37
3.2	Structure and Organization of the SNS . . . . .	40
3.3	Role of PBE Healthcare Units . . . . .	44
<b>4</b>	<b>Healthcare Security</b>	<b>49</b>
4.1	Overview of Healthcare Security Challenges . . . . .	49
4.2	Threats and Risks in Healthcare environments . . . . .	51
4.3	Critical Services and Systems in Healthcare . . . . .	59
4.4	Cybersecurity Best Practices in Hospitals . . . . .	61
4.5	Cybersecurity Skills Trend . . . . .	63
<b>5</b>	<b>Research</b>	<b>65</b>
5.1	Research Methodology . . . . .	65
5.1.1	Research Approach and Design . . . . .	65
5.1.2	Data Collection Methods . . . . .	67
5.1.3	Sampling Strategy and Participants . . . . .	70
5.1.4	Data Analysis Techniques . . . . .	71
5.2	Research Findings and Analysis . . . . .	72
5.2.1	Overview of the Research Results . . . . .	72
5.2.2	Analysis of the Survey Responses . . . . .	73
5.2.3	Discussion of the Findings concerning the Research Questions and Objectives . . . . .	77
5.3	Managers Interviews . . . . .	80



5.3.1	Implications and Recommendations for Healthcare Organizations . .	84
<b>6</b>	<b>Proposal for SIEM Implementation in Healthcare</b>	<b>87</b>
6.1	Overview of the Proposed Solution . . . . .	87
6.2	Rationale for Selecting Specific Open-source Tools . . . . .	88
6.3	Architecture and Design Considerations . . . . .	95
6.4	Timeline and Implementation Plan . . . . .	97
6.5	Implementation . . . . .	98
6.6	Expected Benefits and Outcomes . . . . .	109
<b>7</b>	<b>Conclusion and Future Work</b>	<b>117</b>
7.1	Limitations of the Study . . . . .	119
7.2	Future Work . . . . .	119
	<b>References</b>	<b>121</b>
	<b>Appendices</b>	<b>A1</b>
<b>A</b>	<b>Appendices</b>	<b>A2</b>
	<b>Appendices</b>	<b>A2</b>
A	Survey . . . . .	A2
B	Collaboration Request Email . . . . .	A6

# List of Figures

2.1	Definition of each impact level for all areas of consequence when the risks materialize. Source: [11]	14
2.2	Risk Matrix. Source: [11]	15
2.3	Risk matrix for essential services. Source: [11]	16
2.4	Smart Hospitals Objectives. Source: [22]	19
2.5	Architecture of a SIEM with representation of its components. Source: [50]	23
2.6	SIEM Classification (2022) by GARTNER. Source: [25]	26
2.7	Endpoint detection and response - features. Source: the author.	32
2.8	Diagram of the different components of a Security Operations Center (SOC). Source: The author.	34
3.1	Service organization chart.	42
3.2	Health regions of mainland Portugal. Source: The author.	44
3.3	Organization chart of the internal organization of a Public Business Entity (PBE) hospital unit. Source: The author.	45
3.4	Location of PBE units in mainland Portugal. Source: The author.	48
4.1	Map of observed incidents. Source: [21, p.8]	52
4.2	Nature of the incidents. Source: [19]	55
4.3	Example of WannaCry warning window asking for ransom. Source: [9].	57
4.4	Example of Ryuk diagram attack. Source: [33]	58
4.5	Business Continuity Planning Life Cycle. Source: The author	61
5.1	Survey header. Source: The author	69
5.2	Percentage of survey participants chart. Source: The author	73

5.3	Number of hospital units by type that responded to the survey. Source: The author. . . . .	74
5.4	IT Director chart answer classification. Source: The author. . . . .	75
5.5	IT Director/CISO chart answer classification. Source: The author. . . . .	76
5.6	System administrator chart answer classification. Source: The author. . . . .	77
6.1	Wazuh security vulnerabilities. Source: The author. . . . .	90
6.2	Flow diagram between the different components of the Wazuh. Source: [57]	92
6.3	Operating systems compatible with Wazuh SIEM. Source: The author. . . . .	93
6.4	Modular architecture of a W.agent. Source:[58] . . . . .	93
6.5	Wazuh deployment architecture. Source: [60]. . . . .	95
6.6	Architecture used in laboratory for testing. Source: The author. . . . .	96
6.7	Diagram showing the execution of SIEM implementation tasks in the labo- ratory. Source: The author. . . . .	97
6.8	Diagram showing the execution of SIEM implementation tasks in the labo- ratory. Source: The author. . . . .	100
6.9	Wazuh installation. Source: The author. . . . .	101
6.10	Routing add forward ports. Source: The author. . . . .	101
6.11	Wazuh login screen. Source: The author. . . . .	102
6.12	Dashboard for deploying a new agent to Ubuntu. Source: [59] . . . . .	104
6.13	List of agents and properties of endpoints. Source: The author. . . . .	105
6.14	Listing where the agent's status change actions are visible. Source: The author. . . . .	106
6.15	Status of Suricata. Source: The author . . . . .	107
6.16	Flow diagram of VirusTotal Malware Detection. Source:[56] . . . . .	108
6.17	Wrong access via login session in Windows 7. Source: The author . . . . .	110
6.18	Attempted Secure Shell (SSH) access to VM with Internet protocol (IP) 192.168.112.5. Source: The author . . . . .	111
6.19	SSH access related incident listing. Source: The author . . . . .	111
6.20	Nmap's execution. Source: The author . . . . .	112
6.21	Malware download simulation. Source: The author. . . . .	113

6.22	Listing malware detection. Source: The author. . . . .	113
6.23	Vulnerability exploiting. Source: The author. . . . .	114
6.24	Remote screen capture. Source: The author. . . . .	115
6.25	Successful remote login Detected. Source: The author. . . . .	115
A.1	Email sent to ACeS Cabreira/Gerês. Source: The author . . . . .	A6
A.2	Email sent to SPMS. Source: The author . . . . .	A6
A.3	Email sent to Executive Serviço Nacional de Saúde (SNS). Source: The author . . . . .	A7

# List of Tables

2.1	Risk treatment action table . . . . .	17
2.2	Main features of Endpoint Detection & Response (EDR) and SIEM . . . . .	31
4.1	Top 5 countries with the most number of incidents . . . . .	53
4.2	Top 5 countries with the least number of incidents . . . . .	53
4.3	Number of incidents related to threats in period 2021/Q12023 . . . . .	54
6.1	Alienvault OSSIM - SIEM considerations . . . . .	88
6.2	Prelude OSS - SIEM considerations . . . . .	89
6.3	Wazuh SIEM - considerations . . . . .	89
6.4	Table with the Virtual Machine (VM) configurations used in the laboratory. Source: The author. . . . .	99

# List of Listings

6.1	Script with commands to create w-agent on Windows XP . . . . .	102
6.2	Script with commands to create w-agent on Windows 7+ . . . . .	102
6.3	Script with commands to create w-agent on Ubuntu . . . . .	103
6.4	Wazuh settings with JSON file definition to download Suricata . . . . .	107
6.5	Wazuh settings with VirusTotal API KEY . . . . .	108
6.6	Wazuh configuration to control the selected folder . . . . .	108
6.7	Run the nmap command . . . . .	112

# List of Abbreviations

**ACES** Agrupamento de Centros de Saúde

**AI** Artificial Intelligence

**APT** Advanced Persistent Threats

**BCP** Business Continuity Plan

**CCSP** Certified Cloud Security Professional

**CEH** Certified Ethical Hacker

**CIA** Confidentiality, integrity and availability

**CIRAS** Cyber Security Incident Reporting and Analysis System

**CIS** Cyber Security Center

**CISM** Certified Information Security Manager

**CISO** Chief Information Security Officer

**CISSP** Certified Information Systems Security Professional

**CNCS** Centro Nacional de Cibersegurança

**CNPD** Comissão Nacional de Proteção de Dados

**CompTIA** Computing Technology Industry Association

**CSIRT** Computer Security Incident Response Team

**DDOS** Distributed Denial-of-Service

**DL** Decreto-Lei

**DOS** Denial-of-Service

**DRP** Disaster Recovery Plan

**EDR** Endpoint Detection & Response

**EHR** Electronic Health Records

**ENISA** European Union Agency for Cybersecurity

**EPE** Entidade Pública Empresarial

**EU** European Union

**FDA** U.S. Food and Drug Administration

**GDPR** General Data Protection Regulation

**HIPAA** Health Insurance Portability and Accountability Act

**IDPS** Intrusion Detection and Prevention Systems

**IDS** Intrusion Detection Systems

**IOMT** Internet Of Medical Things

**IOT** Internet Of Things

**IP** Internet protocol

**IPO** Instituto Português de Oncologia

**IPS** Intrusion Prevention Systems

**IS** Information Systems

**IT** Information Technology

**ITIL** Information Technology Infrastructure Library



**KVM** Kernel-based Virtual Machine

**MCyber** Master in Cybersecurity

**MIOT** Medical Internet of Things

**MSSP** Managed Security Service Provider

**NHS** National Health Service

**NIST** National Institute of Standards and Technology

**NNICC** National Network of Integrated Continuous Care

**NNPC** National Network of Palliative Care

**PBE** Public Business Entities

**PBE** Public Business Entity

**PIO** Portuguese Institute of Oncology

**SAAS** Software-as-a-Service

**SEM** Security Event Management

**SIEM** Security Information and Event Management

**SIM** Security Information Management

**SMB** CServer Message Block

**SNS** Serviço Nacional de Saúde

**SOC** Security Operations Center

**SPMS** Serviços Partilhados do Ministério da Saúde

**SSH** Secure Shell

**SSMH** Shared Services of the Ministry of Health

**ULS** Unidade Local de Saúde

**VM** Virtual Machine

**VMM** Virtual Machine Manager

**VPN** Virtual Private Network

**WHO** World Health Organization

**WN** Wireless Network

**XDR** Extended Detection and Response

# Chapter 1

## Introduction

In the face of growing cyber risks, implementing a Security Information and Event Management (SIEM) system in healthcare settings is critical. This master's thesis investigates the essential issue of protecting patient data and hospital systems, which is being driven by the growing incidence of cyber-attacks on healthcare institutions. The primary purpose is to investigate and implement a SIEM in a hospital setting to enhance its cybersecurity posture. This master's thesis contributes to the field by providing a comprehensive guide to SIEM deployment in the healthcare sector, as well as insights for similar organizations.

This master's thesis is divided into seven distinct chapters. The first parts go deeper into the works examined, providing an in-depth analysis of the organization of the Portuguese health sector. The following chapters focus on health security and related research. In the concluding part, a plan for establishing a SIEM in Healthcare is presented, providing an easy and cost-effective solution to increasing cybersecurity in the healthcare industry.

### 1.1 Context

Recently, cyber security has acquired particular importance, mainly due to the frequent increase in attacks in the health sector. This is partly due to the value of health data. Incidents such as data breaches, ransomware attacks, and disclosure of information that compromises patient privacy and the integrity of medical records have been recurrent. The protection of personal and sensitive data of patients and employees, the security of

medical, registration, and diagnostic systems, as well as the continuity of health services, have become critical and urgent issues. Faced with these challenges, the use of advanced tools to strengthen and improve the cyber security of systems has become essential. In this context, the adoption of SIEM systems represents a proactive approach to quickly detect and respond to threats in real time. This study focuses on one of these tools: SIEM and aims to conduct a detailed analysis of existing SIEM systems. These systems integrate diverse data sources such as security logs and alerts, providing relevant information to the cyber security team to proactively detect threats and respond effectively and efficiently to incidents.

Another of the concerns of this work is to evaluate the current state of hospitals concerning cyber security and the use of SIEM systems. In this way, it is intended to understand the level of adoption of SIEM in health institutions and the main reasons that drive its implementation. This research will employ a qualitative approach over interviews and research conducted with hospital directors, Information Technology (IT) administrators, IT security specialists, and other healthcare professionals in different hospitals to understand existing cybersecurity practices and the challenges faced. A comparative analysis of SIEM systems available on the market will be made, examining their functionalities, scalability, and applicability in the health sector. Based on the findings, a customized SIEM system will be developed that meets the specific needs of healthcare institutions, valuing the accessibility and adaptability provided by open-source principles.

The goal is to develop and implement a custom SIEM system based on open-source principles and easy implementation. The ultimate goal of this work is to help hospitals improve their cybersecurity practices, strengthen their security posture, and protect sensitive patient information. With an approach focused on deploying effective and compliant SIEM systems, it aims to provide valuable insights for healthcare organizations seeking a secure and resilient environment against emerging cyber threats.

## 1.2 Problem Statement and Motivation

Medical care organizations or institutions, in particular hospitals, are subject to various threats and have been the target of computer attacks. In this context, it is imperative to

provide and strengthen cyber security in hospitals, hospital centers, local health units, and oncology institutes, especially those of the (Public Business Entity (PBE) type, with more means to address this problem. The health sector is in an intense process of digitalization, however, cyber security does not always follow this evolution.

On the other hand, cyber security teams are usually small or non-existent, at least full-time, with the utmost dedication. They share much of the other tasks of support, maintenance, installation, and configuration of computer equipment and systems. This is due to the budgetary constraints imposed by successive governments, which limit the investment available. Additionally, there is also a shortage of employees with specific training in cyber security. Thus, the need for tools that can support the work of these teams is urgent. In this sense, a computer solution that is free and open-source, while being easy to install, and configure, appears as an answer to the majority of the problem. This solution, aimed at managing information on events considered security incidents, can be of great value to medical centers.

By adopting such a system, medical centers have the opportunity to strengthen their response capacity, overcome some challenges, and become more resilient in the face of cyber threats. Protecting information systems, and ensuring the confidentiality and integrity of critical patient data, is certainly a more proactive and robust approach.

### 1.3 Objectives

The objectives that are intended to be achieved at the end of this work are essentially the following:

- Comprehensively review the literature to gain a deeper understanding of the topic, with a special focus on exploring relevant concepts related to cyber security and the implementation of SIEM, based on recommended standards and norms. Use as a source, reports from recognized organizations in this area, namely, National Institute of Standards and Technology (NIST), European Union Agency for Cybersecurity (ENISA), Centro Nacional de Cibersegurança (CNCS), and Comissão Nacional de Proteção de Dados (CNPd);
- Conduct a qualitative study, using a questionnaire, and interviews, with the collab-

oration of professionals in the area of cyber security, information technologies, and data protection to obtain relevant perspectives and opinions.

- Develop a reasoned proposal for the implementation of a SIEM system, taking into account the factors identified during the related work.
- Validate the proposed model and implement a SIEM in a laboratory environment, using virtual machines as a testing platform.
- Explore the feasibility of integrating SIEM with other security systems and IT infrastructure in the hospital context.
- Identify possible challenges and obstacles faced during the implementation of a SIEM system, that may also occur when implementing in hospitals and propose strategies to overcome them.
- Analyse the results obtained with the implementation of a SIEM system and evaluate the contributions of this study to guide future research.
- Contribute to the advancement of knowledge in cyber security in the health sector, and to the adoption of security solutions, such as SIEM, that are effective in hospitals.

## 1.4 Contributions

As already mentioned in the previous point, the main objective of this thesis is to analyze and study the process of implementing a SIEM system in hospital environments. It provides a more comprehensive view of relevant problems, best practices, and concerns in the health sector, deepening the understanding of SIEM systems integration in this key domain. This document presents an adequate SIEM system developed to meet the basic cyber security needs in hospitals. The methodology takes into account the specificities of healthcare, privacy concerns, and the diverse IT ecosystems present in hospital environments, providing a practical roadmap for effective SIEM systems implementation.

The validation and evaluation of the proposed SIEM system are carried out through practical tests in a simulated hospital environment, confirming the effectiveness and efficiency of the established SIEM structure. The results demonstrate the system's ability to

successfully detect, assess, and respond to cyber security issues, increasing confidence in their implementation. Adoption of these tools contributes to strengthening hospital infrastructure and its systems, preserving confidential patient data protecting against threats, and improving security in the health sector.

Based on the research results, this master's thesis also presents practical recommendations for future SIEM implementations in other hospitals. In addition, it is intended that this thesis contributes to the academic literature and can serve as a resource for researchers and professionals to address this topic.

## 1.5 Organization

This master's thesis is divided into seven chapters, each addressing a different aspect of SIEM analysis and implementation in a hospital. The first chapter begins with an introduction to the topic, emphasizing the importance of cyber security in the health sector. Furthermore, it establishes the objectives of the study, outlining the search for an effective and adaptable solution to increase and strengthen information security in a hospital context. The practical and relevant contributions of this study are also provided in this introductory chapter, focusing on solving the real problems faced by cyber security in a hospital. In Chapter 2, related work is carried out addressing the main concepts associated with cyber security, with references to other studies relevant to this thesis. Chapter 3 discusses the structure of the National Health Service in Portugal and the role of hospitals within it. Chapter 4 discusses cyber security in the health sector, focusing on key threats and risks, as well as a reference to the most critical services and appropriate cyber security best practices. The purpose of Chapter 5 is to discuss the methods used to assess the current level of cyber security in hospitals, and the results and analyses conducted on the current state of the Portuguese panorama. In Chapter 6, the planned implementation of SIEM in the field of health, more precisely in a hospital, is detailed. The focus is on the use of open-source software, with special attention to the most critical areas. A description of the architecture adopted is presented, along with the implementation process and the results obtained to validate the proposed approach. Finally, section 7 summarizes the master's thesis, presenting conclusions and considerations for future academic or

professional work, as well as a brief mention of the use of artificial intelligence, which is expected to be a significant improvement factor for related or similar work in the future.



## Chapter 2

# Related Work

This chapter explores the key components of cybersecurity. It begins with a comprehensive study of cybersecurity, threats, risks, and resilience, providing a clear picture of the current scenario. The focus then moves to SIEM systems, emphasizing their critical function and significance in ensuring strong security. A comparative study of Endpoint Detection & Response (EDR) and SIEM is conducted to highlight their relative strengths and applications. The chapter concludes with an analysis of the Security Operations Center (SOC), emphasizing its critical role in coordinating security measures.

### 2.1 Cybersecurity, Threats, Risks, and Resilience

Hospitals face the difficulty of protecting sensitive data in the face of numerous cyber threats as the healthcare sector becomes increasingly computerized. Implementing a SIEM system is a practical option widely used in other industries. To improve global cyber security in health facilities, this literature study will analyze the adoption of a SIEM system in a hospital environment, focusing on its intelligence and understanding.

An article by Wang [55], explores the importance of controls in cyber security, specifically in the detection and mitigation of threats. Threats are a constant concern in the cyber security world, and organizations must be proactive in their approach to detecting them, and then proceeding with the mitigation response. Threats come in many forms, such as malware, phishing, and social engineering attacks [37]. These attacks can lead to data breaches, financial losses, reputational damage, and disruption of hospital ser-

vices. In the CNCS risk management guide [10] it was found the most common threats to organizations, whether of natural (N), accidental (A), or intentional (I) origin, are as follows:

- System failure:
  - Equipment or system failure (A)
  - Saturation of the information system (A) (I)
  - Violation of the conditions of use of the information system that allows its maintenance (A) (I)
  - Defects (“bugs”) in the system (A) (I)
  - Abuse of rights or permissions (A) (I)
  
- Natural phenomenon:
  - Climatic phenomenon (N)
  - Seismic phenomenon (N)
  - Volcanic phenomenon (N)
  - Meteorological phenomenon (N)
  - Flooding (N)
  - Pandemic/epidemic phenomenon (N)
  
- Human error:
  - Improper disclosure of information (A) (I)
  - Data input from unreliable sources (A) (I)
  - Misuse of equipment (A) (I)
  - Error in use (A)
  - Unauthorized access to systems (A) (I)
  - Use of counterfeit or illegal copies of software (A) (I)
  - Software tampering (A) (I)
  - Violation of laws and regulations (A) (I)

- Malicious attack:
  - Terrorism, sabotage (I)
  - Social engineering (I)
  - Cyber espionage or unauthorized eavesdropping (I)
  - Theft of storage devices, documents, or information (I)
  - Theft of credentials or digital identity (I)
  - Theft of equipment (I)
  - Disclosure of information (A) (I)
  - Data input from unreliable sources (A) (I)
  - Hardware tampering (I)
  - Software tampering (A) (I)
  - Tampering/Compromising of data (A) (I)
  - Exploration using web communications (I)
  - Unauthorized entry into premises (I)
  - Unauthorized use of equipment or device (I)
  - Damage to equipment or devices (A) (I)
  - Sending or distributing malware (A) (I)
  - Intrusion into systems or unauthorized access (I)
  - Spoofing (I)
  - Attack on systems (e.g. distributed denial-of-service) (I)
  - Blackmail, bribery, assault or extortion of employees (I)
  - Improper use of computational resources (I)
- Supply chain failure by third party:
  - Interruption in the supply system (A) (I)
  - Interruption in the cooling or ventilation system (A) (I)
  - Loss of power supply (A) (N) (I)

- Interruption of telecommunication service (A) (I)
- Interruption of telecommunications equipment (A) (I)
- Other:
  - Fire (A) (N) (I)
  - Water (A) (N) (I)
  - Pollution, harmful radiation (A) (N) (I)
  - Serious accident (A) (N) (I)
  - Explosion (A) (N) (I)
  - Dust, corrosion, freezing (A) (N) (I)
  - Electromagnetic radiation (A) (N) (I)
  - Thermal radiation (A) (N) (I)
  - Electromagnetic impulses (A) (N) (I)
  - Lack of human resources (A) (N)
  - Lack of resources (A) (N)

To combat some of these threats, organizations must implement detection controls such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), log monitoring, and threat intelligence. The IDS and IPS can be of various types, in particular, intrusion detection or prevention systems are based on:

- Host
  - HIDS – Host-based intrusion detection system;
  - HIPS – Host-based intrusion prevention system;
- Networking
  - NIDS – Network-based intrusion detection system;
  - NIPS – Network-based Intrusion Prevention System

The article emphasizes the importance of continuous monitoring and analysis of system logs to identify anomalous behaviors and potential threats. It also highlights the need for threat intelligence to keep up to date on the latest threats and attack methods. By implementing these controls, organizations can improve capabilities before threats cause significant damage.

### **2.1.1 Confidentiality, Integrity, and Availability**

Known as the trinity, Confidentiality, integrity and availability (CIA) are the main pillars of information security. Confidential information is accessible only to authorized persons and is protected from unauthorized access or disclosure. Integrity ensures the accuracy and reliability of data by preventing unauthorized changes or manipulations. It ensures timely and reliable access to resources and data by authorized users when needed, preventing downtime and interruptions. The CIA Triad serves as a guiding principle for building strong security measures and helping organizations protect the confidentiality, integrity, and availability of critical information assets. Achieving a balance between these three principles is critical to developing a comprehensive and effective security posture. Any breach in these areas can lead to serious consequences such as data loss, loss of reliability, and disruption of operations. Organizations must constantly evaluate and adapt their security strategies to support the principles of privacy, integrity, and availability in an ever-changing threat environment.

### **2.1.2 Data Protection and Privacy**

Data protection and privacy are critical in today's digital age where vast amounts of personal information are collected, processed, and shared across multiple platforms. These concepts revolve around protecting individuals' data from misuse, unauthorized access, and privacy breaches. Data protection is the implementation of measures to secure sensitive information throughout its life cycle. This includes its collection, storage, processing, and finally disposal. Organizations are obliged to adopt strict security measures, encryption techniques, access controls, and regular audits to ensure data security compliance. On the other hand, privacy focuses on an individual's right to control their personal information. Obtain clear consent before data is collected, inform individuals about the

purpose and scope of data use, and allow them to access, modify, or delete their data. Privacy policies and statements are essential components of transparent data practices, building trust between organizations and their customers.

Data breaches and privacy violations can have dire consequences, from financial penalties to reputational damage. Regulatory frameworks such as Europe's General Data Protection Regulation (GDPR) [38] have raised the bar for data protection standards and strengthened individuals' rights. As data-driven technologies continue to advance, finding the right balance between using data to drive innovation and respecting individuals' privacy rights will become increasingly complex. Organizations must navigate this landscape ethically and responsibly, ensuring that the principles of data protection and privacy are upheld throughout their operations. In doing so, they not only comply with regulations but also foster a culture of respect for individual's personal information, developing trust and maintaining long-term relationships with their stakeholders.

### 2.1.3 Threats

Cybersecurity threats are a growing and changing challenge in the digital world, including malicious activities that target systems, networks, and data, compromising integrity, privacy, and availability. These threats include viruses, malware such as ransomware, phishing attacks that trick people into revealing sensitive information, social engineering tactics that exploit human psychology [37], Denial-of-Service (DOS) attacks, and DOS attacks. Fault data, internal operational threats, Advanced Persistent Threats (APT), open-source software vulnerabilities, payment encryption data, and vulnerabilities in Internet Of Things (IOT) devices. Addressing these threats requires regular updates, strong authentication, employee training, network security measures, incident response plans, and data backup strategies. The landscape requires constant adaptation and preparedness that encourages individuals and organizations to be vigilant, implement rigorous security measures, and promote a culture of cybersecurity awareness to protect digital assets.

### 2.1.4 Risks

Organizations also have to keep in mind the risk factor, that is, it is necessary to understand the risks to which they are subject, and this action is called risk management. Risk

management is a structured, ongoing process that organizations use to identify, measure, and prioritize the risks they face. This practice aims to establish clear risk acceptance criteria and set goals relevant to the organization. The purpose of risk management is to deal with uncertainty and its impact on organizational objectives by adopting necessary measures to reduce the likely effects and consequences of risks to a level considered acceptable by the organization. In summary, risk management involves making informed decisions to address uncertainty and protect the interests of the organization. Risk is also often presented as the product of the probability of happening by the impact it may cause, represented under the mathematical formula [11]:  $\text{Risk} = \text{Probability} \times \text{Impact}$

Therefore, it is necessary to carry out a risk survey, and for this, the following steps of this process must be taken into account:

- Identification of risks: this step aims to determine the situations that may result in losses for the organization, considering several factors, such as the cause, location, and reason for these losses. It is paramount to adopt a methodical and organized approach to list all relevant activities and identify the associated risks, even those that are not under the organization's domain. Some of the most common tasks for identification are vulnerability analysis, questionnaires, security audits, incident investigation, and risk assessment, among others.
- Risk analysis: it is essentially at this point to make a qualitative and quantitative analysis of each risk, according to probability and impact. This analysis is based on specific criteria, especially to verify the origin of the risks, the probability of occurrence, and the impact it has on the organization. Thus, risks ranging from the lowest level, "Very low" (1), to the most critical, "Very high" (5) are defined. It is possible to classify each level of impact for the different areas, regarding the consequences of the materialization of the risks, as shown in the figure below Fig. 2.1 [11]

Níveis de impacto	Legais e Regulatórios	Perdas Operacionais/ Financeiras	Perdas de Produtividade	Perdas de Clientes	Reputação e Imagem	Segurança e Saúde
<b>Muito Alto (5)</b>	Impacto legal/regulatório muito alto, com coimas altas associadas, podendo interromper a prestação do serviço, bem ou sistema	Quebra operacional significativa, podendo ser total e/ou definitiva	Impacto interno e externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir com as suas funções e responsabilidades	Descontentamento generalizado de um grupo de clientes críticos ao negócio, sem possibilidade de reverter a situação	Evento é conhecido externamente à organização e foi publicado por fontes de comunicação social, incluindo internacionalmente	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto total na organização
<b>Alto (4)</b>	Impacto legal/regulatório de alto impacto com coimas associadas	Quebra operacional parcial com impacto elevado nas operações	Impacto interno ou externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir com as suas funções e responsabilidades	Descontentamento de um grupo de clientes críticos ao negócio com possibilidade de reverter a situação.	Evento é conhecido externamente à organização e foi publicado por pessoas individuais	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto em mais do que um departamento da organização
<b>Médio (3)</b>	Impacto legal/regulatório de médio impacto	Quebra operacional parcial com algum impacto residual nas operações	Impacto interno ou externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir parcialmente com as suas funções e responsabilidades	Descontentamento de um grupo de clientes considerável com possibilidade de reverter a situação.	Evento ficou circunscrito internamente na organização	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto num departamento ou área da organização
<b>Baixo (2)</b>	Impacto legal/regulatório de baixo impacto	Quebra operacional parcial com muito baixo impacto nas operações	Impacto interno comprometendo a prestação do serviço, bem ou sistema, porém não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Descontentamento de um grupo reduzido de clientes com possibilidade de reverter a situação.	Evento ficou circunscrito internamente no departamento ou área afetada	Com registo de ausência colaboradores com baixa médica ou de seguro, sem impacto nas funções da organização
<b>Muito Baixo (1)</b>	Sem impactos previstos ao nível legal/regulatório	Sem impacto operacional / Financeiro para a organização	Impacto interno não comprometendo a prestação do serviço ou sistema, e não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Descontentamento de um grupo pequeno de clientes com possibilidade de reverter a situação no imediato.	Evento ficou circunscrito internamente na área afetada	Sem registo de ausência colaboradores com baixa médica ou de seguro

Figure 2.1: Definition of each impact level for all areas of consequence when the risks materialize. Source: [11]

In the end, a matrix is obtained, as already mentioned above, and which is represented in Fig. 2.2 [11]





Figure 2.2: Risk Matrix. Source: [11]

However, in services considered essential in the Cyberspace Security Legal Regime, (Article 3 of Law 46/2018, of August 13) [39], which may be a public or private entity that provides essential services in the energy, transport, banking, financial market, health, water supply, and digital infrastructures sectors, there may be a need to have a different configuration of the risk matrix, as can be seen in the Fig. 2.3, from [11]



Figure 2.3: Risk matrix for essential services. Source: [11]

- Risk assessment: the final stage, risk assessment, aims to support risk treatment decisions based on an acceptable level. It involves the analysis of previously identified risks to determine which require mitigation, transfer, or risk avoidance action. Risks considered tolerable, in the context of the organization or aligned with the pre-established level of acceptance, are also identified

The treatment of risks involves the identification, formalization, and execution of action plans to control and reduce risk factors. Risks are identified in the assessment, as can be seen in Table 2.1, and it is critical to designate a responsible person and date to implement these same plans. The goal is to decrease the level of risk after plans are completed. Possible approaches are:

- Minimize: reduce exposure and create plans with controls.

- Avoid: eliminate the cause of the risk and suspend certain activities.
- Transfer: place responsibility on third parties (e.g., suppliers)
- Accept: do not take any of the previous actions for risks considered low.

Table 2.1: Risk treatment action table

<b>Value of the risk and its treatment</b>	
<b>Description</b>	<b>Recommended treatment</b>
Very Low	Accept
Low	Accept / mitigate / transfer
Medium	Mitigate / Transfer
High	Mitigate / Transfer
Very high	Avoid

Risk communication seeks consensus in management, sharing data between managers and stakeholders, and maintaining this practice on an ongoing basis. It is essential to periodically review risk treatment plans in information security and cyber security, supported by decisions made. Collaboration with communication and external relations is crucial, especially in crises.

### 2.1.5 Resilience

An organization's resilience in the context of cyber security is its ability to adapt, recover, and maintain complex operations in response to a cyber-attack. This requires the implementation of robust cybersecurity measures and effective response strategies. To prevent this, early incident planning, vulnerability identification, and contingency planning are required. Furthermore, employees must be trained to recognize and face such threats. A well-protected IT infrastructure with regular backups and network segmentation contributes to stability, as mentioned by Eichelberg [18]. The ability to isolate and restore affected systems quickly is a critical factor. Conducting regular testing, including incident simulations, assists in the assessment and improvement of resilience.

The European Parliament and the Council of the European Union in their proposal for a regulation on horizontal cyber security requirements for products with digital elements and amendment of Regulation European Union (EU) 2019/1020, state that the Cyber

Security Act makes it possible to create certification schemes with references to cyber security standards and requirements. The certification decision is based on risk. Technical specifications and measures similar to those in the Cyber Security Resilience Act should be applied to the design, development, and treatment of software vulnerabilities, causing the cyber security of systems such as Electronic Health Records (EHR), even when delivered as Software-as-a-Service (SAAS) or developed in-house by healthcare institutions [13].

This document also states that manufacturers must obtain a European Cyber Security Certification under the European Cyber Security Certification Scheme. In determining the product categories of critical digital assets, the Commission will consider the cyber security risk associated with the product category of digital assets, taking into account one or more criteria from the list of critical products. To assess whether products in this category use or depend on the essential elements defined in the NIS2 Directive. The Resilience Act is a pioneer in establishing cyber security requirements in the commercialization of products with digital components. It builds on previous implementation experiences, the new legislative framework, and the application of existing EU product harmonization regulations, focusing mainly on preparing for the implementation and development of consensual standards.

The concept of a smart hospital is also grounded on resilience, as according to ENISA's November 2016 report on "Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures" [22], cyber security resilience becomes crucial as healthcare providers, including hospitals, must anticipate and deal with change and disruption. These are even more challenging in smart hospitals due to the complexity of factors impacting service availability. In Fig. 2.4 [22], it is represented as one of the main objectives.

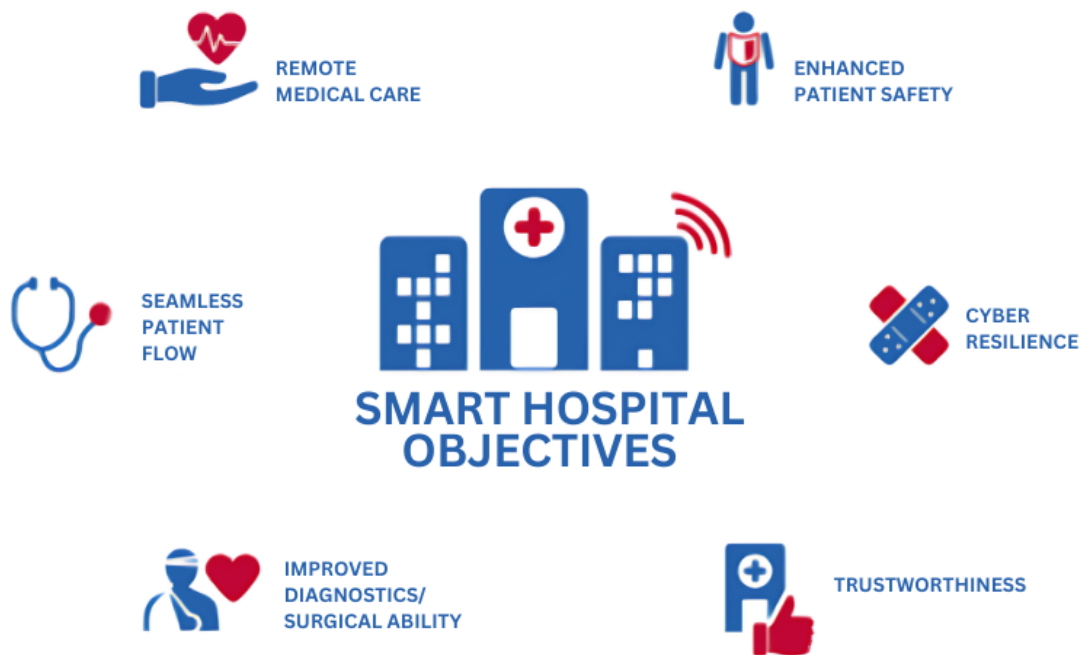


Figure 2.4: Smart Hospitals Objectives. Source: [22]

## 2.2 Security Information and Event Management (SIEM) Systems

In this chapter, the objective is to explore the concepts and attributes of a SIEM system, aiming at a deeper understanding of the utility and potential of this tool. The benefits and importance of proper implementation of a SIEM will be discussed. The emergence of SIEM meets the industry's need for a dynamic approach to network security, to provide visibility into the operational environment. SIEM results from the combination of Security Information Management (SIM) and Security Event Management (SEM). A SIEM allows you to identify and report incidents that need investigation and assist in resolving issues that are detrimental to the organization. With the popularization of cloud solutions in IT and security, SIEM is evolving rapidly. According to Gartner [41], 90% of SIEM systems will have unique cloud capabilities.

SIEM development is driven by the urgent need to detect threats in real-time, prioritizing security alerts more efficiently. SIEM systems identify risks through the collection

and analysis of IT event data, assisting in traffic management in complex infrastructures. However, early SIEM systems faced limitations, such as simplified dashboards and reporting, and basic notifications. The scalability of early SIEM systems presented challenges at several stages, including data collection, policy setting, and alert management.

### 2.2.1 Definition and Components (SIM and SEM)

Naturally, it is intended to clarify the concepts of these 2 components, SIM and SEM, to better understand the definition of a SIEM.

- **SIM:** SIM focuses on the collection, storage, and analysis of security information from multiple sources within an organization, with the primary objective of gaining a comprehensive view and making threat detection effective. SIM collects data such as logs, events, and activities generated by devices, operating systems, and network infrastructure, centrally storing them for deeper analysis, including from sources such as firewalls, intrusion detection systems, and authentication servers. It also allows for analyzing behavior patterns and detecting deviations, issuing alerts for suspicious activities, and contributing to the organization's regulatory compliance and safety.
- **SEM:** This component in the context of SIEM focuses on real-time analysis of security events to detect imminent threats or malicious activity. SEM processes and correlates events in real-time, using predefined rules and logic to identify patterns of suspicious activity, such as failed authentication attempts, unauthorized access, and anomalous activity on privileged user accounts. SEM analysis is essential for an immediate response to incidents, triggering automatic actions such as blocking suspicious Internet protocol (IP) addresses or isolating compromised systems. Additionally, it provides immediate insight into network security and necessary mitigation measures.

### 2.2.2 Objectives, Advantages, and Disadvantages

Given the existence of many security tools, it is imperative to understand the advantages and disadvantages of a SIEM and draw conclusions if an implementation justifies the

time and work that is allocated to make it work. SIEM aims to protect the organization's assets and data, identify threats, respond effectively to incidents, ensure compliance, and optimize security operations, within the protection of the organization's assets and data.

The main objectives and advantages of a SIEM, as in this case they do not make sense separately, are as follows:

- **Threat detection and malicious activity:** SIEM aims to identify and alert about suspicious activity, anomalous behavior, and potential cyber threats in real time. This includes the identification of intrusion attempts from the detection of malware, for example, unauthorized access and other malicious actions that could compromise the security of the systems and the network.
- **Data analysis and correlation:** SIEM collects information from various sources, such as event logs, system logs, security devices, and applications. Its purpose is to correlate and analyze this data to identify patterns and trends that may indicate suspicious activity or evolving threats.
- **Identification of vulnerabilities:** a SIEM allows a global understanding of threats, assessment of the current security posture, and identification of potential vulnerabilities in the systems.
- **Incident Response:** SIEM facilitates effective incident response, enabling rapid detection, assessment, and mitigation of threats. Through alerts and response automation, security teams can act promptly to minimize the impact of an incident.
- **Ensures regulatory compliance:** organizations need to comply with certain rules and regulations (e.g., GDPR), and for this purpose SIEM assists in this process, monitoring and recording relevant events that jeopardize these compliances. It also allows producing reports to demonstrate compliance to regulators (e.g., CNPD).
- **Improved operational efficiency:** By automatically monitoring the collection, standardization and analysis of safety data, SIEM improves the efficiency of safety operations, allowing teams greater dedication to other activities of greater importance.

- Reduced response times: if the detection and response capacity is faster, the organization's exposure time to computer attacks is shorter. Incidents and damage they may cause to the structure are minimized.

Potential disadvantages that may arise in certain implementations, due to the software in use or the size and complexity of the organization, include the following:

- Complexity: Implementing and configuring a SIEM can be complex and time-consuming, requiring specialized technical knowledge. The integration with other existing tools in the organization can make it difficult and result in increased costs.
- Cost: Acquiring, implementing, and maintaining a SIEM can often be costly, particularly for small organizations.
- False positives: A SIEM can generate false positives, which can lead security teams to an increase in work that was not foreseen. However, with a reset of rules, the system can improve considerably.
- Frequent adjustments: To maintain effectiveness, a SIEM requires adjustments to keep up with changes in infrastructure and threats. The more regular they are, the more dedication is needed from the cyber security teams.
- Training: Security teams should conduct drills, i.e. conduct drills to effectively use a SIEM, which can increase time and costs.

### 2.2.3 Architecture and Components

The architectures of SIEM can be diverse, but fundamentally they consist of a set of frameworks defined as the individual components that interact to provide a complete cybersecurity solution. It covers everything from how data is collected and stored, to running analytics to identify real-time threats and security trends. A SIEM is tasked with creating an environment that allows for the seamless integration of multiple data sources and the efficient performance of complex analyses, as visible in Fig. 2.5 [50].



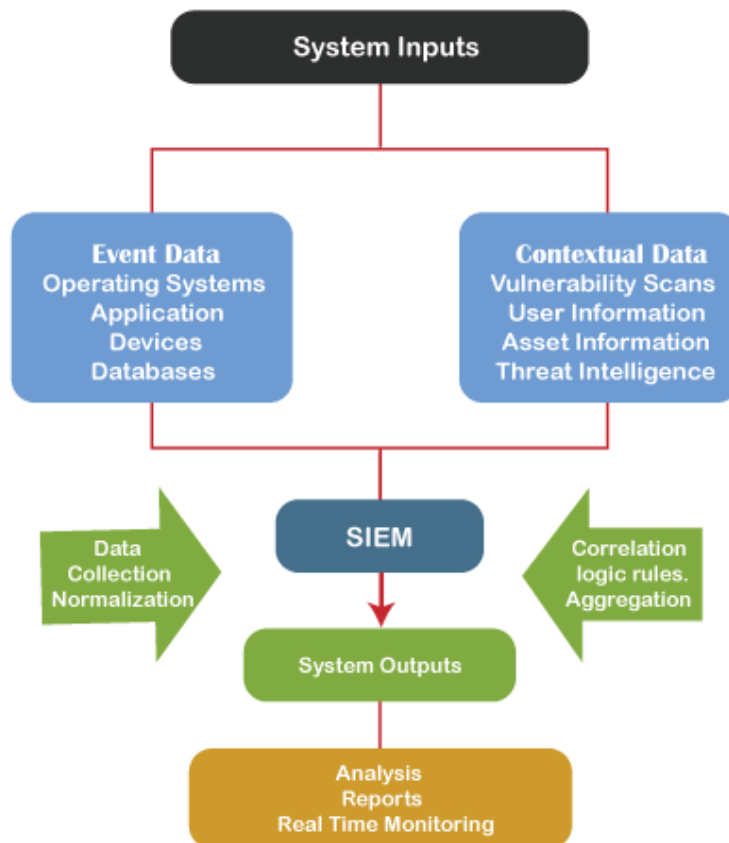


Figure 2.5: Architecture of a SIEM with representation of its components. Source: [50]

Concerning the installation and configuration of SIEM in an organization, the approach adopted may vary according to the characteristics, to adapt to different contexts and needs. The choice is influenced by several elements, in particular by security requirements, existing infrastructure, available resources, and preferences of the organization. Each type of architecture has its advantages and disadvantages, and the decision must be based on the specific needs of the organization and security objectives. Following are some of the main types of SIEM architectures:

- **On-Premises:** In this model, SIEM is installed and maintained within the organization's facilities. All security data is collected, processed, and stored on the organization's internal servers. This gives you greater control over data and infrastructure, but it also requires significant resources for system maintenance and upgrade.
- **Cloud-Based:** In this approach, SIEM is hosted in the cloud by a service provider.

Security data is sent to the cloud for processing and storage. This can be advantageous in terms of scalability and flexibility, allowing you to adjust features as needed. However, some organizations may have concerns about data security in the cloud.

- **Hybrid:** This is a combination of on-premises and cloud-based approaches. Data is processed both on-premises and in the cloud, offering a combination of direct control and scalability.
- **Distributed:** In this model, multiple SIEM instances are deployed to different locations in the organization. Each instance can be responsible for a specific segment of the network or a department. This can be useful for large organizations with multiple branches or stand-alone departments.
- **Managed Security Service Provider (MSSP):** when a third-party company MSSP manages and operates SIEM on behalf of the organization. This is beneficial for organizations with limited security resources or that prefer to delegate SIEM management to external experts.

#### 2.2.4 Workflow Processes

The main workflow processes in a SIEM are structured sequences of actions designed to effectively manage security events and incidents. These ensure the collection, analysis, correlation, and appropriate response to safety events in a coordinated manner. Workflows define steps, procedures, and automation to deal with security scenarios, namely:

- **Data Collection:** Obtaining security data from various sources, such as network devices, servers, applications, and endpoints. Workflows configure data sources to send logs, events, and details to SIEM
- **Normalization and Analysis:** the formatting of data sources and their normalization to a standard is necessary for correct analysis.
- **Event Correlation:** The identification of relationships between events aims to detect complex attack patterns.

- **Alert Generation:** the creation of alerts indicative of threats determines the prioritization of the most critical situations.
- **Incident Investigation:** Analysing alerts and events to assess the severity and impact of incidents guides analysts through the investigation steps.
- **Threat intelligence integration:** involves incorporating external sources of threat information to enrich SIEM data and enhance threat detection capability. This process encompasses the collection, correlation, and use of data from threat intelligence sources to strengthen the system's effectiveness in identifying potential.
- **Automation of responses:** in this process, automated, rule-based action definitions are created so that specific triggers occur and corresponding responses are executed.
- **Manual Responses:** It is possible to establish a set of step-by-step procedures so that analysts can address threats by following specific steps manually.
- **Generate reports:** for the management of security operations, as well as for the demonstration of compliance requirements with regulations, and regulatory authorities, it is important to create reports.

### 2.2.5 Examples of Vendors and Products

On the market, there are SIEM open-source and free solutions, as well as options that involve costs. As in Chapter 6, some open-source SIEM systems will be addressed, and reference is now made only to those that require acquisition or subscription. For this choice, we opted for the last classification (2022) by Gartner for SIEM [25], in Fig. 2.6.



Figure 2.6: SIEM Classification (2022) by GARTNER. Source: [25]

- IBM QRadar<sup>1</sup>: is a software-based security solution that provides flexibility when deployed in physical, virtual, and cloud environments. Its structure comprises several layers, including data sensors, a management console, analysis components, and integration with other security systems.

– Advantages:

\* Assortment of Features: IBM offers a diverse range of security, integration,

<sup>1</sup><https://www.ibm.com/qradar>

and analytics capabilities, allowing organizations to customize SIEM to their needs and on demand.

- \* Support: The technical support of this company is recognized for being robust and, as well as its consulting services, fundamental for successful implementations and operations.

– Disadvantages:

- \* Complexity: The feature richness of IBM’s solution can result in complexity in configuring and using SIEM, requiring advanced technical capabilities from the employees who operate it.
- \* High cost: Implementing and maintaining the IBM SIEM system can be costly, especially for small and medium-sized organizations.

- Splunk Enterprise Security<sup>2</sup>: is an advanced SIEM system that allows organizations to collect and analyze security data from a variety of sources, identifying malicious activity and suspicious patterns. The system offers event correlation tools and alerts to identify complex threats, while including automation and orchestration capabilities to speed up the response to security incidents.

– Advantages:

- \* Flexibility and customization: Customization of settings and search queries according to the specific needs of the organization is one of the great advantages.
- \* Data analysis: The great data analysis capacity of this platform is a strength, as it has robust data analysis capabilities, useful for detecting complex threats.

– Disadvantages:

- \* Cost: SIEM Splunk can have high costs for the organization, especially if data and requirements increase substantially.
- \* Learning: The learning curve, to make the most of Splunk’s features, can be accentuated by requiring a lot of technical knowledge and training.

---

<sup>2</sup><https://www.splunk.com/en-us/products/enterprise-security.html>

- Securonix<sup>3</sup>: This security service provider offers several possibilities for incident management systems, in particular Unified Defense SIEM, which is a more advanced solution. Furthermore, it has a solution dedicated to the health sector, which allows the monitoring of employees and how they interact with patient records. Compliance with regulatory requirements through advanced safety monitoring and behavioral analysis, and one of the added value.
  - Advantages:
    - \* Threat detection: Securonix is known for its advanced threat detection capabilities and use of behavioral analytics.
    - \* Unified platform: The ability to integrate data from multiple sources into a single platform is one of the great advantages of this SIEM.
  - Disadvantages:
    - \* Initial Complexity: initial configuration and adaptation to the detection logic can be complex.
    - \* Cost: The costs of this solution may limit some organizations, especially smaller ones.
- Exabeam<sup>4</sup>: Exabeam’s SIEM systems work in the cloud and offer a comprehensive set of functionalities, including alert management, correlations, search, and automation.
  - Advantages:
    - \* Behavioural analysis: stands out for the detailed analysis of user behavior, assisting in the identification of anomalous activities.
    - \* Ease of use: These SIEM have an intuitive interface that simplifies setup and use, even for less experienced users.
  - Disadvantages:
    - \* Cost: This solution can be expensive, especially if more advanced features are considered.

---

<sup>3</sup><https://www.securonix.com/products/unified-defense-siem/>

<sup>4</sup><https://www.exabeam.com/product/siem/>

- \* Integration: Integration of EXABEAN SIEM is quite complex, especially with specific systems and data sources, which can be a challenge.
- LogRhythm<sup>5</sup>: LogRhythm SIEM provides integrated modules, dashboards, and rules that contribute to the effectiveness of the SOC, while also creating a coherent security narrative by consolidating user or device data and activities into a single view.
  - Advantages:
    - \* Automation: LogRhythm offers robust automation capabilities, making incident and repetitive task response more agile.
    - \* Monitoring: the large capacity for detailed monitoring and the possibility of creating complete reports is one of the advantages.
  - Disadvantages:
    - \* Cost: Implementation and maintenance can be costly, especially for smaller organizations.
    - \* Learning: An initial learning curve may be required to fully explore your capabilities.
- Rapid7<sup>6</sup>: InsightIDR is a cloud-based SIEM that maximizes the power of cloud analytics to solve and respond to urgent problems. In this solution, the detection results are constantly updated with Metasploit search results.
  - Advantages:
    - \* Simplicity: Rapid7's intuitive interface makes it easy to set up and use, making it very user-friendly for users with different levels of experience.
    - \* Detection and response: the highlight of this solution is the speed in identifying and responding to incidents, minimizing the impact they may cause.
  - Disadvantages:
    - \* Scalability: Scalability with Rapid7 is limited, which can be a problem for larger organizations.

---

<sup>5</sup><https://logrhythm.com/solutions/security/siem/>

<sup>6</sup><https://www.rapid7.com/products/insightidr/>

- \* Features: Some features made available are less advanced compared to other SIEM.
- Fortinet<sup>7</sup>: FortiSIEM is designed to be the pillar of security operations, it allows the automatic management of asset inventory, the application of advanced behavioral analysis for agile detection and response to threats, among other possibilities.
  - Advantages:
    - \* Integration: Integration with other security products is high, enabling a holistic approach to protection.
    - \* Performance: the high performance and speed allow, with this solution, more effective analysis and detection.
  - Disadvantages:
    - \* Complexity: the variety of features and products can result in complexity in the configuration and management of this solution.
    - \* Cost: The high costs of implementing this SIEM can be a limiting factor for some organizations with fewer financial resources.
- DEVO<sup>8</sup>: DEVO's cloud-based SIEM system enables insight into security, risk, and threat detection.
  - Advantages:
    - \* Data Centralization: DEVO's SIEM is known for centralizing large volumes of data, providing more comprehensive visibility.
    - \* Advanced analytics: This solution stands out for providing advanced analytics in real-time, allowing immediate identification of threats.
  - Disadvantages:
    - \* Cost: The price of this solution can be a deterrent for organizations on a budget.
    - \* Learning: It takes a lot of time to fully master this platform and its features.

---

<sup>7</sup><https://www.fortinet.com/br/products/siem/fortisiem>

<sup>8</sup><https://www.devo.com/platform/intelligent-siem/>



In short, these solutions, cloud-based or not, have advantages that are usually reflected in the offer of complete resources and advanced features. On the other hand, the disadvantages focus mainly on implementation and maintenance costs, as well as the time required for learning and the technical knowledge needed by the professionals in charge of the operations.

### 2.3 EDR vs. SIEM

Sometimes, some managers and system administrators prefer EDR over SIEM due to its greater usefulness in the daily life of organizations. EDR focuses on endpoints in detecting specific threats, and suspicious activity, and provides contextualized information about incidents [30]. This allows security teams to quickly mitigate malicious activity and restore affected systems. In these activities, tools are used that include data collection, screening, analysis and detection of suspicious activities, data exploitation, and allowing to interrupt malicious activities. However, it is relevant to mention that SIEM covers security information and events throughout the organization's IT infrastructure, identifying anomalous patterns, and threats and responding to legal regulations. Privacy and data protection are key elements and are intrinsically linked to cyber security.

To better understand the difference between an EDR and a SIEM, the table 2.2 was elaborated, which contains the main features of each one.

Table 2.2: Main features of EDR and SIEM

<b>EDR</b>	<b>SIEM</b>
Incident data collection at endpoints and IT systems.	Integration with various security tools
Alert screening and analysis of suspicious activity	Collects and correlates data from multiple sources, such as networks, endpoints, and other devices
Detection of suspicious activity	Creates alerts
Enables data exploration or threat hunting	Manage Alerts Workflow
Provides manual and automated tools to stop malicious activity	Allows you to get information about the entire infrastructure.
Automates incident response	Enables improved compliance with legal regulations and standards.

Therefore, the best choice will always depend on what organizations and their managers want to achieve. If the focus is on protection and detailed endpoint monitoring, a EDR may be more appropriate, providing automated response and granular visibility. On the other hand, if the need involves a holistic view of security across the network, an SIEM offers the ability to analyze and correlate data from multiple sources, making it easier to detect and respond to large-scale threats. In the Fig. 2.7, it is represented the main features.

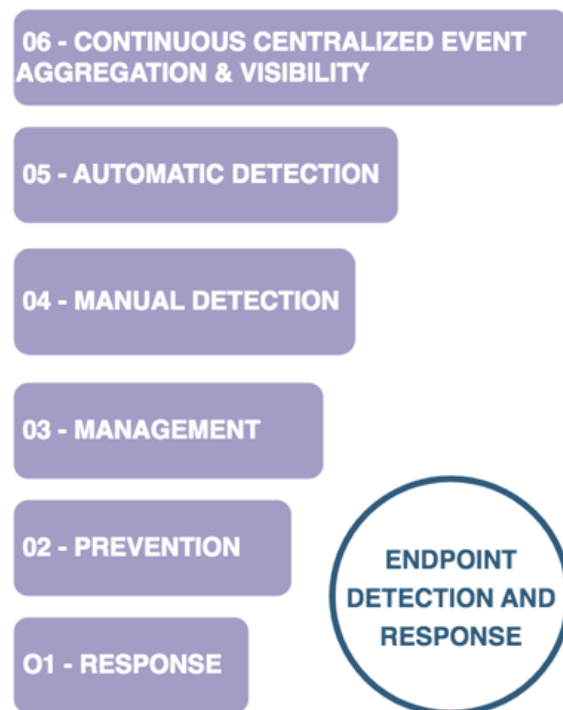


Figure 2.7: Endpoint detection and response - features. Source: the author.

## 2.4 Security Operations Center (SOC)

### 2.4.1 Definition and Functions

A SOC is a centralized facility comprised of a team of information security professionals and IT professionals who analyze, monitor, and defend the organization against cyber attacks. SOC teams respond to incidents by continuously monitoring networks, web traffic, servers, desktops, databases, endpoints, applications, and other IT components for evidence of security incidents [1]. The members of this center generally have the necessary

skills to identify and respond to cyber security incidents, and most often work in shifts, as SOC operate 24/7. Some companies outsource their SOC to external suppliers, when they cannot have one in-house or when this is more advantageous for the organization. SOC is an important strategy to reduce the costs of a data breach and to help respond quickly to attacks.

The most relevant functions of a SOC, in Fig. 2.8, represent the main features that lead organizations to constitute or hire it, are the following:

- **Resource Assessment:** A SOC is responsible for securing devices, processes, and applications, as well as maintaining security tools.
- **Preventive maintenance:** A SOC implements several preventive measures to prevent incidents and deter potential attackers.
- **Continuous monitoring:** these centers have tools that guarantee the detection of anomalous activities and notify emerging threats, in a continuous period, i.e. 24/7.
- **Alert management:** the management and analysis of alerts carried out by the SOC are issued by the tools, with the disposal of false positives, determining the degree of each threat found.
- **Recovery/remediation:** After each incident, a SOC proceeds to restore the systems and recover any lost data. Creates backups so that it is possible to restore the system, thus avoiding ransomware attacks.
- **Records management:** A SOC collects and reviews network activity records, identifying patterns and threats, used in post-incident remediation.
- **Investigation:** A SOC investigates incidents by tracing back to the origin to prevent similar situations in the future.
- **Security improvement:** a SOC contributes to the continuous improvement of the organization, in the preparation of strategies to overcome the techniques used by cyber criminals, through procedures used by Red-teams.

- Compliance management: a SOC ensures compliance with regulations, protecting data entrusted by the holders, avoiding damage to the organization's reputation and the payment of fines.

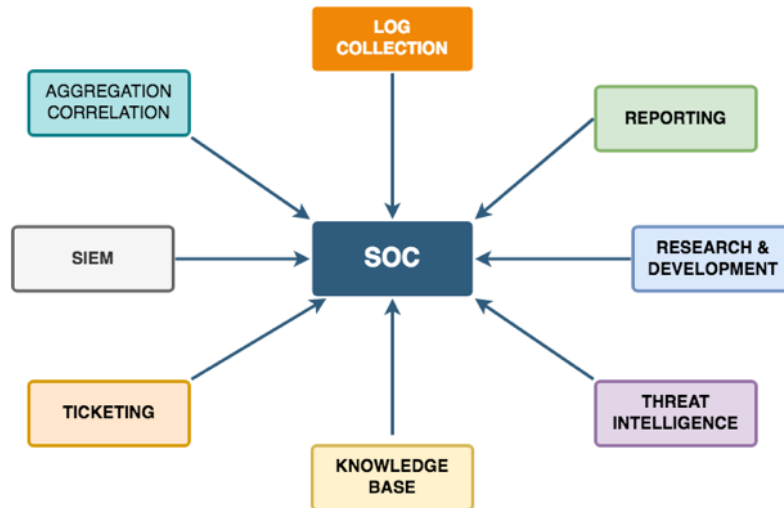


Figure 2.8: Diagram of the different components of a SOC. Source: The author.

### 2.4.2 Open-source Examples of SOC tools

To create a SOC, it is essential to have a set of tools that allow you to fulfill your various responsibilities. Solutions such as SIEM, intrusion detection and prevention tools (IDS/IPS/Intrusion Detection and Prevention Systems (IDPS)), incident response, and malware analysis, among others, are needed, according to Zuech(2015) [61]. Among the free and open-source alternatives, the following options stand out:

- Wazuh<sup>9</sup>: Wazuh is a SIEM platform that makes it simple to collect data through agents and syslogs. Wazuh demonstrates efficiency when monitoring IT infrastructure devices.
- Suricata<sup>10</sup>: Suricata is a high-performance network intrusion detection and prevention tool (IDS/IPS/IDPS)

<sup>9</sup><https://wazuh.com/platform/siem/>

<sup>10</sup><https://suricata.io/>

- Snort<sup>11</sup>: Snort is the best-known intrusion detection and prevention solution (IDS/IPS/IDPS) for Windows and UNIX operating systems, providing intrusion analysis, packet monitoring, and predicting intrusions in real-time.
- ClamAV<sup>12</sup>: ClamAV is a framework for email gateway virus scanning and is available on Windows, OS X, Linux, and BSD applications.
- Volatility (<https://www.volatilityfoundation.org/>): The Volatility Framework is an incident response solution, developed in Python.
- SIFT Workstation<sup>13</sup>: SIFT Workstation is a collection of incident response tools designed to perform detailed forensic examinations.
- TheHive<sup>14</sup>: TheHive project is an incident response framework that allows you to conduct incident investigations at the same time.
- Zeek (Bro)<sup>15</sup>: Zeek is a malware analysis tool, which analyses network traffic and creates transaction logs and can be complementary to a SIEM.
- Cuckoo<sup>16</sup>: Cuckoo Sandbox is free software that automates analyzing any malicious file under Windows, macOS, Linux, and Android. This solution provides detailed reports of the behavior of these files when executed in a real environment. It then allows you to understand the context, motivations, and objectives of the violations of these files.
- GRR<sup>17</sup>: GRR is an agent developed in Python and installed on endpoints and the infrastructure where the servers are located to perform forensic analysis of incidents remotely.

Open-source SOC tools provide comprehensive resources for detecting, preventing, and responding to cyber threats. In the supervision of incidents up to malware analysis,

---

<sup>11</sup><https://www.snort.org/>

<sup>12</sup><https://www.clamav.net/>

<sup>13</sup><https://www.sans.org/tools/sift-workstation/>

<sup>14</sup><https://thehive-project.org/>

<sup>15</sup><https://zeek.org/>

<sup>16</sup><https://cuckoosandbox.org/>

<sup>17</sup><https://github.com/google/grr>

these tools reinforce organizational security and promote an adaptive and collaborative approach.

## Chapter 3

# Organization of the Healthcare Sector in Portugal

This chapter aims to elucidate the structure and organization of the National Health Service (NHS). This objective necessitated a historical review, highlighting key milestones from its establishment in the late 1970s to the present. Subsequently, the composition of the Serviço Nacional de Saúde (SNS), encompassing various entities and organisms, was delineated in line with the directives of the SNS's Executive Direction, supervised by the Ministry of Health. The chapter concludes with an examination of the role of PBE hospital units, the primary focus of this master's thesis.

### 3.1 History of the Healthcare System

The Portuguese National Health Service ("Serviço Nacional de Saúde" or SNS) was established in Portugal by Law 56/79 of 1979, based on the model of the Portuguese Public Administration, to ensure universal, generic, and free access to health care. These objectives were defined by António Arnaut, considered the "father" of the SNS, who was responsible for the development of the system, which faced several problems, including the resistance of the medical class and the country's economic and financial crisis. Since then, the SNS has been a symbol of quality and one of Portugal's proudest, despite problems and criticism, such as the lack of funds and the need for modernization. However, the SNS remained one of the most efficient and accessible health systems in the world and an

example of how health can be a universal right.

The SNS today is the result of the combination of several significant milestones [48], which can be considered fundamental since they have been part of its history since its creation in 1979. In summary and chronological order, some of these achievements are presented here:

- 1979 - Creation of the National Health Service (SNS) (Law No. 56/79, 15 of September);
- 1980 - Year of the Declaration of the Worldwide Eradication of Smallpox;
- 1981 - Institutionalization of the Nursing Career;
- 1982 - Administrative and financial autonomy of the SNS in charge of the Financial Management Department;
- 1983 - Creation of the Ministry of Health (Decree No. 344-A/83, 25 of July); 1984 - Creation of the General Directorate for Primary Health Care (Law No. 74-C/84 2 of March);
- 1985 - Laura Ayres stands out in leading the AIDS Working Group;
- 1986 - Accession of Portugal to the European Union, which marks the beginning of a new cycle for Health;
- 1987 - Creation of the Code of Ethics for the Pharmaceutical Industry;
- 1988 - Approval of the Hospital Management Law (Decree-Law 19/88, 21 of January);
- 1989 - Second Constitutional Revision, amending Article 64, stipulating the right to health protection carried out by the SNS "universal and general and, taking into account the economic and social conditions of citizens, usually free of charge";
- 1990 - The Basic Health Law (Law No. 48/90, 24 of August) was approved;
- 1991 - First Statute of the Medicinal Product: a new era begins in the field of marketing, quality control, and manufacture of medicinal products for human use;



- 1992 - Beginning of the Liver Transplant Program at Curry Cabral Hospital;
- 1993 - Establishment of the European Medicine Agency;
- 1994 - António Torrado da Silva leads the National Maternal and Child Health Commission; the great goal of reaching the single-digit rate of perinatal mortality became a reality, as had already happened for infant mortality, in 1993;
- 1995 - First private management contract of a public hospital: Hospital "Fernando da Fonseca";
- 1996 - Health Reflection Council;
- 1997 - Contracting of Health Services;
- 1998 - Women's and Perinatal Health Leadership;
- 1999 - Institutionalization of the Institute of Quality in Health;
- 2000 - Hepatitis B vaccine;
- 2001 - Urgency and Emergency Hospital Referral Network;
- 2002 - Elimination of polio in Europe, certified and declared by World Health Organization (WHO);
- 2003 - Creation of the Health Regulatory Entity ("Entidade Reguladora da Saúde" or ERS) (Decree-Law No. 309/2003, 10 of December);
- 2004 - Integrated Surgery Enrolment Management System;
- 2005 - Reduction of infant mortality;
- 2006 - National Network of Integrated Continuing Care ("Rede Nacional de Cuidados Continuados Integrados" or RNCCI) (Decree-Law No. 101/2006, 6 of June);
- 2007 - Creation of Family Health Units ("Unidades de Saúde Familiares" or USF) (Decree No. 298/2007, 22 of August);
- 2008 - Creation of Health Centers Groups ("Agrupamentos de Centros de Saúde" or ACES) (Decree No. 28/2008, 22 of February);

- 2009 - Enlargement of the dental check program. A program focused on promoting dental health for the general population by providing a free dental check-up;
- 2010 - Electronic prescription for medication;
- 2011 - Clinical Guidance Standards issued by the General Directorate of Health ("Direção-Geral da Saúde" or DGS);
- 2012 - New "Patient Portal", integrated into the Health Data Platform project, allowing health records made by the patient and the use of online services such as appointment scheduling;
- 2013 - New regime for the availability, sale, and consumption of alcoholic beverages to minors;
- 2014 - Creation of Early Intervention in Oral Cancer;
- 2015 - Introduction of curative therapy for Hepatitis C;
- 2016 - Creation of the National Plan for the Prevention and Control of Vector-Borne Diseases
- 2017 - First artificial heart transplant in Portugal by Dr. José Fragata, at the Santa Marta Hospital;
- 2018 - Approval of the National Vision Strategy;
- 2019 - Implementation of the project of an autonomous management model for hospitals and local health units (Unidade Local de Saúde (ULS));
- 2022 - Creation of the Executive Board for the National Health Service (without regulation so far);

## 3.2 Structure and Organization of the SNS

The Portuguese NHS(SNS) is composed of all public entities and services that provide health care [47], graphically represented in Fig. 3.1 from [47], namely:

- The Groupings of Health Centers (ACeS): o These clusters are responsible for primary health care, meeting the needs of local communities. Each cluster comprises several health centers, being the basic units of the national health service for the provision of non-urgent health care. Several health professionals work in these centers, such as family doctors, general practitioners, nurses, and social service technicians, among others. Routine consultations, nursing, family health, and administration of vaccines from the National Vaccination Program are also provided.
- Health Facilities of various natures: Public hospitals are mainly focused on the provision of differentiated health care. These hospital units can be PBE hospitals, or PBE hospital centers, which manage several hospital units in the same geographical area. Note: PBE hospitals are public companies endowed with legal personality with administrative and financial autonomy, whose activity is financed through production program contracts entered into between the Hospitals and the National Health Service (SNS), as provided for in Decree-Law n. 188/2003, 20 of August.
- The Local Health Units (ULS): the SNS includes local health units (ULS), which cover all health centers and hospitals in a given city or region, providing primary and differentiated care.
- The Instituto Português de Oncologia (IPO): There are three oncology institutes in Portugal. The first, founded by him in 1923 in Lisbon, was named the Portuguese Institute for the Study of Cancer.

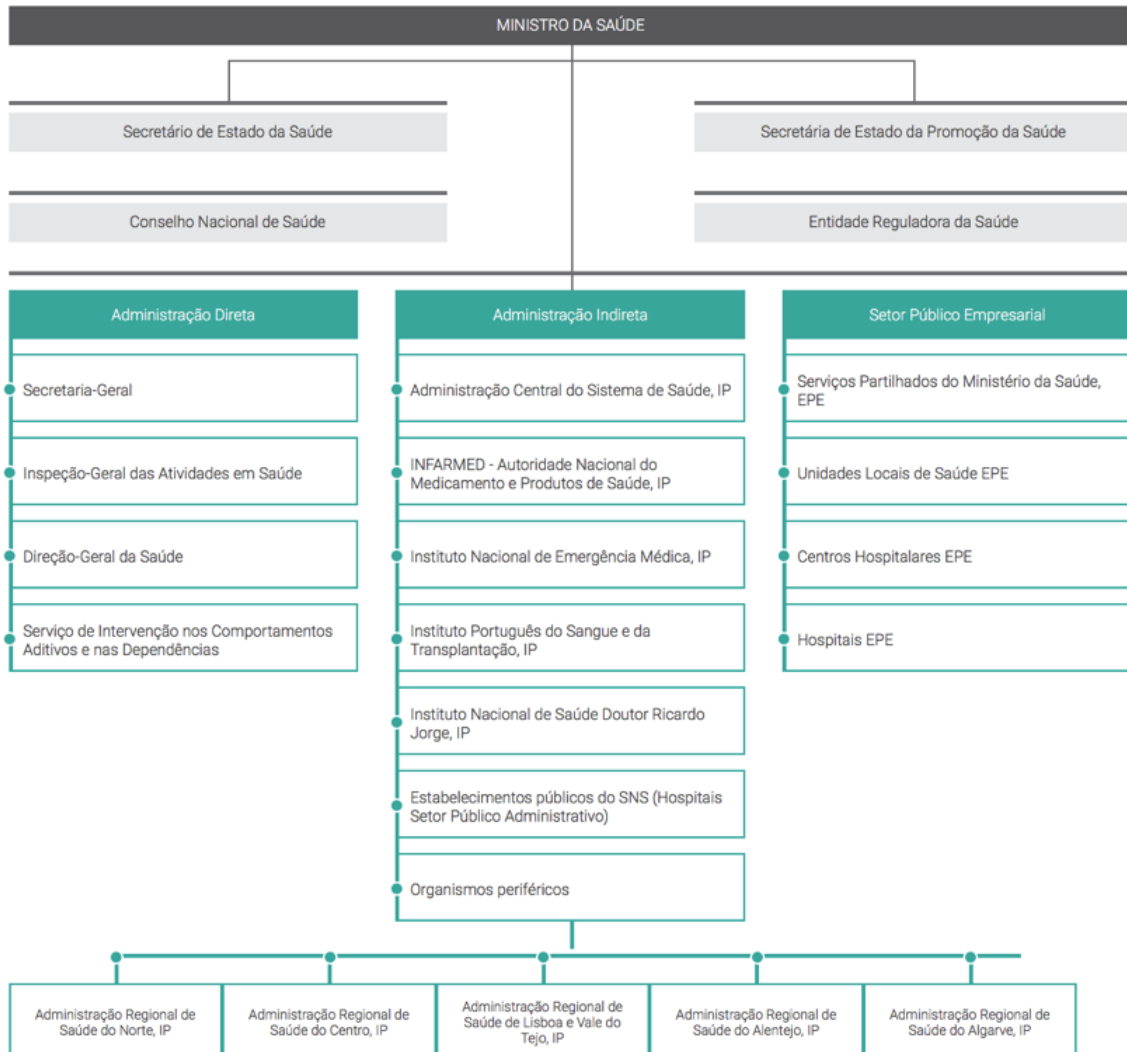


Figure 3.1: Service organization chart.

The new Statute of the SNS, established by Decree-Law No. 52/2022 4 of August, brought a significant novelty by creating the Executive Council for the SNS. This body’s main function is to coordinate the network of SNS health units, including the National Network of Integrated Continuous Care (NNICC) and the National Network of Palliative Care (NNPC). The Executive Council has assumed powers previously delegated to other organizations, such as supervising access to health care and appointing members to the management bodies of health units. The Executive Board of the SNS, in turn, has a distinct role in the Ministry of Health, being responsible for formulating the national health policy, but not for the practical coordination of the SNS responses. This

differentiation is also noted concerning the Central Administration of the Health System, I.P. (“Administração Central do Sistema de Saúde” or ACSS, I.P.), which deals with the negotiation and administration of financial and human resources, and the Regional Health Administration, I.P. (“Administração Regional de Saúde” or ARS, I.P.), whose focus has become the regional management of health resources. As of October 2022, the government approved in the Council of Ministers the creation of the Executive Board of the National Health Service (SNS), with Fernando Araújo, then chairman of the Board of Directors of University Hospital Center São João, in the city of Porto, was appointed as executive director of the SNS. This function encompasses the coordination, management, and guarantee of the continuous improvement of the SNS, in line with the guidelines established by the government, as well as the promotion of public participation in the health system. A series of more recent reforms are also being prepared, including the creation of new Local Health Units such as the Braga ULS, which will include the PBE of Hospital of Braga, Cávado ACES, and Cabreira-Gerês ACES. The organization of the SNS at the territorial level is defined by health regions (North, Center, Lisbon and the Valley of Tejo, Alentejo, Algarve), cf. Fig. 3.2, and at the functional level by proximity parameters, integrated with care with inter-regional service.



Figure 3.2: Health regions of mainland Portugal. Source: The author.

At the end of 2002, 34 hospitals of the SNS were transformed into 31 PBE hospitals (with exclusively public capital). This change consisted of a transition from management models, that is, from public institutes to public companies, adopting a private law regime for management. On the 7 of December 2005, the acting government made a new change, that is, the S.A. hospitals became a Public Business Entity (Entidade Pública Empresarial (EPE))

### 3.3 Role of PBE Healthcare Units

The definition of PBE Hospitals and Hospital Centers is found in the “Statutes – Hospitals and Hospital Centers, EPE, and in particular, in Annex II to Decree-Law No. 233/05, 29 of December [45], amended and republished by Decree-Law No. 12/2015, 26 of January [44]. Essentially, as referred to in Chapter I (General Principles), in Article 1, in its point 1, it is described as ”PBE hospital is a legal person governed by public law of a

business nature endowed with administrative, financial and patrimonial autonomy, under the terms of the legal regime of the business sector of the State and public companies, and of article 18 of the annex to Law No. 27/2002, 8 of November” [46].

Also according to the Legal Statute of PBE Hospitals, its organization is composed of several bodies: the board of directors, the sole auditor, and the advisory board. The Board of Directors is composed of the president, and up to six more individuals at most, of which the clinical director and the nurse director must be a part, as we can see in Fig. 3.3.

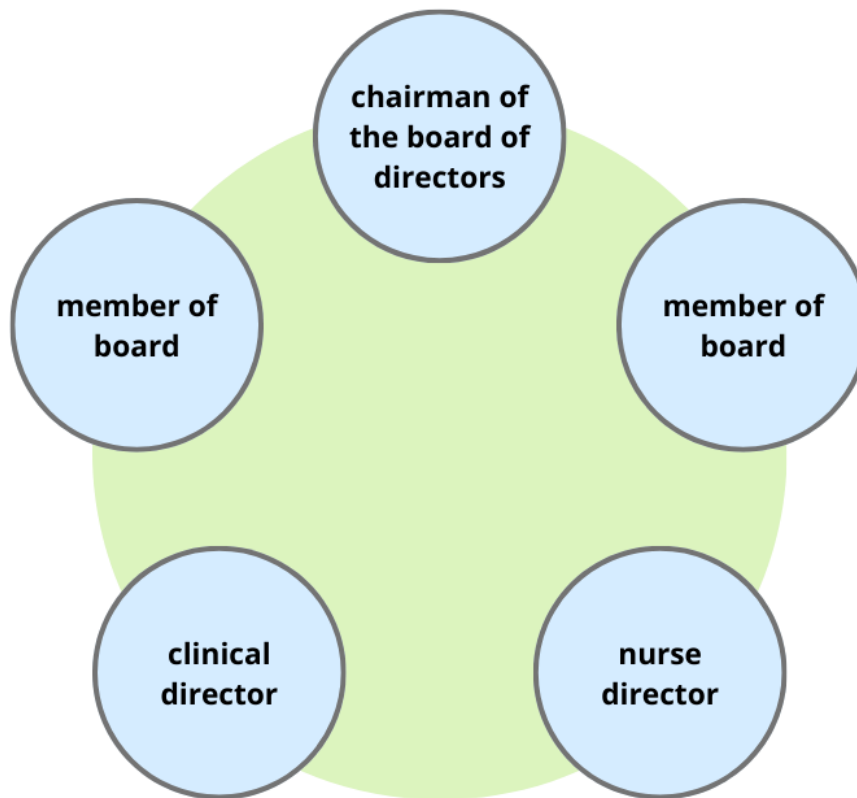


Figure 3.3: Organization chart of the internal organization of a PBE hospital unit. Source: The author.

The PBE hospital is a public entity with the main objective of providing health care to the population. This includes SNS beneficiaries, beneficiaries of health subsystems, among other citizens in general. The hospital is also dedicated to research, training, and teaching activities. Their participation in the training of health professionals depends on their training capacity, which is usually funded by program contracts in partnership

with higher education institutions. As of today, the existing PBE health institutions in the national health service of Portugal are as follows: 11 Hospitals, 21 Hospital Centers, 8 Local Health Units, and 3 Oncology Institutes, in a total of 43 units, represented in Fig. 3.4. They are located in several districts of Portugal, covering much of the central coast and northern coast of mainland Portugal, such that:

- PBE Hospitals
  - Hospital da Senhora da Oliveira Guimarães, EPE (Braga)
  - Hospital de Braga, EPE (Braga)
  - Hospital de Loures, EPE (Lisbon)
  - Hospital de Magalhães Lemos, EPE (Porto)
  - Vila Franca de Xira Hospital, EPE (Lisbon)
  - Hospital Distrital de Santarém, EPE (Santarém)
  - Figueira da Foz District Hospital, EPE (Coimbra)
  - Hospital do Espírito Santo de Évora, EPE (Évora)
  - Garcia de Orta Hospital, EPE (Setúbal)
  - Professor Fernando Fonseca Doctor Hospital, EPE (Lisbon)
  - Hospital Santa Maria Maior, EPE (Braga)
  
- EPE Hospital Centers
  - Centro Hospitalar Barreiro Montijo, EPE (Setúbal);
  - Centro Hospitalar de Entre o Douro e Vouga, EPE (Aveiro);
  - Centro Hospitalar de Leiria, EPE (Leiria)
  - Centro Hospitalar de Lisboa Ocidental, EPE (Lisbon);
  - Centro Hospitalar de Setúbal, EPE (Setúbal);
  - Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE (Vila Real)
  - Centro Hospitalar de Vila Nova de Gaia/Espinho, EPE (Porto)
  - Centro Hospitalar do Baixo Vouga, EPE (Aveiro)



- Centro Hospitalar do Médio Ave, EPE (Braga)
- Centro Hospitalar do Médio Tejo, EPE (Santarém)
- Centro Hospitalar do Oeste, EPE (Leiria)
- Centro Hospitalar do Tâmega e Sousa, EPE (Porto)
- Centro Hospitalar e Universitário de Coimbra, EPE (Coimbra)
- Centro Hospitalar de Póvoa de Varzim/Vila do Conde, EPE (Porto)
- Centro Hospitalar Tondela Viseu, EPE (Viseu)
- Centro Hospitalar Universitário Cova da Beira, EPE (Castelo Branco)
- Centro Hospitalar Universitário de Lisboa Central, EPE (Lisbon)
- Centro Hospitalar Universitário de Santo António, EPE (Porto);
- Centro Hospitalar Universitário de São João, EPE (Porto);
- Centro Hospitalar Universitário do Algarve, EPE (Faro)
- Centro Hospitalar Universitário Lisboa Norte, EPE (Lisbon)
  
- Local Health Units (ULS)
  - ULS de Matosinhos, EPE (Porto),
  - ULS do Norte Alentejano, EPE (Portalegre),
  - ULS da Guarda, EPE (Guarda)
  - ULS do Baixo Alentejo, EPE (Beja)
  - ULS do Alto Minho, EPE (Viana do Castelo)
  - ULS of Castelo Branco, EPE (Castelo Branco)
  - ULS do Nordeste, EPE (Bragança)
  - ULS do Litoral Alentejano, EPE (Setúbal)
  
- Portuguese Institute of Oncology
  - Instituto Português de Oncologia Dr. Francisco Gentil do Porto, EPE
  - Instituto Português de Oncologia Dr. Francisco Gentil de Coimbra, EPE
  - Instituto Português de Oncologia Dr. Francisco Gentil de Lisboa EPE

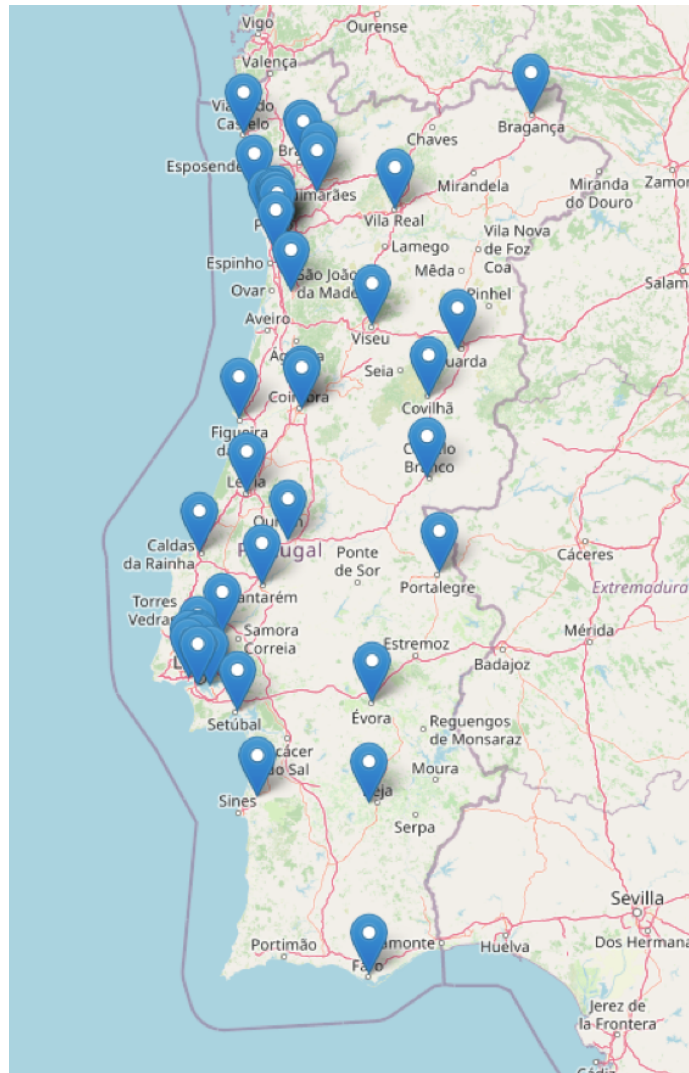


Figure 3.4: Location of PBE units in mainland Portugal. Source: The author.

Hospitals in the Autonomous Region of the Azores were not considered, as they now have another designation Regional Public Business Entities (*Entidades Públicas Empresariais Regionais*; EPER), under Regional D.L. No. 22/2015/A 18 of September [2]. As for the Autonomous Region of Madeira, the procedure is identical, as Regional Decree No. 8/2020/M 13 of July [32] changed the designation of SESARAM EPE to SESARAM, EPERAM with its statutes. However, the analyses produced in this work can certainly apply technically to these organizations.

## Chapter 4

# Healthcare Security

Healthcare security is a significant field that addresses challenges from the protection of patient data to the uninterrupted operation of medical equipment. It encounters evolving threats from cybercriminals who exploit system vulnerabilities, disrupting critical services. Therefore, it is essential for hospitals to adopt effective cybersecurity best practices, which include rigorous network security, regular system updates, and comprehensive staff training. The industry is also focusing on the enhancement of cybersecurity skills, acknowledging the critical role of human elements in maintaining a secure healthcare system.

### 4.1 Overview of Healthcare Security Challenges

Cyber security has become a growing concern in the healthcare sector, driven by technological advances and digital transformation in medical service delivery. The dematerialization of processes, due to SNS reforms, raises crucial questions about the privacy and protection of patient and employee data, as well as the integrity of data and IT systems, as previously mentioned. Growing reliance on information systems exposes hospitals and healthcare institutions to unique security challenges. The use of digital technologies and electronic medical records has brought benefits to patient care but has also generated new risks and threats to data security.

Several challenges are common to other organizations, but in this specific case, this sector faces a significant delay compared to other sectors (e.g. financial, energy, among

others) in terms of cyber security measures, making it an attractive target for cyber attacks [3]. It is extremely important to establish additional protective measures since compromising the health care provided to the patient can have serious consequences, even reaching the risk of life.

Some of the most significant challenges in the field of cyber security may jeopardize the protection of patient data and the integrity of systems, and arise from the following factors:

- **Absence or poor definition of policies:** sometimes, in organizations, only a few cyber security policies and procedures are defined, but they are not explicitly defined, giving the possibility of various interpretations by the stakeholders, and organization personnel.
- **Rapid evolution and use of technology:** Constant technological improvements make it difficult to keep up with new threats and weaknesses. As new technologies are used, hackers create new ways to exploit them, requiring the constant updating of hospital security. This requires an in-depth investigation and the timely taking of robust defensive measures against these risks [3].
- **Resource limitation:** Due to the budget limits of hospital institutions, investment in human and logistical resources dedicated to cyber security is scarce. In this way, it is more difficult to implement and maintain robust procedures and security measures. The computer attacks on hospitals are perpetrated by criminals, when they take advantage of outdated system (legacy) flaws, exploiting existing vulnerabilities [29].
- **Complexity of systems:** hospitals have several large systems that handle a large volume of data, and thousands of interconnected access points. This situation makes it extremely difficult to protect the vulnerabilities of each of them.
- **Lack of user awareness or experience:** The lack of information, training, and training of an organization's employees, or their little experience concerning cyber security can cause risky behaviors, such as using weak passwords, being the target of social engineering attacks, and opening or clicking on links in an email containing phishing.

- Technical or legal non-conformities: there are technical and legal regulations that are not complied with, that is, there is no total or partial compliance. One of the most recent cases is the Privacy and Data Protection Regulation (GDPR) [38] or Law 65/2011 [14].
- Increased use of Internet Of Medical Things (IOMT) equipment: The increased use of IOMT in hospital or residential environments, such as infusion pumps, vital signs monitors, medication dispensers, and ultrasounds, among others, present major challenges for the cyber security of health institutions. These are exposed to threats such as cyber-attacks, causing the theft of personal data, as mentioned by Le Bris [31], change of values, and/or even the interruption of systems.

## 4.2 Threats and Risks in Healthcare environments

There are potential dangers known as cyber threats, which can occasionally exploit vulnerabilities in a system or infrastructure. Hackers in general and cyber criminals in particular seek to identify flaws in systems, regardless of the motivation behind their actions, whether ideological, financial, or espionage. However, the causes of cyber threats may go beyond those that will be addressed, also including natural disasters such as earthquakes and fires. However, this study focuses specifically on cyber threats stemming from malicious actions. It is essential to recognize that cyber threats are not limited only to the digital world, but can have tangible impacts on the physical world and the day-to-day operations of organizations. It was only in December 2020 that Serviços Partilhados do Ministério da Saúde (SPMS) became part of the National Network of Computer Security Incident Response Team (CSIRT), with a team dedicated to cyber security.

Electronic health records and patient information cover not only medical history but also other important data. This information is crucial for proper treatment, providing indications for diagnosis and treatment, such as allergies or drug counter-indications. Information systems encompass appointment scheduling, patient follow-up, laboratory service orders and results, drug prescriptions, and smart health devices. Additionally, they cover non-medical technology systems such as institutional websites and management systems. The EU, through its agency ENISA [21], identified and analyzed cyber threats, actors,

impact, and trends in the health sector in Europe (hospitals, health centers, dental clinics, analysis laboratories, pharmaceutical laboratories, among others), as shown in Fig. 4.1, in the map of observed incidents.

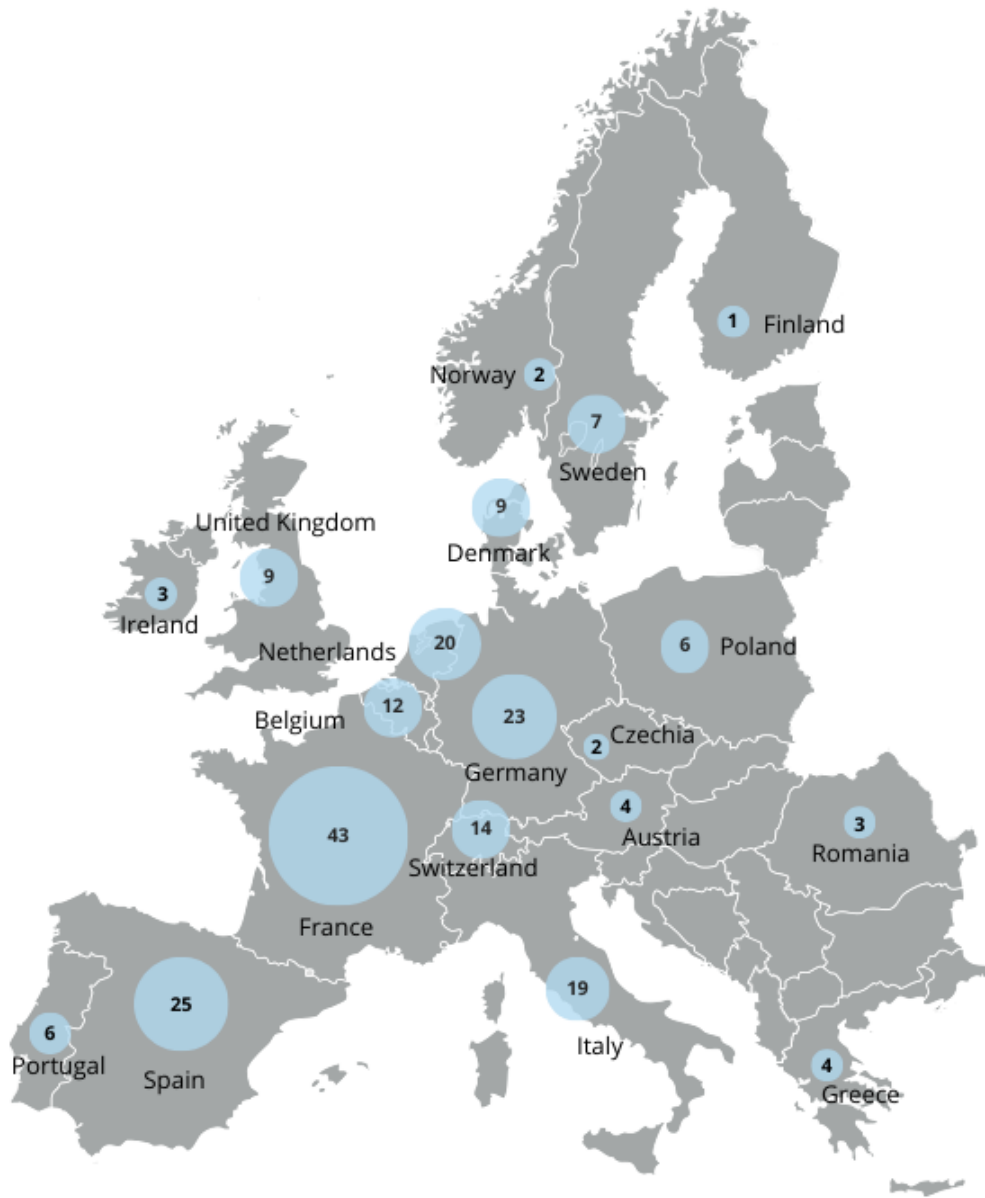


Figure 4.1: Map of observed incidents. Source: [21, p.8]

Overall, in accounting terms of the number of incidents, there were 91 in 2021, 84 in 2022, and 40 in Q1 2023, and it is not foreseeable that they are decreasing the number of attacks. In Portugal alone, the number of incidents was 6, with 2 incidents in 2021, and 4 in 2022, as Q1 2023 did not have any known incidents. In an analysis of the number of

incidents, the 5 countries with the most and the 5 countries with the least occurrences are listed in Tables 4.1 and 4.2.

Table 4.1: Top 5 countries with the most number of incidents

<b>Countries</b>	<b>2021</b>	<b>2022</b>	<b>Q1/2023</b>	<b>Total</b>
France	19	17	7	43
Spain	7	11	7	25
Germany	13	6	4	23
Netherlands	9	7	4	20
Italy	8	8	3	19

Table 4.2: Top 5 countries with the least number of incidents

<b>Country</b>	<b>2021</b>	<b>2022</b>	<b>Q1/2023</b>	<b>Total</b>
Finland	1	0	0	1
Rep.Czech	1	1	0	2
Norway	0	2	0	2
Romania	2	0	1	3
Ireland	2	1	0	3

Based on the report, concerning the number of incidents occurring in the health care provided to patients, covering hospitals, health centers, mental health clinics, dental clinics, and emergency services, among others, 53% of the total recorded incidents target health services. Within this context, 89 incidents occurred in hospitals, while 9 affected health centers or similar institutions.

As already mentioned, this July 2023 report refers to the period from January 2021 to March 2023, where it identifies the nine most frequent cyber threats, and the number of incidents related to these threats is shown in Table 4.3.

- **Ransomware:** is a type of attack in which cyber criminals encrypt the data looking for the payment of ransom to provide the key to decrypt. In this context, these incidents caused, according to the report, interruptions in services impairing medical care to patients (closure of emergency service and operating rooms).
- **Data threats:** Technically, data threats can mainly be classified as data breaches and data leaks. A data breach is an attack planned by cybercriminals to gain unauthorized access and reveal sensitive or confidential information. A data leak is

Table 4.3: Number of incidents related to threats in period 2021/Q1/2023

<b>Cyber threats</b>	<b>2021</b>	<b>2022</b>	<b>Q1/2023</b>
Ransomware	46	56	14
Threats against data	44	141	14
Denial-of-Service attacks	4	1	15
Malware	8	3	0
Social engineering threats	7	1	0
Supply chain attacks	10	3	2
Mistakes, wrong configurations, and incorrect security practices	8	1	0
Bad information or misinformation	2	0	0
Intrusion	7	15	5

the accidental disclosure of sensitive, confidential, or proprietary information due to misconfiguration, vulnerability, or human error. About half of the incidents (46%) referred to in this report involved sensitive information from health institutions

- Denial-of-service attacks: Accessibility is a frequent target of Distributed Denial-of-Service (DDOS) attacks. These attacks compromise access to systems and data, disrupting services through resource overload or disruption, compromising data availability. In 2021, due to the COVID-19 pandemic, several entities were unable to process data and refused services related to vaccination and testing due to this type of attack.
- Malware: It is unauthorized software that compromises systems, with types such as viruses, worms, trojans, viruses, rootkits, and ransomware. During the reporting period, 60% of malware attacks were ransomware, which led to certain pharmaceutical organizations experiencing downtime in drug production.
- Social engineering threats: covers activities that exploit human errors to obtain information or services, using tricks to deceive victims and access confidential data. This can be done by encouraging the opening of suspicious documents or access to unauthorized websites. This type of threat involves vectors such as phishing, fraud, and counterfeiting. In Europe in the period from 2021 to Q1/2023, some attempts were made to mine cryptocurrencies on hospital servers.
- Supply chain attacks: A supply chain attack involves the relationship between com-



panies and suppliers, requiring at least two types of attacks combined, and both suppliers and customers can be targeted. ENISA states in the analysis carried out that these attacks caused interruptions and incurred costs.

- Mistakes, misconfiguration, and incorrect security practices: Mistakes or misconfigurations can have major impacts. In the report of incidents in the health sector, the ENISA Cyber Security Incident Reporting and Analysis System (CIRAS) [19], 284 incidents were reported in 2022. System failure appears with 68%, followed by 16% for human errors and 16% for harmful actions, as we can see in Fig. 4.2.

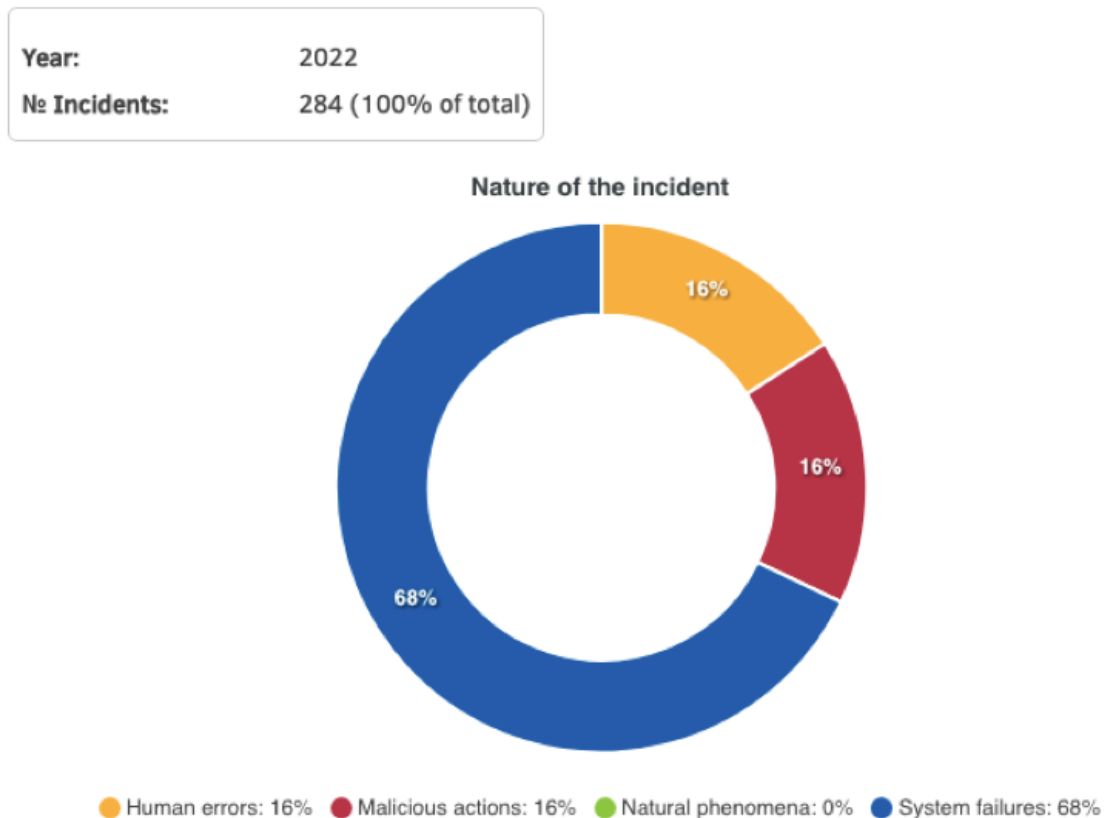


Figure 4.2: Nature of the incidents. Source: [19]

- Poor information/misinformation: these attacks seek to spread false information on the internet, taking the pandemic as an example, where during the vaccination periods topics such as health passports, mandatory vaccinations, and isolation were addressed. Such campaigns occur mainly on social networks and through phishing to

steal credentials and spread malware. According to the ENISA report [20], the theft of data related to the Pfizer/BioNTech vaccine by the European Medicines Agency has caused confidence in COVID-19 vaccines to decrease before their distribution.

- **Intrusion:** Intrusion attacks are improper access to the system, and obtaining administrator permissions that allow unauthorized actions to be taken. Generally, the presence of an intrusion is known, but the details of how it occurred are unclear.

The health sector worldwide has faced significant challenges due to several cyber attacks, many of them involving malware, especially ransomware, as evidenced in Table 4.3, and as can be seen in the Fig.4.3, and Fig.4.4. The following are some of the most recognized attacks, which have more detailed information:

- **Name:** WannaCry
  - **Target institutions:** NHS in the UK; Hospitals in Spain, India, the United States, China, and Russia, among others.
  - **Date:** 05/2017
  - **Vector:** EternalBlue Vulnerability Exploitation (Windows CServer Message Block (SMB))
  - **Vulnerabilities:** Vulnerability exploitation in the Windows SMB protocol (Shared folders). Fixed by Microsoft with patch MS17-010.
  - **Commitment:** caused interruptions, leading to the cancellation of surgeries, and difficulties in care, among others.



Figure 4.3: Example of WannaCry warning window asking for ransom. Source: [9].

- Name: NotPetya
  - Type: Malware
  - Target institutions: hospitals in Ukraine
  - Date: 06/2017
  - Vector: via fake MeDoc software updates
  - Vulnerability: Vulnerability exploitation in Windows SMB protocol
  - Compromise caused: caused interruptions, leading to the cancellation of surgeries, difficulties in care, and loss of data.
  
- Name: Ryuk
  - Type: Ransomware
  - Target institutions: hospitals in the US
  - Date: from 2018 to 2020
  - Vector: through phishing emails

- Vulnerability found: Unpatched vulnerabilities in systems and networks
- Compromise caused: hospitals with encrypted systems with high ransom requests for recovery and data access.

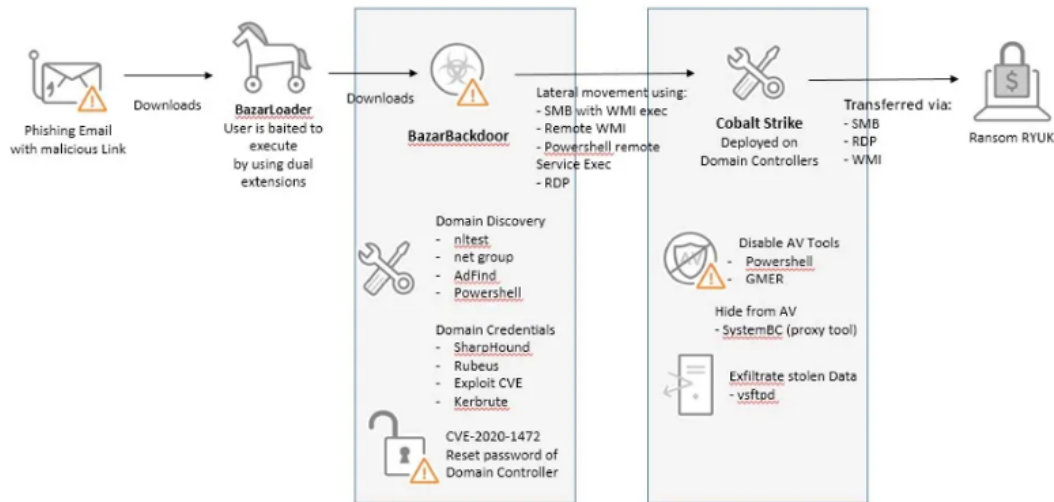


Figure 4.4: Example of Ryuk diagram attack. Source: [33]

- Name: DoppelPaymer
  - Type: Ransomware
  - Target institutions: Düsseldorf Hospital University
  - Date: 09/2020
  - Vector: exploited vulnerabilities of VPN systems
  - Vulnerability: CVE-2019-19781 on Citrix ADC (NetScaler ADC)
  - Compromise: System paralysis leading to the death of a patient.

In the health sector, and concerning cyber security, it is also necessary to know the risks. Risk, by definition [11], is “A reasonably identifiable circumstance or event, with a potentially adverse effect on the security of networks and information systems”. It is also known as the result of the product of the probability of a threat occurring, due to the impact it may have on the organization, and the survey of risks and their analysis will

allow the construction of a risk matrix, as already mentioned in Chapter 2 of this master's thesis.

Vulnerabilities of health organizations to cyber criminals have been exploited, and the pandemic has further intensified this threat by promoting teleworking, making home networks a vector for access to sensitive data [40]. In this context, a comprehensive approach to cyber security for healthcare institutions is recommended, incorporating not only technical measures but also process and risk management considerations, exemplifying the Resilience Management Model (CERT-RMM) [42] and the integration of cyber security into strategic planning and budgeting. It is essential to emphasize the potential consequences of a cyber security breach on health, including the exploitation of vulnerabilities in medical devices that compromise clinical care and the exposure of sensitive patient information, as well as the risks of identity theft, adverse health effects, and, in extreme situations, loss of life, making ransomware attacks particularly prominent for their ability to impact access to essential systems and data [53].

### 4.3 Critical Services and Systems in Healthcare

There are several critical systems in a hospital, and it is certainly difficult to find a definition of which service is considered most critical. From employee to employee, regardless of function or department, the notion of criticality or importance varies. A safety failure in the emergency department may be more severe than in the operating room or intensive care unit. The systems that handle business data are also very important, as they support the areas of planning, production, finance, accounting, and the administration of the hospital unit itself. Usually, the systems are installed locally on servers in the datacenter, or on servers under the responsibility of the Shared Services of the Ministry of Health (SSMH). In both cases, it is necessary to take certain protective measures. Hence, it is also necessary for hospitals to have business continuity and disaster recovery plans.

Healthcare institutions should implement robust security measures such as firewalls, antivirus, encryption, restricted access policies, strong authentication, and continuous monitoring [43], among other measures, to protect their IT systems, as well as patient and employee data. Furthermore, investing in cyber security awareness programs for

healthcare professionals and other employees is crucial to creating a culture of IT safety and responsibility. Collaboration between healthcare organizations, technology providers, and regulators is vital to develop best practices [17] and ensure the use of internationally recommended safety standards. Only by harnessing synergies will it be possible to address safety challenges and ensure a safe and reliable environment for the delivery of quality healthcare.

The quality of the Information Technology (IT) infrastructure is also crucial to ensure the excellence of IT services. Infrastructures encompass resources and associated services used to provide and support large portions of IT services, such as hardware platforms, software applications, operating systems, networking, and telecommunications tools. Information security implies that the IT infrastructure has adequate configuration management, change management, records, and monitoring.

Configuration management aims to maintain an up-to-date inventory of IT assets and the interactions between the different components. Efficient configuration management drives vulnerability management and security updates. Change management, defined by Information Technology Infrastructure Library (ITIL) as a systematic approach serves to deal with all changes in a standardized way, avoids unnecessary interruptions in services, and proves valuable during a cyber attack. Rigorous audit logs and the monitoring of log records play an emerging role in quickly detecting attacks and obtaining pertinent details about them.

Recently, there has been a push to promote cyber security as a value proposition among medical device manufacturers, encouraging them to value and sell it as an asset. For example, the U.S. Food and Drug Administration (FDA) requires medical device manufacturers to demonstrate the ability to apply security updates and patches throughout the life of the device, as well as to promote the analysis and mitigation of any device problems that may have undesirably affected patients. While these measures place the responsibility on manufacturers, the most implicated and proactive cyber security approach should not be limited to them, but should also be adopted by healthcare institutions. Hospitals should invest in prevention by assigning resources and budgets early on, rather than relying on reactive approaches after the attacks, even considering the history of under-investment in human resources and funding in hospital information

security.

The implementation of the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP) brings a set of advantages to health institutions. While BCP ensures business continuity, that is, allows essential medical services to be served while minimizing operational impacts, DRP focuses on recovering data and systems, reducing downtime, and preserving operational integrity. The implementation of these plans strengthens risk management and compliance with regulations such as patient data protection, preparing staff for coordinated reactions during crises [52], and accelerating effective responses. In summary, benefits span business continuity, agile recovery, risk management, and compliance, empowering healthcare institutions to meet unforeseen challenges confidently and effectively. The life cycle of the BCP can be plotted as in the diagram represented in Fig. 4.5.

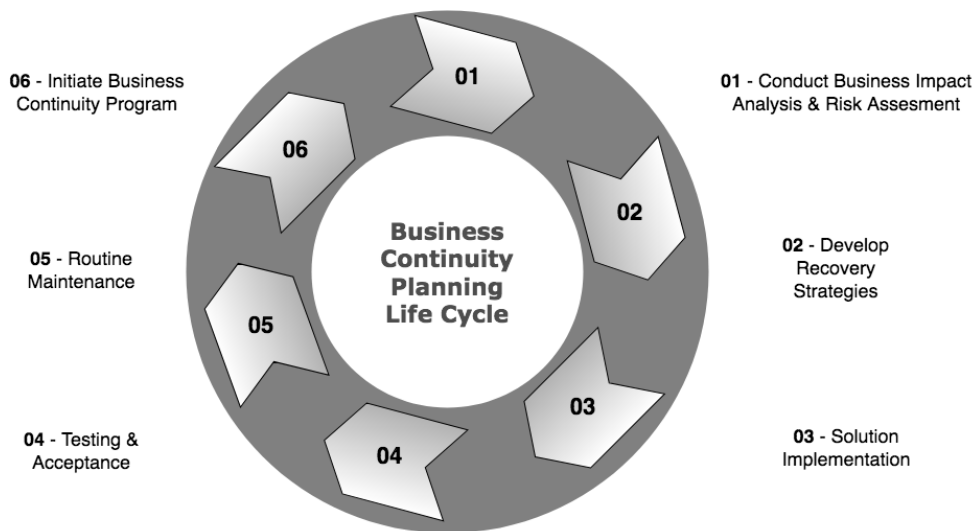


Figure 4.5: Business Continuity Planning Life Cycle. Source: The author

## 4.4 Cybersecurity Best Practices in Hospitals

Good cyber security practices in a hospital, or to implement mitigation measures, aim to increase the security of systems, networks and minimize vulnerabilities, and reduce existing risks, through the taking of several measures, including:

- Risk Assessments: Conduct regular risk assessments to identify vulnerabilities and

prioritize security measures.

- Access controls: Implement strong access controls such as multifactor authentication and permission-based access.
- Network segmentation: Network segmentation plays a crucial role in cyber security by strengthening the safeguarding of information technology systems. By dividing the network into isolated segments, it is possible to reduce exposure to threats and mitigate the impact of attacks. This approach preserves the confidentiality of sensitive data, simplifies the monitoring and detection of suspicious activity, and contributes to regulatory compliance. The segmentation facilitates maintenance and updating procedures, reinforcing the overall resilience of operations.
- Training: administering regular cyber security training to hospital employees, as well as disclosing some of the threats, also serves to raise awareness of best practices [17], according to guidelines from the hospital's cyber security officer.
- Updates: regularly update and patch software and other systems to address known vulnerabilities through security patches. Update whenever possible the hardware firmware, especially the one related to the protection of the various perimeters.
- Security audits: conducting security audits, have to be carried out regularly to find the weaknesses, and realize there are new flaws.
- Response plans: Implementing response plans is a cornerstone of good cyber security practice. These plans define clear procedures to address threats and incidents, minimizing impact and ensuring coordinated action. By anticipating risk scenarios, response plans strengthen recovery capacity and reinforce the organization's resilient posture.
- Management tools (prevention, detection, and response): the use of software to assist in the prevention and detection of security events, IDS/IPS, SIEM, and EDR, among others. Hospitals can set up automatic alerts and responses to quickly mitigate threats and minimize the impact of cyber attacks.



## 4.5 Cybersecurity Skills Trend

Specialization in cyber security sets a marked trend, as organizations look for professionals capable of facing complex challenges arising from the expansion of digital ecosystems and the improvement of threats. The convergence between technical and strategic proficiency emerges as a distinct aspect, with skills in ethical hacking, threat detection, and encryption being the most valued. This demonstrates the importance of professionals' ability to face threats and guide risk management strategies. These days, cyber security experts collaborate with lawyers, data scientists, and other compliance experts. Adaptability plays a crucial role in protecting and strengthening resilience in the face of ever-evolving threats.

However, it appears that there is a large and diverse number of educational formations in the market. Some low-cost online, but without great appreciation. Others are internationally recognized, but at a very high cost (Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Computing Technology Industry Association (CompTIA), Certified Cloud Security Professional (CCSP), among others). The Technological Specialization Courses referred to in the Cyber Security in Portugal - Society 2021 Report of the Cyber Security Observatory, states that only 11 Cyber Security courses exist in continental territory [12].

There are other formations at the higher education level, with the offer of several courses such as Professional Higher Technical Course (CTeSP) of 2 academic years, postgraduate courses (non-degree conferring) of 6 months to 1 academic year, master's degrees (degree conferring) of 2 academic years, and doctorates (degree conferring) with 4 academic years, in public or private educational establishments, but which still do not have due recognition by the institutions. In a study on Post-secondary and Higher Education in Cyber Security carried out by the CNCS [54], dated April 2022, not counting postgraduate courses that do not confer a degree, there are only 23 undergraduate courses with cyber security content in public education (polytechnic and university) in mainland Portugal, and Master's degrees in public education total 25.

Finally, it should be noted that the number of students who completed courses successfully, in the academic year 2019/20, with curricular units in cybersecurity, were: 79

CTeSP, 6 degrees, 65 masters, and only 1 with a doctorate.

# Chapter 5

## Research

This chapter consists of 3 sections. The first section presents the methodological framework used to explore and understand the state of implementation and use of a security system, as well as SIEM in a hospital context. Through a qualitative approach, data were collected in a survey and made available through a questionnaire, which serves as the basis for the analysis carried out in this study. The scope of the research describes the selection criteria of the participants and details the flow of the necessary procedures. In the second section, there is an overview of the survey, as well as the results, the analysis carried out, and the consequent discussion regarding the findings, that is, some of the possible conclusions about the answers given by the participants. In the third section, the results from 4 interviews conducted with SNS professionals in management positions are presented. In these interviews, questions were asked to understand the perspective of these professionals and according to the view of senior management.

### 5.1 Research Methodology

#### 5.1.1 Research Approach and Design

The qualitative research model offers several approaches to exploring and understanding social phenomena, retaining participants' individual experiences and perspectives [7]. The qualitative approach provides a direct understanding of the opinions of the participants, revealing some considerations, even by the words used, that are specific to the study groups, which are often neglected in more deterministic documents. Through diverse data

collection and analysis techniques, qualitative research involves coding, categorization, and interpretation to identify themes and patterns [23], encompassing the understanding of complexity, details, and context [34]. However, adopting a qualitative approach means refusing to conceptualize a research design as a single document that is a comprehensive plan before a study [22].

The central problem that is expected to be understood is whether the employees with direct responsibility in the implementation and use of a SIEM in a PBE-type hospital have the necessary conditions and knowledge and whether they are using this tool effectively. In this context, we seek to analyze whether professionals are adequately trained to operate the SIEM system and whether they are applying its features to ensure information security in the hospital environment. Understanding this issue is crucial to assess the impact of SIEM implementation and its effectiveness in managing safety information in the hospital. The investigation also aims to identify any challenges or obstacles that may be limiting the effective use of SIEM by employees. By exploring this central problem, we seek not only to verify the presence of SIEM but also to analyze how it is integrated into the routine of employees to help organizations improve information security.

At the origin of this study, several questions arose to understand whether SIEM are implemented and how important it is to use them in a hospital institution. The vulnerabilities of information systems in the hospital context, in particular PBE hospitals, in the face of growing cyber threats that compromise the security of patient data and the continuity of services. The lack of human and logistical resources in the SNS makes the implementation and use of SIEM difficult. With so many difficulties, it is legitimate to reflect and formulate the following questions:

- Is the investment in cyber security in the health sector, in particular in PBE hospital units, enough?
- Do boards see cyber security as a priority and fundamental?
- Do hospitals not have a SIEM in place due to the high financial costs they represent?
- What are the biggest difficulties faced by teams responsible for hospital cyber security?

- Are SIEM implementations difficult and unfriendly tasks, or do they just require some time, dedication, and technical knowledge?
- Do the elements involved in cyber security believe that a SIEM can be an asset or, on the other hand, it does not add value?
- What will a SIEM of the future look like, and what improved or new features will it have?

The general objective of this investigation is to interpret and characterize PBE hospital units concerning their cyber security maturity, particularly through the implementation and use of a SIEM. However, there are some more specific objectives, in particular:

- Characterise the perspective of decision-makers and direct stakeholders in the cyber security of a hospital regarding the investment that is made by the SNS.
- According to the view of the stakeholders, characterize the need and importance that may or may not have to the implementation of a SIEM;
- List some of the use cases in which the uses of a SIEM were fundamental to prevent or contain any cyber threats;
- Identify the measures taken for the development of this type.
- Identify some of the future improvements of a SIEM to increase the safety of a hospital unit;
- Understand the state of cyber security maturity of PBE-type hospitals, namely through the implementation and use of SIEM.

### 5.1.2 Data Collection Methods

The method chosen was qualitative, to obtain an approach to the main problem, that is, a rational approach to the question. Thus, given the geographical distribution of the hospital units and their employees (chosen participants), it was decided to collect data through a questionnaire survey. In the planning of the survey, according to several authors such as Brito (2012) [6] and Hill (2014) [28], it was essential to previously define the

problem, the objectives, the study hypotheses when necessary, as well as the method, the study population, and the sample. Qualitative research involves the formulation of open questions designed by researchers, according to Braun [5]. Subsequently, these questions are made available to participants in a self-administered manner, following a predefined and uniform sequence. Qualitative responses obtained through research questions that require textual responses have the possibility of being gathered and examined directly from the export of data (in the case of online surveys) or other documents (in physical surveys).

A survey, depending on the problem, method, questions, and research objectives, is a data collection [15] strategy that aims, through a systematized set of questions, to obtain answers from a given study population, according to Ghiglione [26]. Although it presents challenges in the analysis due to its complexity, it contributes to investigations, addressing "why" and "how" questions. Surveys seek to understand perspectives, opinions, and attitudes, analyzing responses in detail to formulate hypotheses. They are excellent for understanding points of view and more effective with small samples, being crucial for identifying weaknesses in organizations. The electronic questionnaire, as a type of application of the instruments, for inquiry, has, according to Carmo and Ferreira [8], and Sousa and Baptista [51], pros and cons, namely:

- Pros:
  - Easy administration
  - Fast
  - It can reach the entirety of the target audience. The participant responds when it suits them.
- Cons:
  - Some digital literacy required
  - Internet access is required
  - Requires motivation to respond

The survey with 10 open-ended questions was made available through an online Microsoft Forms page designed specifically for this purpose, the header is shown in Fig. 5.1.

## SURVEY - Implementação de System Information and Event Management em Hospitais/C.H /ULS/IPO E.P.E

Viva! Preciso apenas de 10 minutos da sua atenção para preencher este questionário. Ele surge no âmbito da minha dissertação de Mestrado em Cibersegurança no Instituto Politécnico de Viana do Castelo, subordinada ao tema: "*Analysis of Implementation of a Security Information and Event's Management System in E.P.E Hospitals*". O preenchimento do questionário deverá ser efetuado (preferencialmente) até 25/07/2023 (Nova data max. 12/08/2023).

O objetivo principal deste estudo é analisar a implementação e uso de *Security Information and Event Management* em hospitais públicos do tipo E.P.E. O estudo visa identificar a importância da cibersegurança para os hospitais, os desafios na implementação de um SIEM, bem como a sua mais valia, e conhecer a visão dos intervenientes para o futuro deste tipo de sistemas. Espera-se que este estudo sirva como um ponto de partida para otimizar determinadas estratégias e sistemas, a fim de melhorar a cibersegurança no setor da saúde.

A sua colaboração neste projeto será muito útil. Desde já, será garantido sob compromisso de honra, o anonimato dos dados pessoais e institucionais dos participantes, a fim de preservar a confidencialidade.

Obrigado!

Emanuel Gonçalves  
e.goncalves@ipvc.pt

Figure 5.1: Survey header. Source: The author

The questionnaire for each participant is composed of 10 questions and divided into 4 distinct domains, namely: investment in cyber security, implementation of SIEM, use cases, and forecasting for the future, such as:

- Investment in Cyber Security: To evaluate the degree of relevance attributed to cyber security in a hospital environment, as well as investigate the allocation of human resources, hardware, and software specifically aimed at this purpose, this study aims to understand the recognition of the hospital unit concerning cyber security and the existence of concrete investments in these areas.
- SIEM implementation: this domain was created to understand if there is expertise in this area within a hospital context, if it is ongoing, or if this activity is planned.
- Use cases: use cases are important to understand if the effective uses of a SIEM have already been useful for the health institution, that is, if they have already served to

detect and provide data, to mitigate vulnerabilities, reduce risks and even detect an attack or intrusion, for example.

- Forecast for the future: The way stakeholders predict the future of SIEM use, to perceive whether they believe there will be an alternative tool, a complementary, or frankly a completely different one, but more efficient and proactive, with the adoption of processes linked to artificial intelligence.

### 5.1.3 Sampling Strategy and Participants

The strategy of the sample used, given the number of human resources, in this area of information technologies/systems and cyber security, being very variable from hospital unit to hospital unit, was to contact by email and WhatsApp, the participants of the various PBE hospital units, to facilitate contact, response, as well as collection and consequent analysis.

The sample selection addressed the variability in human resources dedicated to information technologies/systems and cyber security in PBE hospital units, using communication via email and WhatsApp to speed up contact, obtain answers, and collect data. This approach involved a wide range of professionals, including information systems, cyber security, and hospital management, eliminating the need for physical travel. The data collected will be analyzed to determine the understanding of the implementation of SIEM in PBE units in Portugal, referred to previously in Chapter 3.

Survey participants are IT directors, Chief Information Security Officer (CISO), and system administrators. As in some cases, the IT director accumulates functions with the role of CISO, it was decided to create its category. Since two of the participants' roles, namely the CISO and the IT Director/CISO (where the IT Director, accumulates roles as CISO), had identical questions and both received a reduced number of responses in the survey, it is considered that the combination of these two categories is an appropriate approach. In this context, merging similar categories can bring several advantages, including more robust representativeness, consistency, and more accessible analysis, all while preserving anonymity. However, despite the aggregation, it was ensured that the data and evaluation were not compromised.



#### 5.1.4 Data Analysis Techniques

The information was collected, read, and classified to be integrated into a database created for the research in question. Data preparation, especially response coding, was performed following analysis criteria for each response, as well as a qualitative assessment. Subsequently, this data was converted into numerical values to be entered into the evaluation grid. The four criteria formulated for this study were as follows:

- **Relevance of the answer:** the evaluation of the relevance of the answers to the research objectives to guide the selection of essential information.
- **Accuracy and clarity:** the search for concise and transparent answers contributes to the accurate understanding of the data presented.
- **Scope of the response:** the consideration of the breadth of the responses offers a complete view of the topics covered, enriching the analysis.
- **Coherence and consistency:** The evaluation of the harmony and consistency of the responses ensures the integrity and reliability of the results obtained.

The evaluation was translated, according to the criteria already mentioned, into the following correspondences:

- **Excellent (4 points):** Very relevant, precise, clear, comprehensive, and coherent response;
- **Good (3 points):** Relevant, precise, clear, comprehensive, and coherent response;
- **Satisfactory (2 points):** Partially relevant, accurate, clear, comprehensive, and coherent response;
- **Poor(1 point):** Unrelevant, inaccurate, confusing, limited, and inconsistent response.

Based on the assessment, the objective will be to complete an assessment grid, for each participant's response.

The ethical considerations considered in this study were the privacy and confidentiality of the participants. These were ensured throughout the entire process, from the beginning

of the study, as indicated in the header of the questionnaire itself, any data provided or connections with the participant's hospital unit were treated with discretion within the scope of the study. From the beginning, it was exercised with care so that there was no reference to certain details to protect the secrecy of each hospital unit surveyed. Therefore, the following personal information was never requested: participant's name, contact number (mobile or landline), email address, and address. In this study, although the identification of the participant's health institution and position was requested, this relationship is not mentioned in the results for privacy reasons.

## **5.2 Research Findings and Analysis**

### **5.2.1 Overview of the Research Results**

In this context of analysis and implementation of a SIEM in hospital environments, the research offers a comprehensive view of the results of a survey aimed at employees with direct responsibility. The participation included a total of 21 participants, among whom 11 are IT directors, 2 are IT directors and CISO, 3 are CISO, and 5 are system administrators, representing a comprehensive sample of the 43 health facilities in question, as seen on in Fig. 5.2.

In the questionnaire, no contact data was collected, whether email addresses, telephone, mobile phones, home addresses, or the names of the participants. This ensured that the minimum collection needs were met and that they complied with all the rights of data subjects under the GDPR.

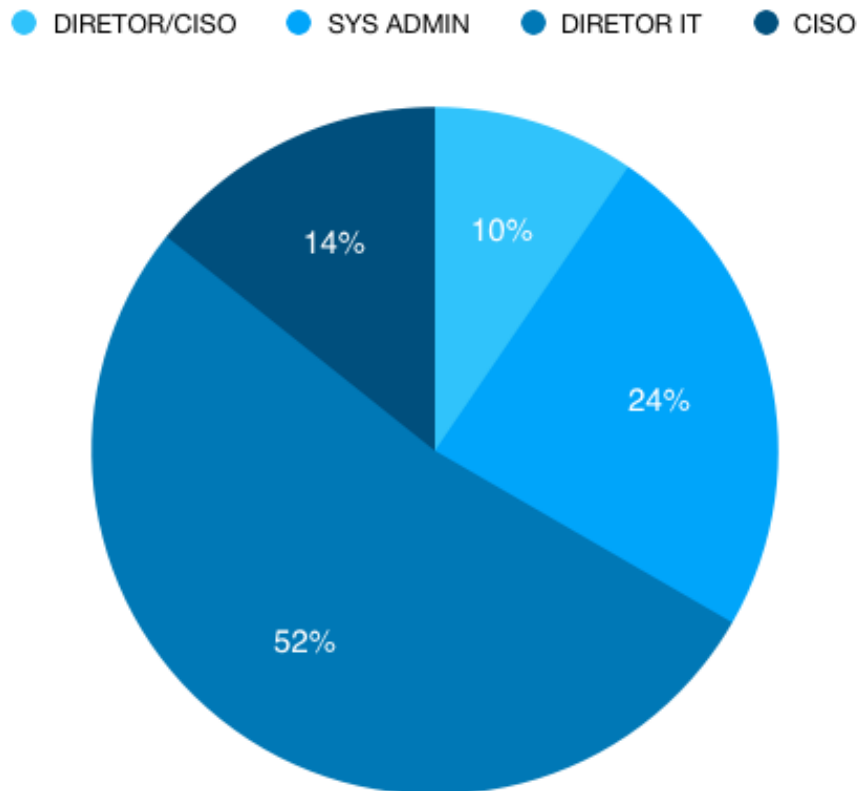


Figure 5.2: Percentage of survey participants chart. Source: The author

### 5.2.2 Analysis of the Survey Responses

To ensure the confidentiality and security of the hospital units addressed in the questionnaire, this study avoids making any reference that establishes links between the function of the participants and the units in question, in order not to compromise their integrity. Therefore, it is not feasible to determine which units participated and, likewise, it is not possible to identify the specific answers that each of them provided for each question asked.

Data analysis aims at organizing, structuring, and extracting meaning from the information collected in the research. Transcriptions, according to (Morse 2016). [36], require repeated reading, followed by organization, integration, and interpretation. However, the great challenge is to summarize the data, seeking to reduce it.

From a total of 43 hospital units of the (PBE) type, already mentioned above, one or more employees responded to 14 of them. In particular, employees from 2 Hospitals, 8 Hospital Centers, 3 ULS, and 1 IPO responded, as shown in Fig. 5.3

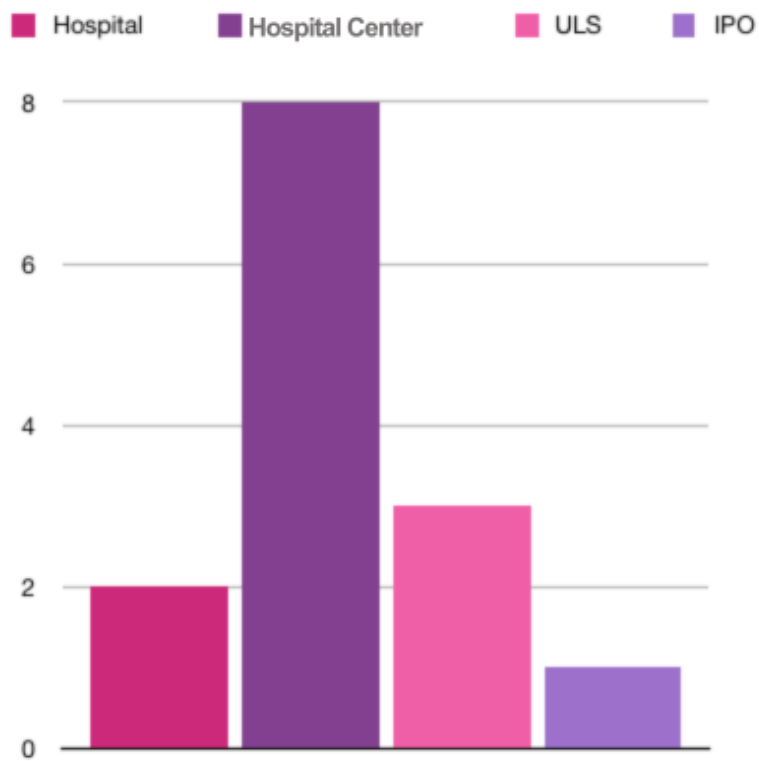


Figure 5.3: Number of hospital units by type that responded to the survey. Source: The author.

Analyzing, it is possible to verify that, according to the reference criteria, the directors of the IT departments have a greater consensus on issues Q1, Q3, Q4, and Q5. This means they agree on the importance of cyber security for hospitals, considering that cyber threats are increasingly prevalent. Additionally, they believe that the implementation of a SIEM contributes to better safety and resilience of hospitals, as can be seen in Fig. 5.4

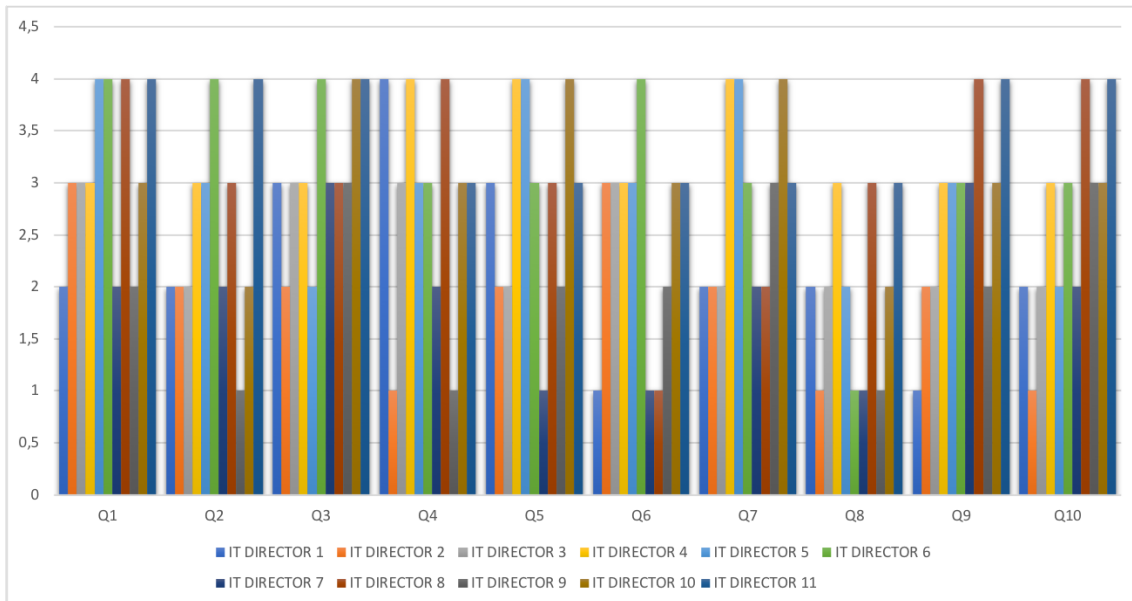


Figure 5.4: IT Director chart answer classification. Source: The author.

However, regarding the effective implementation of a SIEM and its impact on the organizations that already use it, the responses were less clear, coherent, and comprehensive. This suggests that there may be some ambiguity or lack of consensus between the IT directors and CISO on how exactly SIEM is being implemented and what the observed results are in the organizations that employ it, as can be seen in the Fig. 5.5

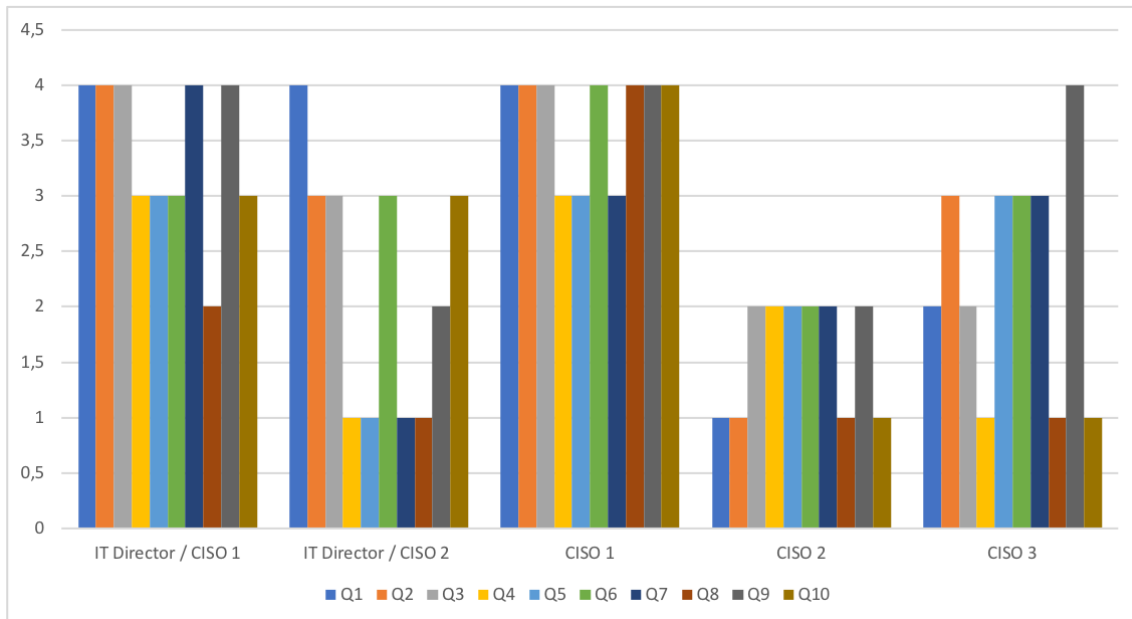


Figure 5.5: IT Director/CISO chart answer classification. Source: The author.

Regarding the more reasoned opinion of IT Directors who also perform functions as CISO, questions Q1, Q2, Q3, Q6, and Q9 receive a higher score, according to the evaluation performed. This means that they consider the implementation of a SIEM in hospitals crucial and demonstrate knowledge of the main associated challenges. Furthermore, they have expectations regarding the future of cyber security in the Portuguese NHS.

While recognizing the need to implement a SIEM, most have never done so and have limited information on practical situations where SIEM has contributed to countering cyber threats.

System administrators have a more technical and operational-centric approach. However, since most have not yet effectively adopted a SIEM, due to the use of other different or alternative solutions to SIEM, the most relevant answers focused on questions Q1, Q8, Q9, and Q10, as can be seen in the Figure. 5.6. These questions are those in which the other participants also demonstrate greater familiarity, addressing the relevance of cyber security and the use of tools such as SIEM. Additionally, they point to a growing future need to adopt these solutions, and artificial intelligence could optimize the cyber security of hospitals.

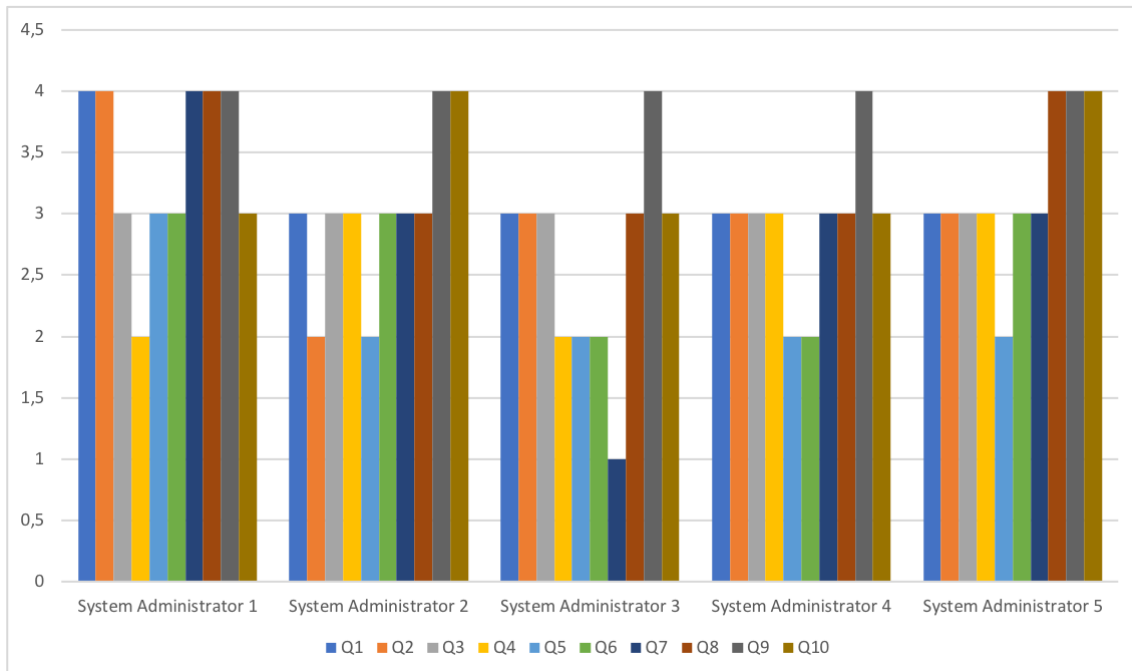


Figure 5.6: System administrator chart answer classification. Source: The author.

Based on the answers offered for questions Q4, Q5, Q6, and Q7 which showed less clarity and consistency, it is possible to infer that the respondents have a less in-depth understanding of SIEM. However, they recognize the SIEM potentialities and look positively at its implementation in hospitals.

### 5.2.3 Discussion of the Findings concerning the Research Questions and Objectives

Within the context of the master's thesis, the analysis of the results seeks to understand the implications of the findings concerning the research questions and the previously established objectives. Thus, the results will be presented according to the specific purposes of each question, allowing a comprehensive and in-depth approach to the research. Additionally, this discussion offers valuable points of view for a critical evaluation of the responses obtained, and for the contextualization of the findings within the scope of the investigation (hospital units)

- Question: How important is an investment in cyber security?

Concerning investment in cyber security in hospitals, the results indicate that participants, from most institutions, recognize, regardless of their function, the importance of cyber security, as this sector has increasingly suffered some attacks.

- Question: How is the participant's role involved in planning and implementing cybersecurity measures?

In this question, which investigated the participation of those involved in the formulation and implementation of cyber security measures, it is observed that there is often a consultation of the needs for improvement and resilience of hospital units. This process, in general, begins with suggestions from the technical teams, which are later forwarded to management for validation and consequent investment.

- Question: What is the participant's opinion on implementing a SIEM?

As for implementing a SIEM in a hospital and the associated benefits, the prominent conclusion is that critical hospital services can be impacted in the event of an incident, impacting both the quality of patient care and organizational functioning. With the increasing digitization and interconnection of hospital services, vulnerabilities and threats also increase, making it essential to adopt preventive and protective measures, such as the implementation and use of a SIEM.

- Question: What is your experience implementing a SIEM?

On this question, through the analysis carried out, it appears that most participants have never implemented or assisted in the implementation of a SIEM. However, those who have done so, indicate that such an initiative has proved crucial in strengthening cyber security and protecting sensitive information assets, ensuring the integrity, confidentiality, and availability of patient data and hospital operations. The implementations of a SIEM constituted complex projects that required planning, technical knowledge, and continuous commitment.

- Question: Do you consider that the implementation of SIEM contributes to improving the security of systems and the privacy of patient or employee data?

Concerning the fifth question, with the protection and privacy of patient data, as well as the possibility of a SIEM contributing to this safeguard, it can be stated



that, although most consider a SIEM as an asset when dealing mainly with threats, compliance with the GDPR is not explicitly mentioned. Many SIEM offer solutions in the market to meet these regulatory requirements.

- Question: Does the organization you work for now have a SIEM set up?

This question received detailed responses from a few participants. Some claimed not to have such tools in their organizations, while others mentioned having similar or complementary tools. A limited number indicated having implemented and using such tools. However, most participants who do not have a SIEM implemented, and intend to present technical solutions to their administrations, aiming at their implementation in the near or medium-term future.

- Question: What are the main challenges in implementing a SIEM?

In the seventh question, the main challenges and difficulties related to the implementation of a SIEM were explored. Among the few answers that proved to be clear and practical, the participants highlighted the behavior of licensing in the acquisition and services. Furthermore, the parameterizations or configurations of the system, play a crucial and challenging role in the implementation. The need for more human resources has also been referred to as an imperative need and, if there are no hires, it can also bring difficulties. However, given that many have never been involved in implementations or lack experience in this area, their responses followed that conclusion.

- Question: Do you have any examples of use cases where threat identification was made possible by SIEM?

Asked about use cases, where SIEM implementations have been a determining factor in threat detection and containment, most participants do not have a formed opinion, as they are unaware of situations in which this has occurred.

- Question: What are your expectations for the future of cyber security?

Expectations for the future differ according to the function performed, but in general, they are quite optimistic. It is believed that the recent incidents that affected some Portuguese hospitals may act as an alert for other hospital units and SNS

institutions. This may, in turn, may encourage additional investments in the area, aimed at improving preventive measures in the field of cyber security.

- Question: Do you believe that the contribution of Artificial Intelligence (AI) can be an enriching factor for cybersecurity?

This question, which questioned whether the use of artificial intelligence in cyber security could make a significant contribution, was answered by the majority, and in a very positive way. That is, they believe that AI can play an important role in freeing human resources from tasks, detecting and responding much faster when cyber threats exist, as well as identifying vulnerabilities in the organization's devices.

The analysis of the results concerning the research questions, and the objectives outlined, substantially emphasized the fundamental importance of implementing a SIEM in hospital environments. By identifying the challenges faced, as well as the benefits observed and the prospects outlined, a comprehensive panorama emerged that can guide decision-making. This study provides essential guidelines for the continuous evolution in the field of hospital cyber security.

### 5.3 Managers Interviews

In addition to the questionnaire developed to acquire answers of a more technical nature, interviews were conducted with four representatives who occupy management positions in various entities of the Portuguese NHS, known as SNS, to gather perspectives on issues deemed relevant. These interviews, all of them authorized, were conducted as follows: two by face-to-face meetings and two by email.

- Member of Board - Clinical and Health Council of ACeS Gerês/Cabreira at ARS de Saúde do Norte, I.P. (Personal interview)

- Q1 - Do you consider cyber security important in the health sector?

- Yes, it is important. Cybersecurity is now a priority, addressed both individually and in the professional context. The protection of data and systems in the health sector is key to ensuring the confidentiality and quality of care.

- Q2 - Do you consider that the health sector, in particular the ACeS, is well protected in terms of cyber security?

I believe that clinical data is well protected, and currently, the servers are under the management of SPMS. However, occasionally mistakes can occur, such as sending emails. Another situation happens due to the diversity of applications, and the management of different passwords may not be the best. Furthermore, there are tools necessary for the activity that are not made available by the services, and others are used unofficially to overcome this difficulty. As for data protection, there is greater knowledge and maturity, since even in court requests, we do not transfer data without prior verification and validation.

- Q3 - Is the training given or provided to ACeS employees sufficient?

I think there should be more training for professionals. There are some documents in the official repositories and recommendations made by "ARS Norte", but there is no obligation to read, validate and remember the concepts, for example, annually. There is a certain sensitivity, but this is mainly based on what is generally disseminated by the media regarding the care to be taken.

- President - Board of Directors of Hospital de Braga E.P.E (Personal interview)

- Q1: What is your opinion on the importance of cybersecurity for a hospital?

Cybersecurity is a vital component of an institution's security. In the case of hospitals, it takes on even greater significance due to the volume of health data that is processed within information systems.

- Q2: What is the hospital's policy regarding investments in cybersecurity and how is it defined?

The investment policy is defined in collaboration with the information systems management, taking into account the identified vulnerabilities.

- Q3: How is the hospital's senior management involved in the cybersecurity decision-making process? Is the IT/Information Systems (IS) department and/or external vendors involved?

The Board of Directors makes decisions based on technical information gathered by IT professionals, who in turn consult with vendors.

- Executive Member – SPMS Administrative Council (Email interview)
  - Q1: SPMS are responsible for much of the cyber security of hospitals. However, do you consider that Portuguese hospitals, in general, have a high level of maturity on this topic or is there still a long way to go?

SPMS, PBE's mission is to provide specific shared services in the area of health in terms of purchasing and logistics, financial services, human resources, information and communication systems and technologies, and other complementary and subsidiary activities, to all SNS establishments and services, regardless of their legal nature, as well as to the bodies and services of the Ministry of Health and any other entities when carrying out activities in the area of health. Given its duties about information and communication systems and technologies, cyber security and information security matters are of great importance, not only because of the sensitive and personal information that the sector deals with, but also because in situations of cyber security incidents, the impacts are likely to affect the provision of health care.

SPMS has been taking an active role in cyber security matters through awareness, training, and capacity building of health institutions. It should be noted, however, that SPMS is not responsible for cyber security in hospitals, which are responsible for ensuring an information security and cyber security management system that involves governance, processes, people, and technologies.

Cyber security in the health sector is a challenge, not only because of the criticality of electronic health data that must remain confidential, with its integrity preserved and be made available where and when necessary but also because the attack surface that a hospital has is comprehensive, considering all supply chains, partner networks, infrastructures, medical devices through IoT, among others. Another difficulty of the sector is the false (abstract) perception of the connection between cyber security and the safety of users since the impacts of cyber security incidents do not seem to immediately present damage or mortality in users, however, there are more and more examples that contradict this perception, highlighting the importance that has been given to cyber security

in the health sector.

- Q2: In your opinion, do you believe that the implementation of a SIEM can improve the security of systems and information in a hospital?

A SIEM can improve the ability to detect cyber security events and incidents in a hospital, and consequently the information security of a hospital, however, this technological platform will have to be supported by adequate governance, processes, and people.

It is considered that the implementation of a SIEM in a hospital alone may not represent improvements in the security of systems or information, since at an early stage it will be necessary to ensure that the infrastructures, networks, and information systems are collecting the relevant information and events that can be analyzed and correlated in the SIEM. It is also necessary to ensure that there are the necessary and adequate resources to parameterize, interpret, and develop the appropriate actions with the information provided by SIEM, at the risk of creating a false perception of security.

- Q3: What advice would you leave to those responsible for hospital cyber security regarding the future implementation of an SIEM in organizations?

SIEM is an excellent technology to aggregate relevant data from various sources, identify deviations from normality, and support decision-making, and its implementation must be supported by a 360<sup>o</sup> strategy, culture, and level of protection and safety, including adequate processes and people.

- Member of the SNS Executive Board - (Email interview)

- Q1: Do you consider that the logistical and human resources dedicated to cyber security in the SNS, in particular in hospital units (hospitals, hospital centers, ULS, and IPO) are satisfactory?

At the moment, there is a big bet on cyber security in all state entities. In each of its institutions, the SNS has services that work on the risk and exposure of health data. They have not yet reached the optimum point, but they have been working to make it happen.

- Q2: Do the reforms you intend to implement in the SNS include measures that seek to increase cyber security for the health sector? If so, what are they?

Cyber security is a bet of SPMS, SSMH, with the technical competence for this development and monitoring, either centrally or individually, in each SNS institution.

- Q3: It appears that many of the occurrences that affect and compromise confidentiality, integrity, and availability happen due to a lack of information/-training of SNS employees on good practices, regardless of academic training or computer literacy. Is there any training plan for the future of the SNS to improve this gap?

There is a training plan that accompanies the implementation of the actions.

### 5.3.1 Implications and Recommendations for Healthcare Organizations

Considering the survey-based research focused on the implementation of a SIEM in hospital environments, relevant guidelines can be identified. Based on the results obtained, health organizations can consider the following implications and recommendations:

- Focus on cyber security: the results highlight the need to prioritize cyber security in hospital institutions, with a particular reinforcement of resource allocation for a more effective SIEM implementation.
- Training and awareness: it is suggested to make more investments in training programs and training to sensitize employees to the risks of cyber threats to the sector and the proper use of SIEM.
- Collaboration: there is a need for greater involvement and collaboration in the definition of cyber security topics and the successful implementation of SIEM, between top management, IT service management, and employees with cyber security intervention, seeking a more comprehensive strategy.
- Continuous Evaluation: Regular evaluation of SIEM performance and adjustment needs is recommended as organizations' requirements grow.

- Sharing good practices: Sharing good practices and use cases between health institutions can strengthen cyber security [4].
- Incident Response: Regularly review incident response policies to address potential security breaches.

Due to the particularities of each hospital in terms of hardware, software, and human resources, it is important to choose and implement a SIEM that meets the needs and size of each institution. Consider incorporating Artificial Intelligence solutions to automate tasks and optimize the identification and containment of cyber threats.

From the interviews conducted with directors and managers of various SNS institutions, it is possible to identify and consider some highlighted ideas, such as:

- Importance of cyber security: In a hospital environment, cyber security plays an extremely important role, since it has to deal with a substantial volume of data that constantly circulates through its systems. Ensuring the integrity, confidentiality, and availability of this data is essential to preserve the efficient functioning and trust of both healthcare professionals and patients.
- Continuous improvement: Cyber security is a priority for state entities. The effort towards continuous improvement is evident in the SNS, demonstrated by the commitment to cyber security. Identifying weaknesses and communicating them directs informed investments. Data protection and confidentiality are essential in primary care frameworks, but the implementation of the necessary tools can be enhanced for greater effectiveness.
- Training and awareness: Training is a fundamental component of a comprehensive plan and will be present in several actions. Awareness and training emerge as prominent areas, emphasizing that cyber security is the intrinsic responsibility of each hospital unit.
- Protection of the health sector: cyber security permeates supply chains in the health sector, to ensure the protection not only of the partners involved but also of the infrastructures and medical devices, thus providing the necessary security and tranquillity for users.

- SIEM Potentiality: Beliefs in the potential of a SIEM to detect security incidents in hospitals are real. However, it is important to stress the relevance of effective governance, well-defined processes, and the proper allocation of resources to enhance their effectiveness and impact.

In short, both survey and interview participants agree on the crucial importance of cyber security in the field of health. They recognize the benefits of the existence of complementary tools to reinforce this security, such as SIEM. The need for more available information, training opportunities, and coaching also stands out as a relevant consideration, both now and in future initiatives. Strengthening the resilience of hospital facilities and all bodies linked to the Portuguese NHS emerges as a unified goal of the entire community involved.



## Chapter 6

# Proposal for SIEM

## Implementation in Healthcare

This chapter presents an all-encompassing strategy to augment healthcare security. It provides an overview of the proposed solution and rationalizes the choice of specific open-source tools, considering their effectiveness and relevance. The architecture and design considerations are meticulously delineated, leading to a robust and scalable system. A timeline and an implementation plan are articulated, facilitating a structured approach towards the deployment of the solution. The implementation process is exhaustively discussed, with a focus on practical aspects and potential challenges. The chapter concludes by outlining the anticipated benefits and outcomes, underscoring the transformative potential of the proposed solution in bolstering healthcare security.

### 6.1 Overview of the Proposed Solution

Hospital units have always faced some financial constraints that limit their ability to invest in software and hire additional human resources to strengthen cyber security. However, it is imperative to address this need as the implementation of a SIEM) is essential.

The ideal solution should be free, open source, easily scalable to meet the demands of the hospital environment, and easy to implement. Additionally, the chosen SIEM must be compatible not only with the operating systems used but also with other monitoring software in use in hospitals. Successful implementations of a comprehensive and afford-

able SIEM will enable hospitals to strengthen their cyber security posture and respond effectively to growing digital threats.

It is essential to understand the purpose of the application and choose appropriate implementation strategies by accurately defining security levels. Defining communication standards, listing compliance obligations, and configuring SIEM for real-time audits all play a critical role. The organization of digital assets in the IT infrastructure and the formulation of policies for personal devices are fundamental elements. Regularly adjusting SIEM settings help reduce false alerts (false positives), while rapid incident response strategies are imperative.

## 6.2 Rationale for Selecting Specific Open-source Tools

In today's ever-evolving cyber threat landscape, healthcare institutions face significant challenges in protecting their critical assets and data. In this context, SIEM systems play a crucial role in mitigating these threats. For this purpose, after a search carried out on the internet through Google, 3 of the various free and open-source solutions available were identified and analyzed, namely AlienVault OSSIM (Table 6.1), Prelude OSS (Table 6.2), and SIEM Wazuh (Table 6.3). In this analysis, the following parameters were taken into account: ease of installation, functionalities, number of vulnerabilities (cve.mitre.org), and integration with other tools.

Table 6.1: Alienvault OSSIM - SIEM considerations

<b>Name</b>	Allienvault OSSIM
<b>Installation</b>	Easy to install solution and sensors
<b>Features</b>	Asset inventories. Security log analysis. Vulnerability detection. Security Framework Assessment. Does not manage logs. Does not allow the monitoring of assets in the Cloud.
<b>Number of vulnerabilities</b>	32 CVE confirmed (last in 2020)
<b>Integration with other tools</b>	integrates with third parties: Meerkat, VirusTotal, Snort, and others. Does not integrate with Jira.

Wazuh SIEM, as an enterprise open-source solution, has established itself as a robust

Table 6.2: Prelude OSS - SIEM considerations

<b>Name</b>	Prelude OSS
<b>Installation</b>	Installation of the manager and GUI modules. Installation of LML agents and correlator. Limited version, ideal for testing and studies (<10 endpoints)
<b>Features</b>	Centralization of logs; Threat detection. Notifications. Limited in the volume of data to be analysed
<b>Number of vulnerabilities</b>	83 CVE confirmed (last 12 from 2022 onwards)
<b>Integration with other tools</b>	Integration with Snort, Suricata and Samhain

tool for monitoring, detecting, and responding to security incidents. Exploring its potential in key features, architectural elements, implementation strategies, and integration with other security tools, as well as investigating its use for threat detection and incident response, this study provides best practices for improving organizations' effectiveness in protecting their security.

Table 6.3: Wazuh SIEM - considerations

<b>Name</b>	Wazuh SIEM
<b>Installation</b>	Easy installation of server, indexer and agents on multiple OS
<b>Features</b>	Security log analysis. Vulnerability detection. Security framework assessment. Regulatory compliance.
<b>Number of vulnerabilities</b>	5 CVE confirmed (last in 2022)
<b>Integration with other tools</b>	Integration with Snort, Meerkat, VirusTotal, Active Directory, others.

In addition, robustness and ongoing community support are key elements in open-source solutions. In the case of Wazuh, its reputation, and expertise in detecting and responding to cyber threats are widely recognized. Through global collaboration and contributions, constant development and continuous improvements ensure that the solution remains up-to-date and effective in the face of ever-evolving threats. Wazuh's SIEM system offers a wide range of essential features for hospital cyber security, including its behavioral analytics capability to identify anomalous actions and anticipate potential threats. The threat-hunting functionality assists in identifying suspicious activity, allowing an agile and

effective response.

The choice also fell on Wazuh because there are effectively few security vulnerabilities, and since September 2022 [16], there has been no reference, as already mentioned and can be seen in Fig. 6.1, it is represented the main features.

**Wazuh : Security Vulnerabilities**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
 Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)  
[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2022-40497</a>			Exec Code	2022-09-28	2022-09-29	0.0	None	???	???	???	???	???	???
Wazuh v3.6.1 - v3.13.5, v4.0.0 - v4.2.7, and v4.3.0 - v4.3.7 were discovered to contain an authenticated remote code execution (RCE) vulnerability via the Active Response endpoint.														
2	<a href="#">CVE-2021-44079</a>	<a href="#">77</a>		Exec Code	2021-11-22	2021-12-14	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In the wazuh-slack active response script in Wazuh 4.2.x before 4.2.5, untrusted user agents are passed to a curl command line, potentially resulting in remote code execution.														
3	<a href="#">CVE-2021-41821</a>	<a href="#">191</a>		DoS	2021-09-29	2021-10-12	4.0	None	Remote	Low	???	None	None	Partial
Wazuh Manager in Wazuh through 4.1.5 is affected by a remote Integer Underflow vulnerability that might lead to denial of service. A crafted message must be sent from an authenticated agent to the manager.														
4	<a href="#">CVE-2021-26814</a>	<a href="#">22</a>		Exec Code Dir. Trav.	2021-03-06	2022-07-12	6.5	None	Remote	Low	???	Partial	Partial	Partial
Wazuh API in Wazuh from 4.0.0 to 4.0.3 allows authenticated users to execute arbitrary code with administrative privileges via /manager/files URI. An authenticated user to the service may exploit incomplete input validation on the /manager/files API to inject arbitrary code within the API service script.														
5	<a href="#">CVE-2018-19666</a>	<a href="#">22</a>		Dir. Trav.	2018-11-29	2019-01-04	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The agent in OSSEC through 3.1.0 on Windows allows local users to gain NT AUTHORITY\SYSTEM access via Directory Traversal by leveraging full access to the associated OSSEC server.														

Total number of vulnerabilities : 5 Page : 1 (This Page)

Figure 6.1: Wazuh security vulnerabilities. Source: The author.

The main functionalities of Wazuh SIEM allow:

- Security log analysis: by ensuring the security of the infrastructure meeting compliance requirements, monitoring and controlling all endpoint activity. Wazuh collects, stores, and analyses security event data to identify anomalies or indications of compromise.
- Vulnerability detection: The Wazuh agent installed on the monitored endpoints identifies the vulnerabilities, and prioritizes the identified vulnerabilities to streamline the decision-making and mitigation process. Wazuh’s threat detection capabilities ensure compliance while reducing the attack surface.
- Security framework assessment: Wazuh detects misconfigurations and infrastructure security flaws. The analysis it performs on computers based on the Cyber Security Center (CIS) criteria serves to assist in identifying and correcting vulnerabilities, misconfigurations, and deviations from best practices and security standards.

- Regulatory compliance: This solution plays a key role in assisting organizations in monitoring and demonstrating their compliance with various regulations, covering PCI DSS, NIST 800-53, GDPR, TSC SOC2, and Health Insurance Portability and Accountability Act (HIPAA). This ensures effectiveness and reliability in meeting all established requirements. The platform provides detailed reports and records to streamline the audit and compliance validation processes. Hospital units often need, at a minimum, to comply with the GDPR. It is important to highlight the additional advantage provided by adherence to the NIST 800.53 criteria [49], especially concerning security and privacy controls applicable to information systems and organizations. Regulation related to HIPAA (North American law) defines protocols for the administration of health information, aiming to improve the efficiency of medical services. This covers standards for electronic healthcare transactions, security standards, and unique identifiers. Wazuh provides HIPAA compliance features such as log analysis, file integrity monitoring, and threat detection and response capabilities. The guidelines of this law define controls and assess the physical security of the data center, logical access controls, policies, firewalls, networks, data breach prevention, and intrusions. Although there is no similar guideline in Portuguese or European law, it is believed that in the future a similar regulation may be created.

Wazuh SIEM is a solution composed of 3 components: Wazuh Server (W.server), Wazuh Indexer (W.indexer), and Wazuh Dashboard (W. Dashboard). To better understand what the function of each one is, a brief description follows.

- W.server: analyzes the data received by agents, which are processed through decoders and rules, using threat information to look for compliance indicators. W.server can analyze data from thousands of agents, when deployed as a cluster, and allows you to manage, configure, and update agents if needed.
- W.indexer: Effectively manage and store log and event data collected from various sources such as servers, network devices, and applications. W.indexer organizes this data into optimized indexes, allowing for quick search and analysis when needed. Furthermore, W.indexer supports event correlation, helping to identify complex patterns of malicious activity and take preventative action. W.indexer has four distinct

indexes that are defined to store various types of events: Wazuh-alerts for high-priority alerts, Wazuh-archives for all events, Wazuh-monitoring for Wazuh agent data, and Wazuh-statistics for server performance data.

- **W.dashboard:** is the web user interface and is intended for data visualization and analysis, relying on preconfigured dashboards for security events, regulatory compliance with PCI DSS, GDPR, HIPAA, NIST 800-53, detection of vulnerable applications, file integrity monitoring, configuration assessment results, monitoring events, and other pertinent information. It also serves for the configuration management and monitoring of the Wazuh itself.

To provide a more in-depth understanding of the components of the Wazuh and the flow that occurs between them, the following diagram is presented in Fig. 6.2.

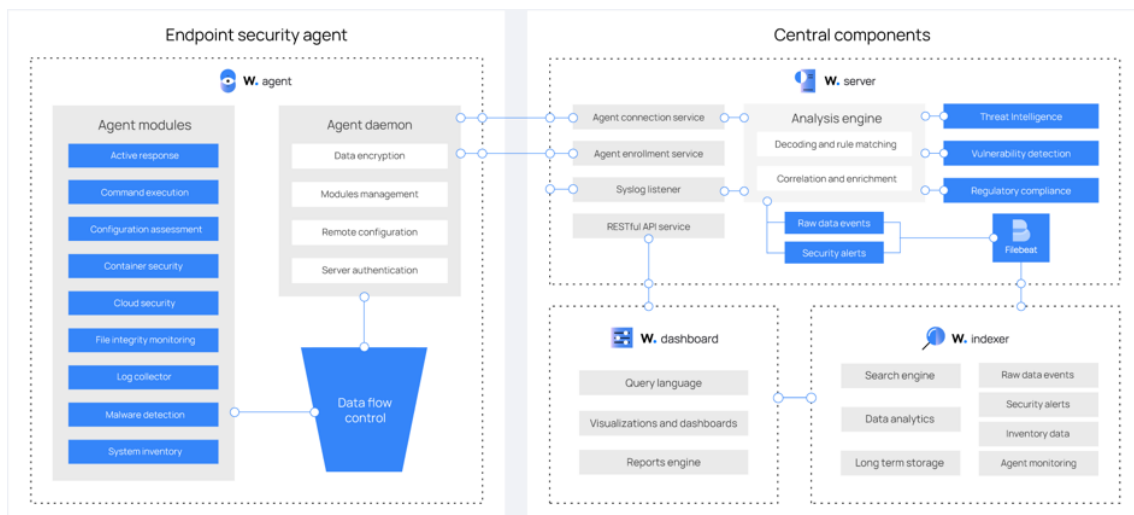


Figure 6.2: Flow diagram between the different components of the Wazuh. Source: [57]

However, although it is not considered a component, there is also the Wazuh Agent (W.agent), which acts as a sensor on endpoints.

- **W.agent:** is an essential component of the Wazuh security system, designed to collect and transmit log data and security information from the devices and systems being monitored. When installed on servers, workstations, and other devices, W.agent collects detailed data about events and activities, such as unauthorized access at-

tempts, changes to critical files, and suspicious behavior. This data is sent securely to W.server, where it is processed, and analyzed to detect potential threats. W.agent plays a vital role in gathering real-time information, enabling faster response to security incidents, and contributing to the proactive protection of information systems. In Fig. 6.4, the W.agent architecture is represented, which is organized in a modular way, where each component performs particular functions, such as file surveillance, record reading, inventory collection, and configuration analysis for the identification of malware.



Figure 6.3: Operating systems compatible with Wazuh SIEM. Source: The author.

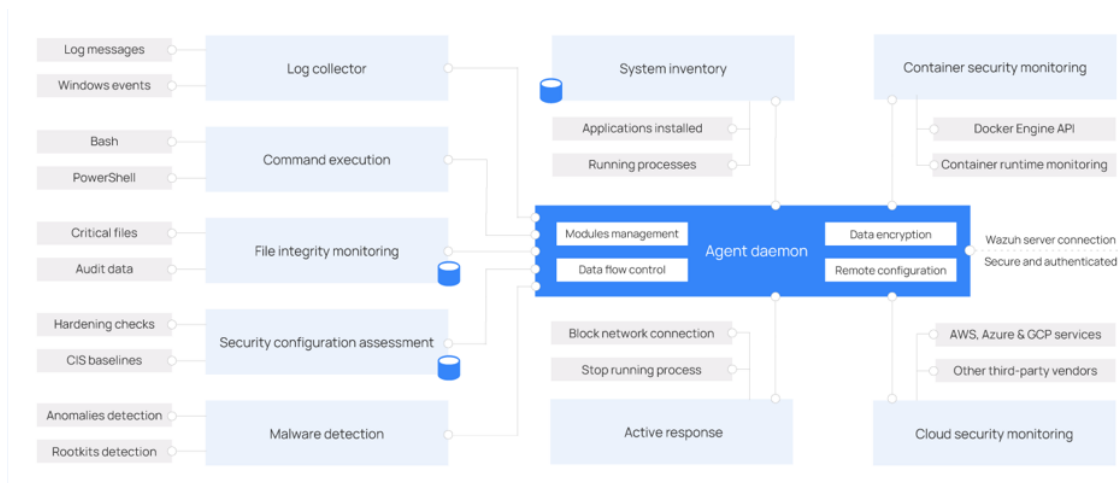


Figure 6.4: Modular architecture of a W.agent. Source:[58]

The operating systems mentioned above, W.agent can be installed in different versions as seen in Fig 6.3, the main ones, such as:

- Windows: Windows XP, Windows Server 2008, Windows 7+
- Linux

- Red Hat Enterprise: Red Hat 5, Red Hat 6, Red Hat 7+
- CentOS: CentOS 5, CentOS 6, CentOS 7+
- Ubuntu: Ubuntu 14, Ubuntu 15+
- Debian: Debian 7, Debian 8, Debian 9+
  
- MacOS X: macOS Sierra+
  
- Solaris: Solaris 10, Solaris 11
  
- AIX: AIX 6.1 TL9+
  
- HP-UX: HP-UX 11.31 +

Wazuh components can be installed in alternative ways, namely:

- Ready-to-use machines:
  - virtual machine (ova)
  - Amazon machine images (AMI)
  
- Containers:
  - Docker deployment
  - Kubernetes deployment
  
- Offline: after downloading the components, the installation is done offline.
  
- Source code: Download the source code, compile, and install each component.
  
- Commercial: Installing Wazuh with Elastic Basic or with Splunk (commercial solution)

SIEM Wazuh has two very useful resources for teams with responsibility for cyber security, in particular, those whose main task is the analysis of security alerts and reports, namely:

- Alerts and notifications: Real-time alerts and notifications are made when security events occur. Wazuh compares events from multiple sources, integrates threat intelligence streams, and provides custom dashboards and reports. It is possible to



customize notifications according to specific needs. This allows security teams to respond quickly to threats and minimize the impact of security incidents.

- Reporting: there is the possibility of producing insightful reports that provide a comprehensive analysis of security events. Wazuh empowers the creation of comprehensive, actionable information that suits each user's unique needs. Wazuh reports can be employed to demonstrate compliance with various regulations and standards.

### 6.3 Architecture and Design Considerations

One of the architectures that can be used in a hospital unit is a little more complex than the one referred to in the implementation in the laboratory created but essentially serves to make an approximation. Below, represented in Fig. 6.5 [60] and Fig. 6.6, are the architectures, respectively one of the ideal architectures to be used in a Hospital and another used in this laboratory simulation.

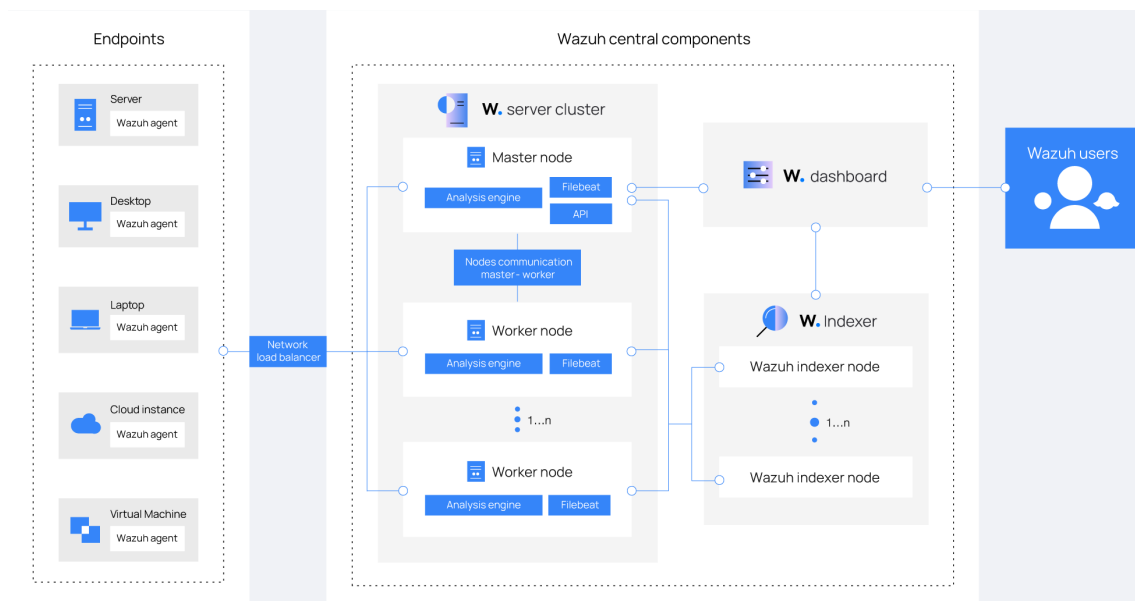


Figure 6.5: Wazuh deployment architecture. Source: [60].

The implementation of the laboratory with a set of virtual machines (Virtual Machine (VM)s), to better simulate an implementation in a real context. The virtual machines were divided into groups, each representing a critical area of a hospital, with different

IP ranges, and with different operating systems where W.agent was installed. Another used machine served as a server, where the Wazuh components (W.server, W.indexer, and W.dashboard) were installed.

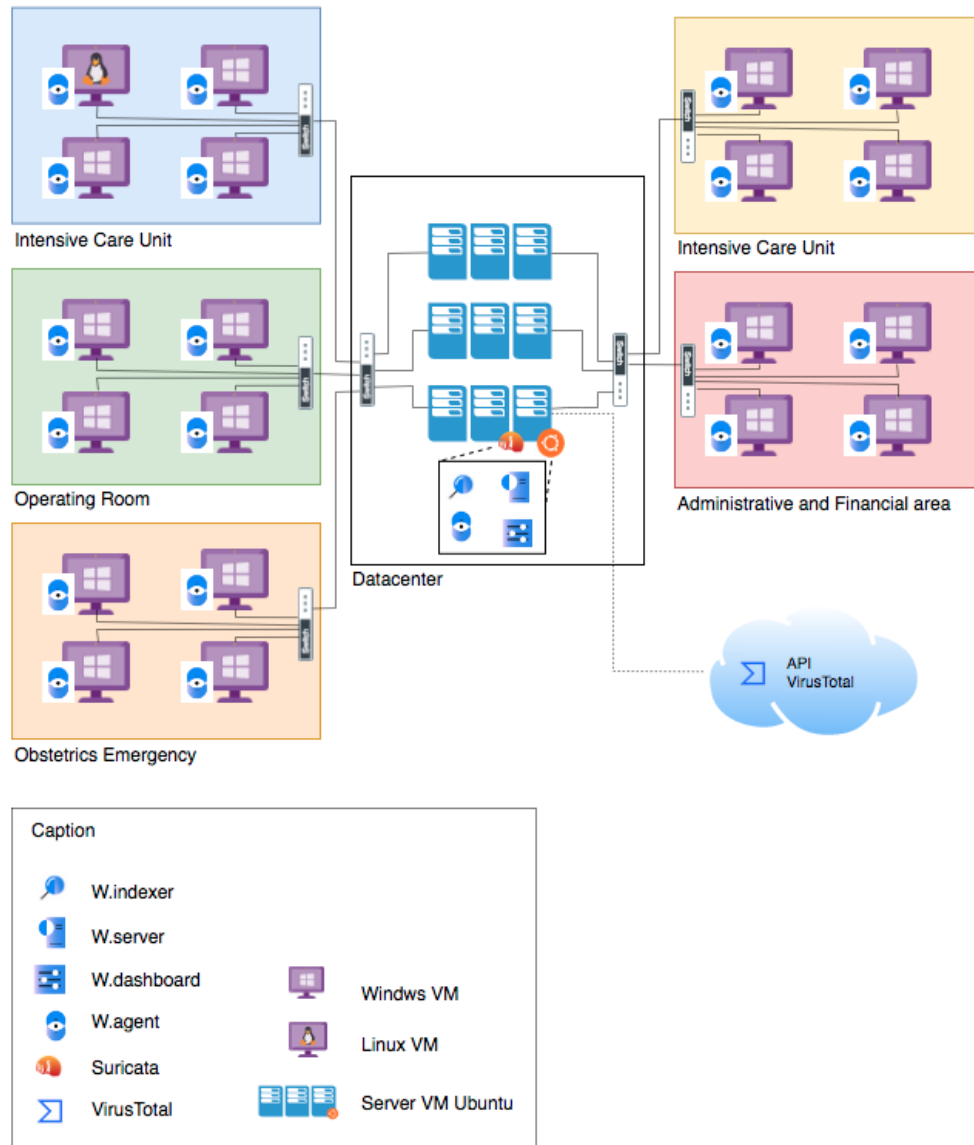


Figure 6.6: Architecture used in laboratory for testing. Source: The author.

In summary, the architecture for implementing SIEM Wazuh plays a crucial role in the effectiveness and responsiveness of the system. The combination of components, including W.server, W.indexer, and W.agent, forms a solid foundation for the collection, analysis, and response to security events.

## 6.4 Timeline and Implementation Plan

After choosing Wazuh as the SIEM implementation, the time allocated to the proposal for this implementation was approximately 64 hours, spread over 4 weeks. This was the time set to be able to carry out a quality laboratory within the scope of this study. For a better interpretation, below is a Gantt chart with the main tasks, as can be seen in Fig. 6.7.

Tasks	Week 1				Week 2				Week 3				Week 4			
Task 1	█	█	█	█												
Task 2			█	█												
Task 3					█	█	█	█								
Task 4							█	█								
Task 5									█	█	█	█				
Task 6											█	█				
Task 7											█	█	█			
Task 8													█	█		
Task 9															█	█
Task 10															█	█
Task 11																
Task 12															█	█
Task 13																

Figure 6.7: Diagram showing the execution of SIEM implementation tasks in the laboratory. Source: The author.

- Task 1: Initial SIEM Wazuh implementation test on a personal computer.
- Task 2: Choice of a workstation with the capacity to serve the test laboratory.
- Task 3: Workstation OS installation, configuration, and update;
- Task 4: Installation and configuration of Virt Manager for VM management.
- Task 5: Configuration and parameterization of virtual network segmentation.
- Task 6: Creation of VM with operating system to install W.server and W.Indexer.
- Task 7: Creation of VM of the chosen operating systems (Windows and Linux) and installation of agents (W.agent) in all VM;
- Task 8: Analysis of the identification and data collection of the logs in the W.dashboard;
- Task 9: Parameterization of integration with VirusTotal;

- Task 10: Analysis of the effectiveness of integration with VirusTotal;
- Task 11: Installation and configuration of the integration with Suricata;
- Task 12: Analysis of the effectiveness of integration with Suricata;
- Task 13: Use case testing to detect other incidents (access attempts, Nmap).

## 6.5 Implementation

For the implementation of the laboratory, a workstation with some responsiveness was required. Within the possibilities, an HP Z440 TWR was used as a host system, which had the following basic characteristics:

- Processor: XEON E5-2650 V4 12-CORE
- Memory: 16GB DDR4
- Storage: 512GB SSD

It is installed on this workstation, the latest version of Debian, and the Virtual Machine Manager (VMM) virtualization software (*virt-manager*) in version 4.1.0. This tool is a graphical interface for managing virtual machines using *libvirt*. It works with Kernel-based Virtual Machine (KVM) VM, but also with Xen and LXC (Linux containers). Enables an overview of running domains, performance statistics, and real-time resources, as depicted in the VMM figure below.

For each critical area, several VM with Windows XP, 7, and 10 operating systems were created, since these systems are still widely used in hospitals in Portugal. Older editions, such as Windows XP and Windows 7, remain in use due to the persistence of clinical and non-clinical applications that have not received updates or have high upgrade costs, being essential for the functioning of the services, as can be seen in Table 6.4. Some VMs with Ubuntu 22.04 LTS were also created, since some medical devices work connected to equipment with this operating system.

Virtual Machine Manager, better known as Virt Manager, plays an important role in the management of VM in enterprise environments, as can be seen in Fig. 6.8. This

Table 6.4: Table with the VM configurations used in the laboratory. Source: The author.

<b>Endpoint name</b>	<b>Area</b>	<b>IP</b>	<b>Operating System</b>
Fin-1	Financial	192.168.116.2	Windows 7
Fin-2	Financial	192.168.116.3	Windows 10
MCI-1	Intensive Care	192.168.112.2	Windows XP
MCI-2	Intensive Care	192.168.112.3	Windows 7
MCI-3	Intensive Care	192.168.112.4	Windows 10
MCI-4	Intensive Care	192.168.112.5	Ubuntu 22.04
OBS-1	Obstetrics	192.168.114.2	Windows 7
OBS-2	Obstetrics	192.168.114.3	Windows 10
OPE-1	Operation Block	192.168.115.2	Windows 7
OPE-2	Operation Block	192.168.115.3	Windows 10
URG-1	Emergencies	192.168.113.2	Windows 7
URG2	Emergencies	192.168.113.3	Windows 10
WaxuhServer VM	Datacenter	192.168.1.244	Debian

application, with an intuitive interface, allows the creation, configuration, and effective administration of these virtual environments, allowing the agile allocation of resources, performance monitoring, and adjustment according to needs since the combination of Virt Manager and KVM offers a comprehensive and robust solution for more complex and dynamic systems.

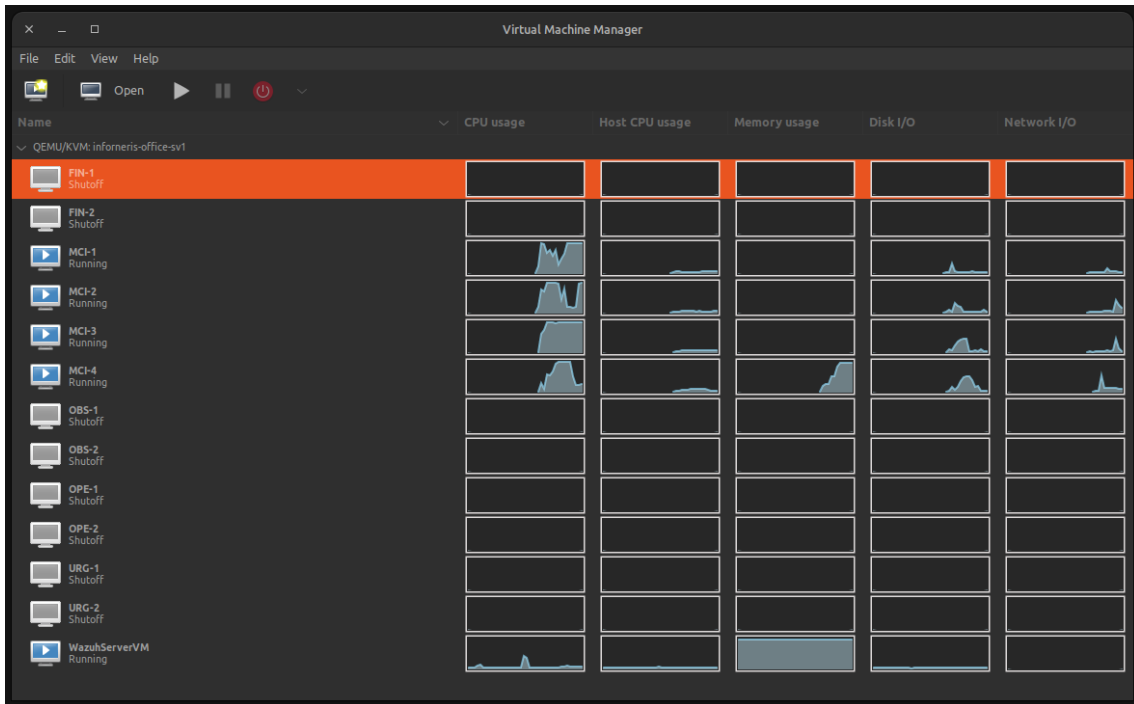
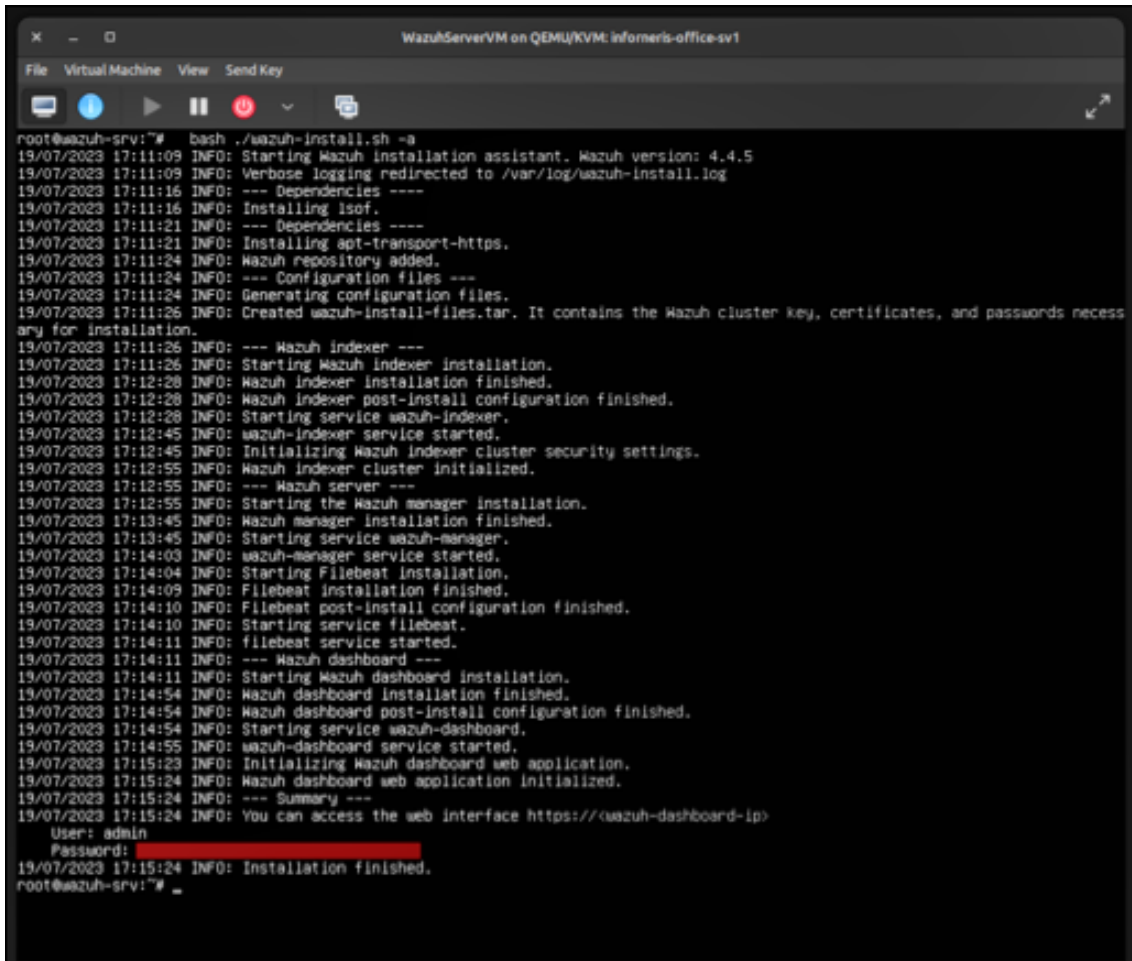


Figure 6.8: Diagram showing the execution of SIEM implementation tasks in the laboratory. Source: The author.

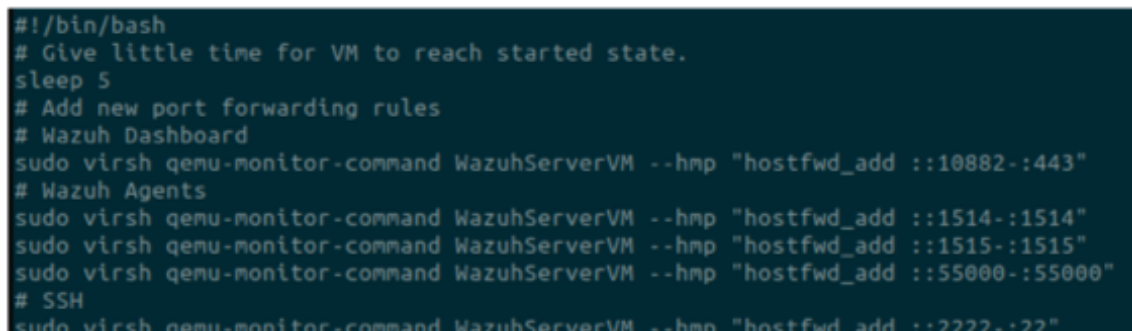
Network segmentation is crucial in any organization’s infrastructure, providing isolated and flexible environments. In this practical exercise, it was also essential to configure each of these networks to reflect and operate according to the needs of each area. When creating a virtual network, it is important to establish an IP address and subnet mask to ensure proper communication between the various virtual machines. The packet routing and forwarding configuration were required, as can be seen in Fig. 6.10, allowing VM to communicate with each other and with the external network.

Initially, a VM was created with the Ubuntu 22.04 operating system to install the various Wazuh components, including the Wazuh Server, Wazuh Indexer and Wazuh Agent, as seen in Fig. 6.9. The W.dashboard web interface was accessed through the browser within that VM, as seen in Fig. 6.11. This setup involved a set of tweaks and updates.



```
root@wazuh-srv:~# bash ./wazuh-install.sh -a
19/07/2023 17:11:09 INFO: Starting Wazuh installation assistant. Wazuh version: 4.4.5
19/07/2023 17:11:09 INFO: Verbose logging redirected to /var/log/wazuh-install.log
19/07/2023 17:11:16 INFO: --- Dependencies ----
19/07/2023 17:11:16 INFO: Installing isof.
19/07/2023 17:11:21 INFO: --- Dependencies ----
19/07/2023 17:11:21 INFO: Installing apt-transport-https.
19/07/2023 17:11:24 INFO: Wazuh repository added.
19/07/2023 17:11:24 INFO: --- Configuration files ---
19/07/2023 17:11:24 INFO: Generating configuration files.
19/07/2023 17:11:26 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
19/07/2023 17:11:26 INFO: --- Wazuh indexer ---
19/07/2023 17:11:26 INFO: Starting Wazuh indexer installation.
19/07/2023 17:12:20 INFO: Wazuh indexer installation finished.
19/07/2023 17:12:20 INFO: Wazuh indexer post-install configuration finished.
19/07/2023 17:12:28 INFO: Starting service wazuh-indexer.
19/07/2023 17:12:45 INFO: wazuh-indexer service started.
19/07/2023 17:12:45 INFO: Initializing Wazuh indexer cluster security settings.
19/07/2023 17:12:55 INFO: Wazuh indexer cluster initialized.
19/07/2023 17:12:55 INFO: --- Wazuh server ---
19/07/2023 17:12:55 INFO: Starting the Wazuh manager installation.
19/07/2023 17:13:45 INFO: Wazuh manager installation finished.
19/07/2023 17:13:45 INFO: Starting service wazuh-manager.
19/07/2023 17:14:03 INFO: wazuh-manager service started.
19/07/2023 17:14:04 INFO: Starting Filebeat installation.
19/07/2023 17:14:09 INFO: Filebeat installation finished.
19/07/2023 17:14:10 INFO: Filebeat post-install configuration finished.
19/07/2023 17:14:10 INFO: Starting service filebeat.
19/07/2023 17:14:11 INFO: filebeat service started.
19/07/2023 17:14:11 INFO: --- Wazuh dashboard ---
19/07/2023 17:14:11 INFO: Starting Wazuh dashboard installation.
19/07/2023 17:14:54 INFO: Wazuh dashboard installation finished.
19/07/2023 17:14:54 INFO: Wazuh dashboard post-install configuration finished.
19/07/2023 17:14:54 INFO: Starting service wazuh-dashboard.
19/07/2023 17:14:55 INFO: wazuh-dashboard service started.
19/07/2023 17:15:23 INFO: Initializing Wazuh dashboard web application.
19/07/2023 17:15:24 INFO: Wazuh dashboard web application initialized.
19/07/2023 17:15:24 INFO: --- Summary ---
19/07/2023 17:15:24 INFO: You can access the web interface https://(wazuh-dashboard-ip)
User: admin
Password:
19/07/2023 17:15:24 INFO: Installation finished.
root@wazuh-srv:~#
```

Figure 6.9: Wazuh installation. Source: The author.



```
#!/bin/bash
# Give little time for VM to reach started state.
sleep 5
# Add new port forwarding rules
# Wazuh Dashboard
sudo virsh qemu-monitor-command WazuhServerVM --hmp "hostfwd_add ::10882-:443"
# Wazuh Agents
sudo virsh qemu-monitor-command WazuhServerVM --hmp "hostfwd_add ::1514-:1514"
sudo virsh qemu-monitor-command WazuhServerVM --hmp "hostfwd_add ::1515-:1515"
sudo virsh qemu-monitor-command WazuhServerVM --hmp "hostfwd_add ::55000-:55000"
# SSH
sudo virsh qemu-monitor-command WazuhServerVM --hmp "hostfwd add ::2222-:22"
#!/bin/bash
```

Figure 6.10: Routing add forward ports. Source: The author.



Figure 6.11: Wazuh login screen. Source: The author.

The creation of agents (W.agent) is done through the Dashboard, in which the choice of the operating system and the version that is intended for the chosen endpoint is made. The system returns a script, necessary to install the agents, simply by executing the generated command on the endpoints. Some generic examples used are below, already with the IP of the server where the W.server is located, with only the name of the group and the machine missing.

- Windows XP

```
1     msiexec.exe /i wazuh-agent-4.4.5-1.msi /q WAZUH_MANAGER
      =192.168.1.244 WAZUH_REGISTRATION_SERVER
      =192.168.1.244 WAZUH_AGENT_GROUP=X WAZUH_AGENT_NAME=
      X-X
2     NET START WazuhSvc
```

Listing 6.1: Script with commands to create w-agent on Windows XP

- Windows 7+

```
1     $client = New-Object System.Net.WebClient; $client.
      DownloadFile("https://packages.wazuh.com/4.x/windows
```



```
    /wazuh-agent-4.4.5-1.msi", "${env:tmp}\wazuh-agent.  
    msi"); msixexec.exe /i ${env:tmp}\wazuh-agent.msi /q  
    WAZUH_MANAGER=192.168.1.244  
    WAZUH_REGISTRATION_SERVER=192.168.1.244  
    WAZUH_AGENT_GROUP=X WAZUH_AGENT_NAME=X-X  
2 NET START WazuhSvc
```

Listing 6.2: Script with commands to create w-agent on Windows 7+

- Ubuntu

```
1 curl -so wazuh-agent.deb https://packages.wazuh.com/4.x  
  /apt/pool/main/w/wazuh-agent/wazuh-agent_4.4.5-1  
  _amd64.deb && sudo WAZUH_MANAGER=192.168.1.244  
  WAZUH_AGENT_GROUP=X WAZUH_AGENT_NAME=X-X dpkg -i ./  
  wazuh-agent.deb && sleep 10 && sudo systemctl daemon  
  -reload && sudo systemctl enable wazuh-agent && sudo  
  systemctl start wazuh-agent
```

Listing 6.3: Script with commands to create w-agent on Ubuntu

In Fig. 6.12 below, an example of the graphical pane of how the options for creating an agent for Ubuntu are presented.

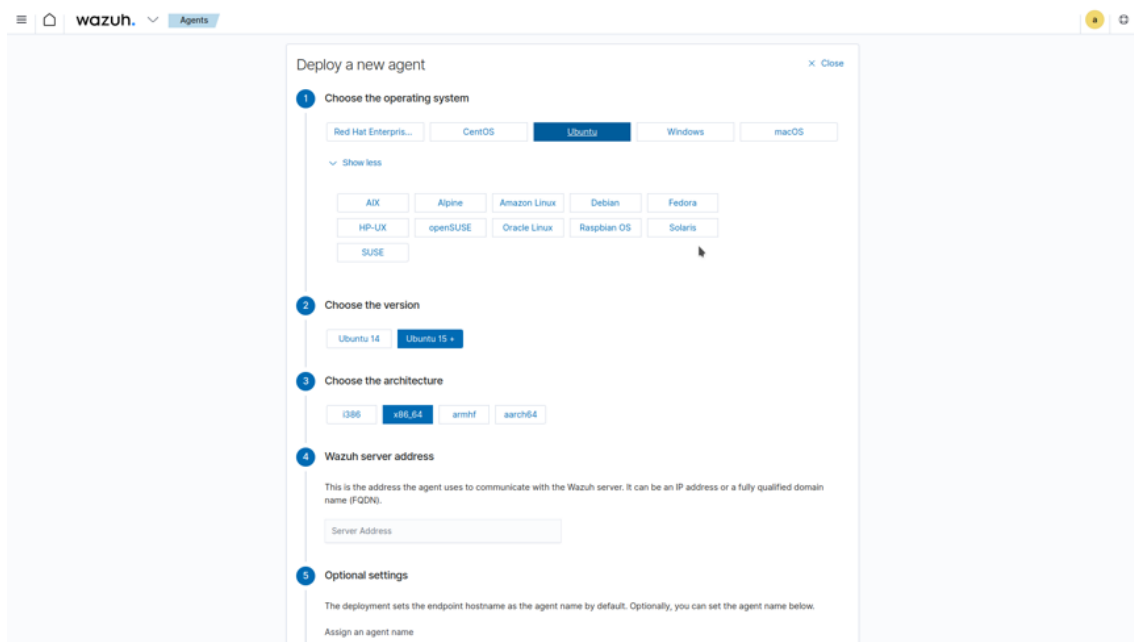


Figure 6.12: Dashboard for deploying a new agent to Ubuntu. Source: [59]

In the Wazuh management dashboard there is also the possibility of seeing the list of installed agents, as graphically represented in Fig. 6.13 with a set of fields that allow an easy perception of the assets that are on the network, namely the fields related to ID, Name, IP, Group, Operating system, Cluster, Version, and Status.

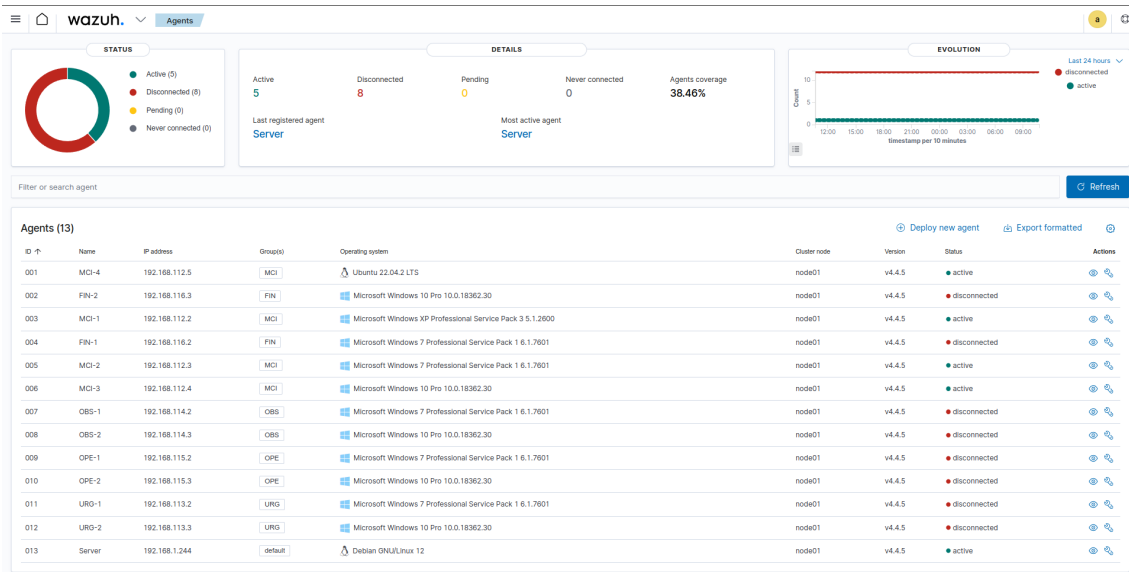


Figure 6.13: List of agents and properties of endpoints. Source: The author.

The agents are active when the machine starts operating, that is, when the computer is turned on, or inactive, when the machine turns off, usually, and this is reflected in the W.dashboard, as can be seen in the Fig. 6.14.

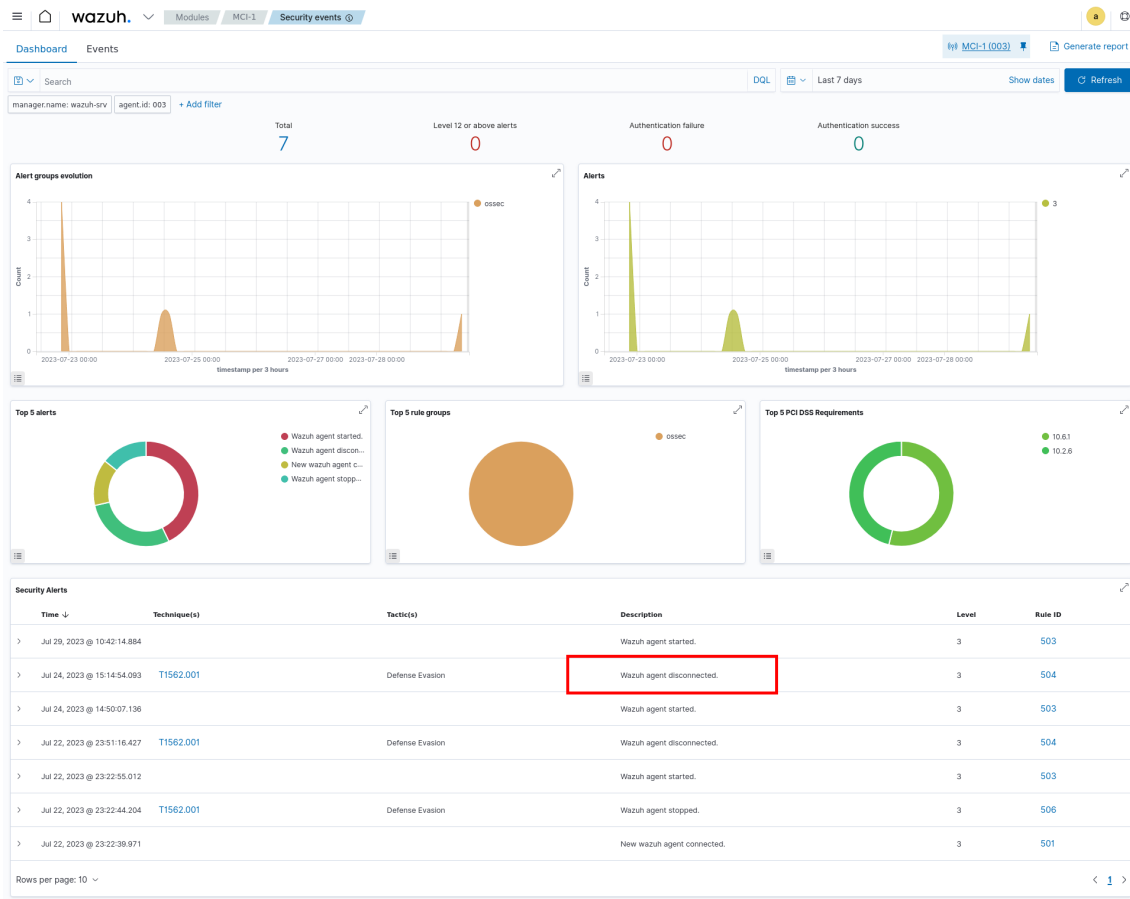


Figure 6.14: Listing where the agent’s status change actions are visible. Source: The author.

In addition to the Wazuh solution, which in itself allows a significant detection and collection of system logs, it was also decided to take advantage of the possibility of integration with other tools. It was then decided to integrate Suricata for intrusion detection and prevention, and also VirusTotal, to identify access to addresses or files considered malicious. The actions required for each of the integrations are detailed below.

The installation and configuration of Suricata followed the procedure described on Wazuh’s website, which has several actions, such as:

- Installation of Suricata on the VM where you have the server or on an endpoint, for example with Ubuntu. For this, the repository was identified and chosen, then the system was updated, and only then the effective installation of Suricata was carried out.

- Then, the rules that define the data source in which the Suricata will act were downloaded and extracted.
- Thirdly, the settings present in the file `/etc/suricata/suricata.yaml` were modified, with the data from the server and the network.
- Then the Suricata service was restarted, as seen in Fig. 6.15;
- Finally, added the configuration to the `/var/ossec/etc/ossec.conf` file of the Wazuh agent, as seen in Listing 6.4.

```
1 <ossec_config>
2 <localfile>
3 <log_format>json</log_format>
4 <location>/var/log/suricata/eve.json</location>
5 </localfile>
6 </ossec_config>
```

Listing 6.4: Wazuh settings with JSON file definition to download Suricata



```
root@inforneris-office-sv1:~# systemctl status suricata.service
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: enabled)
   Active: active (running) since Sat 2023-07-29 11:35:02 WEST; 29min ago
     Docs: man:suricata(8)
           man:suricata-sc(8)
           https://suricata-ids.org/docs/
   Process: 746 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
  Main PID: 841 (Suricata-Main)
    Tasks: 30 (limit: 19010)
   Memory: 234.4M
      CPU: 25.455s
   CGroup: /system.slice/suricata.service
           └─841 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Jul 29 11:35:00 inforneris-office-sv1 systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Jul 29 11:35:02 inforneris-office-sv1 suricata[746]: 29/7/2023 -- 11:35:02 - <Notice> - This is Suricata version 6.0.10 RELEASE running in SYSTEM mode
Jul 29 11:35:02 inforneris-office-sv1 systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
root@inforneris-office-sv1:~#
```

Figure 6.15: Status of Suricata. Source: The author

Firstly, it was necessary to register on the VirusTotal website to obtain the key for the API. The integration of VirusTotal with Wazuh, to detect malicious files, the configuration was quite simple, as it was only necessary to edit the file `/var/ossec/etc/ossec.conf`, putting the code below, and replacing the `APIKEY` tag and in the `syscheck` section, as seen in Listings 6.5 and 6.6, both in `W.server` and in `W.agent`, parameterize the board to be analyzed in each endpoint.

The Wazuh integration can send a request to the VirusTotal API with the hashes of files that are generated or updated in any folder monitored by FIM. If the result from VirusTotal is affirmative, Wazuh will generate an alert in the system, as shown in Fig. 6.16.

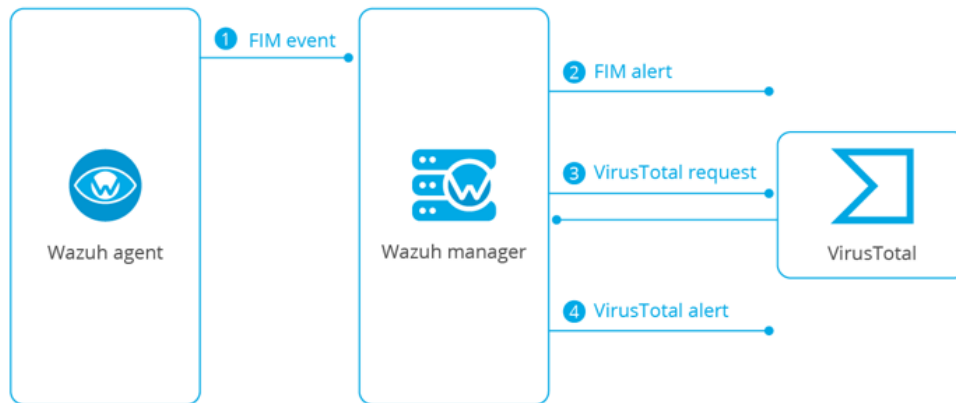


Figure 6.16: Flow diagram of VirusTotal Malware Detection. Source:[56]

```

1 <integration>
2 <name>VirusTotal</name>
3 <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal
   API key -->
4 <group>syscheck</group>.
5 <alert_format>json</alert_format>
6 </integration>
  
```

Listing 6.5: Wazuh settings with VirusTotal API KEY

```

1 <syscheck>
2 <directories check_all="yes" realtime="yes">/media/user/
   software</directories>
3 </syscheck>
  
```

Listing 6.6: Wazuh configuration to control the selected folder

Wazuh receives the data in JSON format and presents it in a dashboard when events occur, as can be seen in the use cases created for this purpose.

## 6.6 Expected Benefits and Outcomes

The implementation and use of the Wazuh SIEM provide a variety of benefits that can be extremely valuable to any organization, especially in the context of Portuguese NHS hospital units. These benefits can be divided into five main categories:

- **Open source:** The possibility of implementing the solution for free, without any costs, and still having the ability to customize it, is one of the main advantages.
- **Documentation:** The documentation provided by Wazuh for the implementation of your SIEM is comprehensive, and detailed and offers a great help to clarify any doubts that may arise.
- **Ease of installation and use:** As you can see, the implementation and configuration of SIEM Wazuh is simple. It is compatible with a wide range of operating systems, and W.dashboard provides excellent visualization as well as several customization options to visualize the data that is considered necessary.
- **Comprehensive features:** Wazuh SIEM offers a wide range of features, such as advanced threat detection, and ensuring cyber security through constant monitoring and real-time alerts. The ability to integrate with diverse data sources and the correlation of events provides crucial insight for the identification and mitigation of risks. File integrity monitoring, centralized data collection, and trend analysis enable proactive security management, while compliance support helps meet regulatory requirements effectively.
- **Integration with other data sources:** Wazuh's SIEM allows integration with many data sources, whether to identify intrusions, vulnerabilities, and even malicious files, among others.

Use cases are intended to describe practical situations in a real-world context in which a particular tool, technology, or approach is applied to solve specific problems or achieve specific objectives. In the context of a Wazuh SIEM, use cases have the function of identifying how the tool can be concretely used to improve an organization's cyber security and risk management. Although several cases have been documented on the Wazuh (Proof

of Concept guide) website, tests were carried out in this study, in this more practical component of the laboratory, where four use cases were verified, namely:

- Use Case 1 – Login

In this exercise, several login attempts were made to assess whether Wazuh collected this information and presented it on the dashboard. Some of the attempts were made with incorrect data, others with correct data, either by session login or by Secure Shell (SSH), as can be seen in the Fig. 6.17, 6.18 and 6.19, respectively. The detection of login attempts is important in terms of cyber security because when it exceeds the maximum authorized limit, it indicates a brute-force attack behavior, for example.

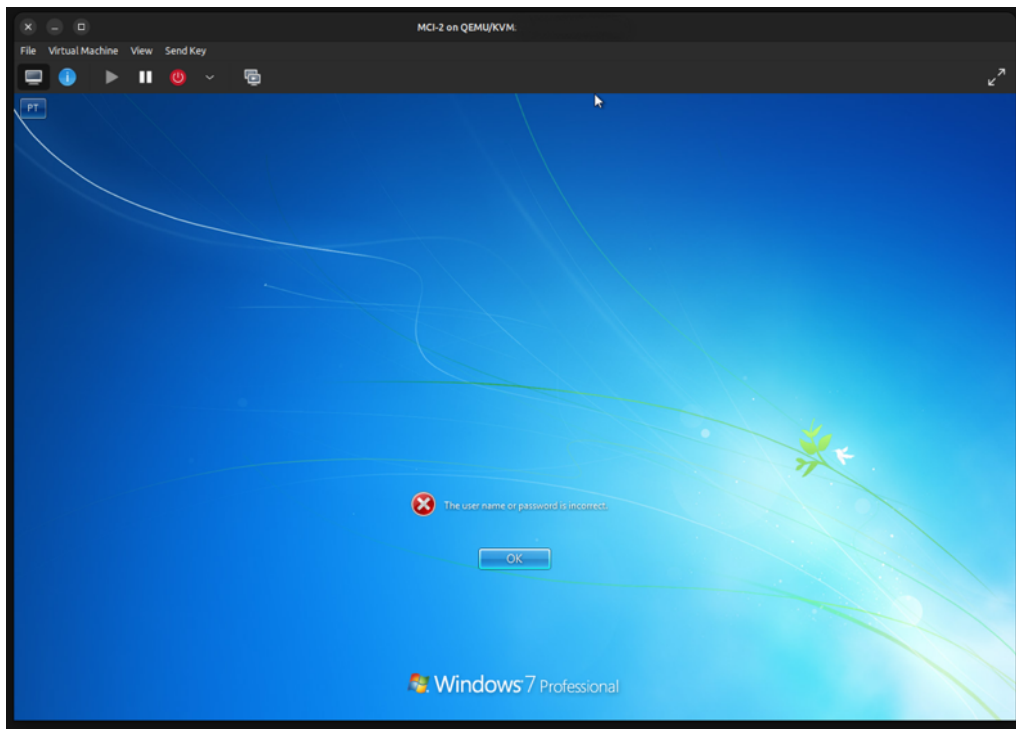


Figure 6.17: Wrong access via login session in Windows 7. Source: The author



```

root@kali:~# nmap -p- 192.168.112.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 17:39 WEST
Nmap scan report for 192.168.112.5
Host is up (0.00010s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 52:54:00:15:2B:6D (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds

root@kali:~# ssh 192.168.112.5
The authenticity of host '192.168.112.5 (192.168.112.5)' can't be established.
ED25519 key fingerprint is SHA256:ZFwMjXPeX2T09tUsoTnskVAwjYDmZLLXef/e3RNnbg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.112.5' (ED25519) to the list of known hosts.
kali@192.168.112.5's password:
Permission denied, please try again.
kali@192.168.112.5's password:
Permission denied, please try again.
kali@192.168.112.5's password:
kali@192.168.112.5: Permission denied (publickey,password).

root@kali:~#
    
```

Figure 6.18: Attempted SSH access to VM with IP 192.168.112.5. Source: The author

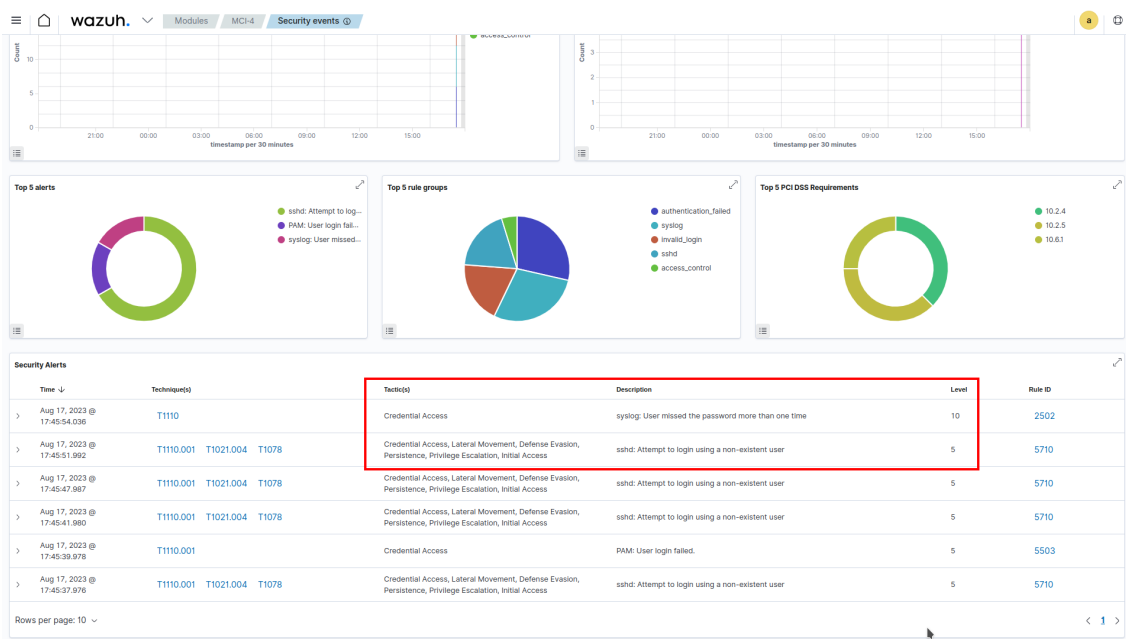


Figure 6.19: SSH access related incident listing. Source: The author

- Use Case 2 nmap command execution

In this test, two commands were executed with "nmap", as can be seen in Fig.6.20 to scan the ports of the known endpoint present in the organization's network, to obtain more detailed information about checking which ports were open, to simulate an enumeration process.

```
1 $nmap -Pn 192.168.112.
```

Listing 6.7: Run the nmap command



```
root@kali: ~
┌──(root@kali)-[~]
│
└─$ nmap -Pn 192.168.112.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:56 WEST
Nmap scan report for 192.168.112.3
Host is up (0.0027s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
18243/tcp open  unknown
MAC Address: 52:54:00:20:53:05 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds

┌──(root@kali)-[~]
│
└─$ nmap -O 192.168.112.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:57 WEST
Nmap scan report for 192.168.112.3
Host is up (0.0018s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
18243/tcp open  unknown
MAC Address: 52:54:00:20:53:05 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.01 seconds

┌──(root@kali)-[~]
```

Figure 6.20: Nmap's execution. Source: The author

- Use Case 3: Malicious file detection

Through integration with VirusTotal, it was possible to identify a malicious file eicar.com.zip, in the download that was made on one of the machines (MCI4). This file is used in the laboratory to simulate malware and is available at: <https://www.eicar.org/download-anti-malware-testfile/>. It was immediately identified by VirusTotal and listed in SIEM Wazuh, as can be seen in Fig. 6.21 below.

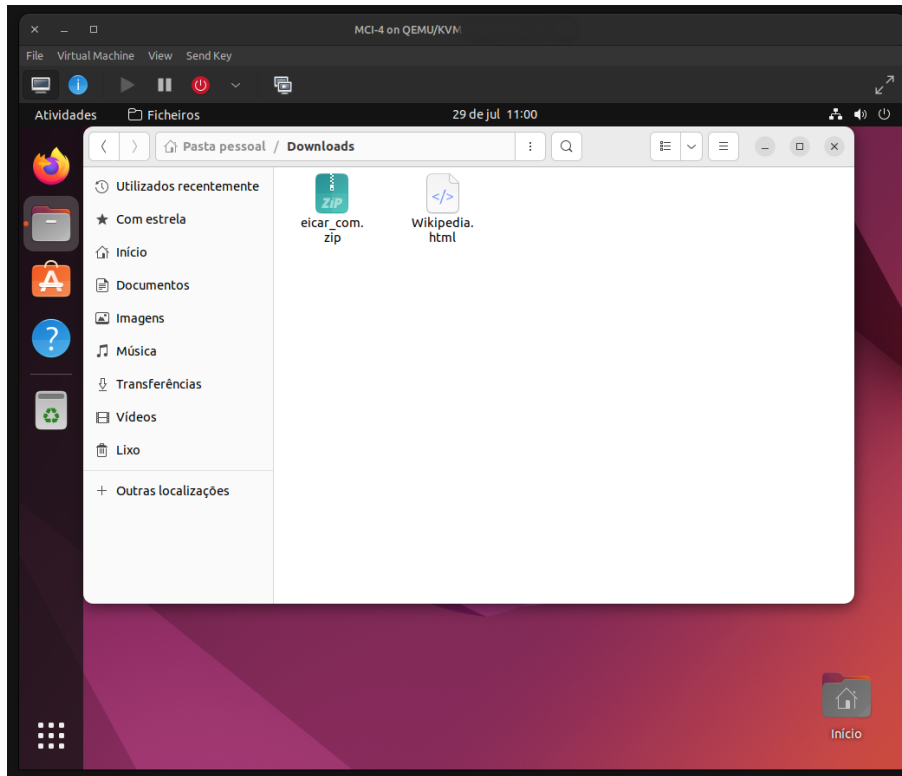


Figure 6.21: Malware download simulation. Source: The author.

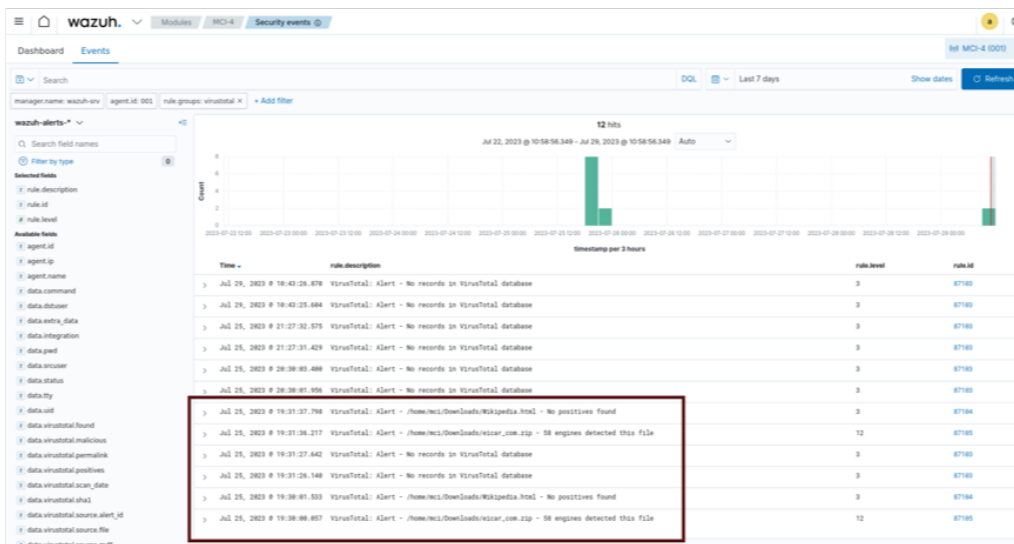


Figure 6.22: Listing malware detection. Source: The author.

- Use Case 4: Identifying and Exploiting Vulnerability

As Wazuh is based on data sources records coming from MITRE ATT&CK (<https://attack.mitre.org/>) on the vulnerabilities that the endpoints may contain, through the vulnerability de-

tector, after selecting one of them (put the name of the vulnerability and context), graphically represented in the Fig. 6.23, we proceeded with an exploit to verify it. Kali, which has already incorporated the software to perform intrusion tests known as Metasploit, was used in another VM created for this purpose, and it was found that it was possible to gain access to the machine. To prove this fact, a print of the target desktop was made and stored in a directory of the attacking system, as evidence, as can be seen in Fig. 6.24.



```
nmap x  msfconsole help x  exploit x  action x
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.112.145:4444
[*] 192.168.112.3:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.112.3:445 - Most is likely VULNERABLE to MS17-010! - Windows 7 Professional 7681 Service Pack 1 x64 (64-bit)
[*] 192.168.112.3:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.112.3:445 - The target is vulnerable.
[*] 192.168.112.3:445 - Connecting to target for exploitation.
[*] 192.168.112.3:445 - Connection established for exploitation.
[*] 192.168.112.3:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.112.3:445 - CORE raw buffer dump (62 bytes)
[*] 192.168.112.3:445 - 0x00000000 57 69 66 64 6f 77 73 20 37 20 50 72 6f 66 66 65 73  Windows 7 Profes
[*] 192.168.112.3:445 - 0x00000010 73 69 6f 64 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7681 Serv
[*] 192.168.112.3:445 - 0x00000020 69 63 65 20 50 61 63 66 20 31         ice Pack 1
[*] 192.168.112.3:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.112.3:445 - Trying exploit with 32 Groom Allocations.
[*] 192.168.112.3:445 - Sending all but last fragment of exploit packet
[*] 192.168.112.3:445 - Starting non-paged pool grooming
[*] 192.168.112.3:445 - Sending SMBv2 buffers
[*] 192.168.112.3:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.112.3:445 - Sending final SMBv2 buffers.
[*] 192.168.112.3:445 - Sending last fragment of exploit packet!
[*] 192.168.112.3:445 - Receiving response from exploit packet
[*] 192.168.112.3:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.112.3:445 - Sending egg to corrupted connection.
[*] 192.168.112.3:445 - Triggering free of corrupted buffer.
[*] Sending stage (204774 bytes) to 192.168.112.3
[*] Meterpreter session 1 opened (192.168.112.145:4444 -> 192.168.112.3:445275) at 2023-08-17 15:46:30 +0100
[*] 192.168.112.3:445 - *-----*
[*] 192.168.112.3:445 - *-----*
[*] 192.168.112.3:445 - *-----*
[*] 192.168.112.3:445 - *-----*
[*] 192.168.112.3:445 - *-----*

meterpreter >
```

Figure 6.23: Vulnerability exploiting. Source: The author.

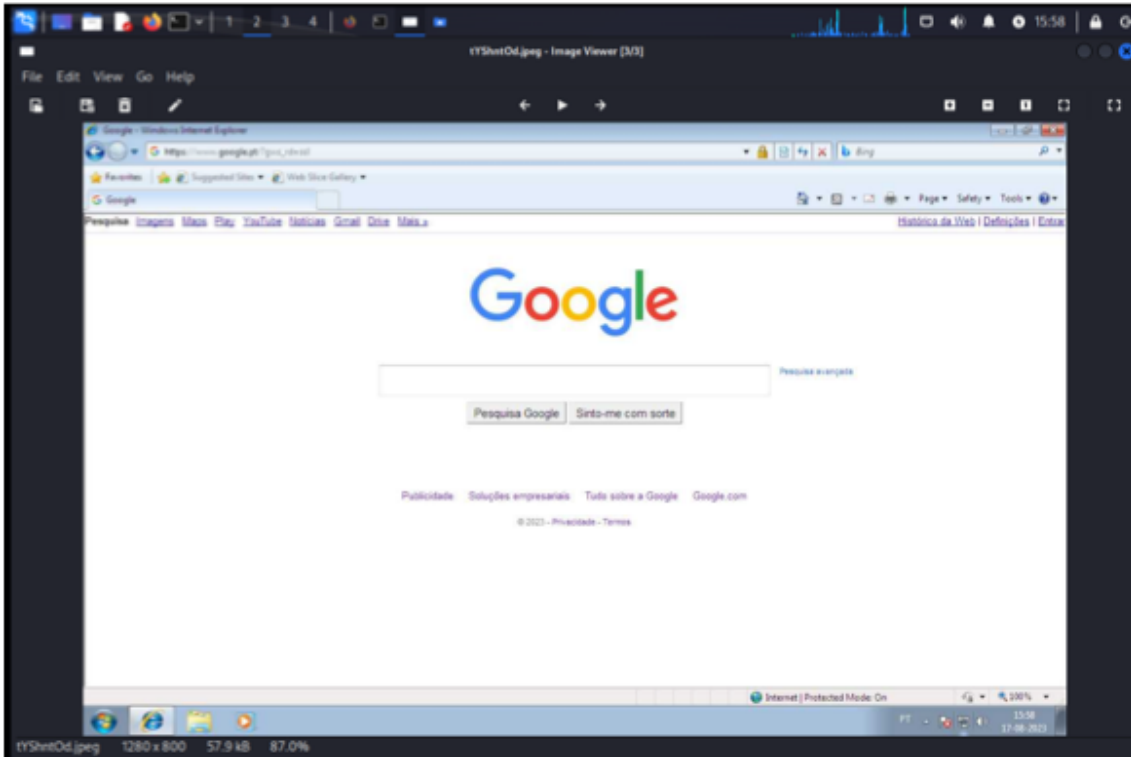


Figure 6.24: Remote screen capture. Source: The author.

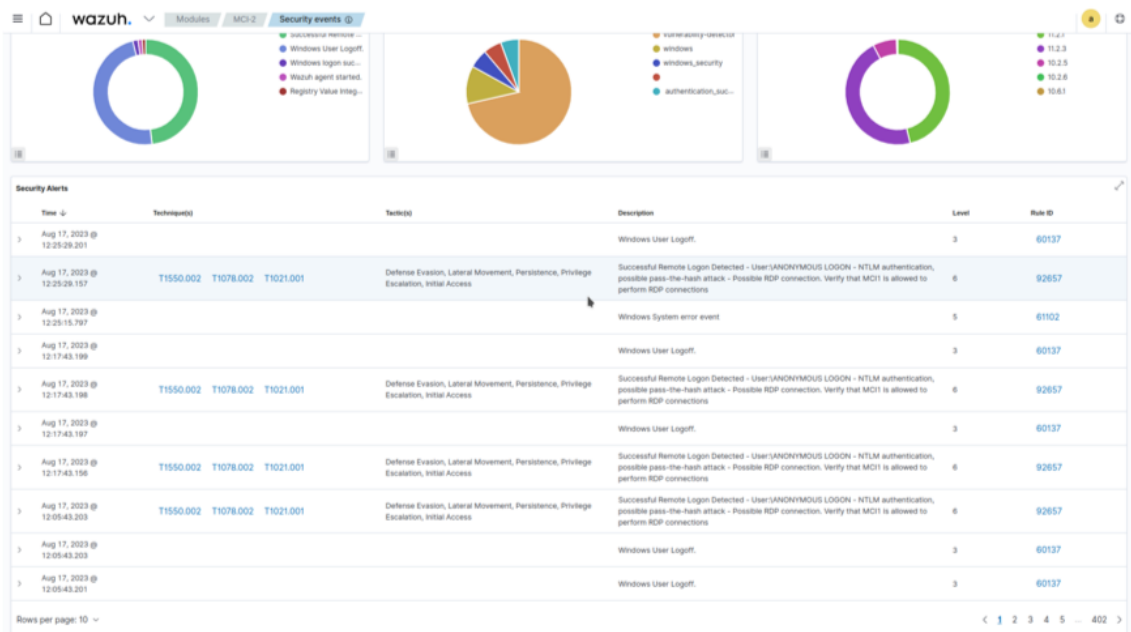


Figure 6.25: Successful remote login Detected. Source: The author.

The integration of Suricata and VirusTotal significantly enriches the SIEM Wazuh implementation, strengthening security through advanced real-time intrusion detection and the identification of suspicious access to addresses or files. These integrations provide a complete defense against cyber threats, increasing the responsiveness and protection of digital infrastructure. The use cases that have been made demonstrate its effectiveness and versatility as an excellent choice to reinforce cyber security. Its ability to identify advanced threats, monitor file integrity, correlate events, and ensure regulatory compliance, along with complete documentation and ease of implementation, reinforce its position as a solid and highly recommended solution for the protection of hospital units whether they are hospitals, hospital centers, ULS or IPO.

## Chapter 7

# Conclusion and Future Work

The research carried out on the analysis and implementation of a SIEM in a hospital unit as a PBE that is part of the SNS brought to light results of high interest. This research provided a deeper understanding of the cyber security situation in the context of health and also highlighted the possibility of a frank improvement in the cyber security posture by incorporating other systems capable of preventing, detecting, and responding to cyber-attacks.

The conclusions that derive from the questionnaire highlight three crucial elements to consider. First, it emphasizes the vital importance of cyber security for the proper functioning of hospitals, demonstrating that the adoption of a solution such as SIEM can play a significant role in this context. Second, there is a lack of resources directed to cyber security in SNS hospitals, and often the professionals responsible for cyber security lack specific training [35]. Finally, investments in technology within the SNS have been limited so far.

Senior management also recognizes the critical importance of cyber security in health-care and is aware of the continued need to adopt measures that strengthen resilience, whether through investments in technological infrastructure or software, as well as through the development of employees' skills, regardless of whether they are technical or not. Thus, it is clear that the research contributed to broadening the understanding of cyber security in the hospital context of the SNS, with emphasis on the relevance of SIEM and the need for proactive actions to address present and future gaps.

The model presented for the implementation of SIEM using open source and labora-

tory software, demonstrated its effectiveness in detecting security threats and responding quickly to incidents, ensuring compliance and the basis for its use. These detections highlight the strategic relevance of SIEM in improving cyber security in hospital environments. Additionally, because of its simplicity and usability, it allows its implementation to be simpler, not requiring in-depth basic knowledge, and then because it is free and open source, it allows costs to be directed to other investments.

Rampant consumption of rapidly emerging AI solutions make it possible to create and alter texts, brands, images, music, videos, data analytics, and more. In the area of cyber security, it is also important to carefully analyze the validity of the proposed solutions, especially when it comes to interfering with systems. Ease of access to these technologies requires a responsible approach to ensure that their use does not compromise the security and integrity of information. Verifying the effectiveness and security of artificial intelligence solutions is essential to protect privacy and mitigate possible risks associated with their use in various fields, including cyber security.

The integration of AI in SIEM emerges as a promising solution to deal with these difficulties. AI applied to SIEM allows you to analyze extensive data in real-time, identifying anomalies and predicting security incidents. This allows the relief of human resources with this responsibility, causing some of the manual work to be taken over by the machines. This improvement brings more efficiency to the SIEM system, which learns and adapts to ever-evolving threats.

The integration of AI into SIEM strengthens threat detection and prevention by analyzing different data sources and alerting analysts to act quickly. Furthermore, predictive analytics with AI allow you to anticipate threats based on historical and real-time data, driving proactive and preventive efforts. Despite the benefits, the integration of AI into SIEM also brings challenges, such as the possibility of false positives and negatives, but with proper training with machine learning [24], these cases can be drastically reduced.

In conclusion, integrating AI into SIEM is auspicious for cyber security as it enables rapid threat response, and predictive analytics, and reduces analyst workload with manual tasks. However, it is necessary to consider the limits of AI and ongoing collaboration between humans and systems to maximize its benefits and protect organizations from ever-evolving digital threats.



## 7.1 Limitations of the Study

The main limitations of this study, which somewhat conditioned the objectives that were intended to be achieved, can be summarized in two parts.

In the first question, it is important to highlight the sample size concerning the number of responses to the survey. The fact that the survey was made available during a considered holiday period may have contributed to the overall low response rate. It would have been extremely advantageous to have obtained a higher number of responses, but the values of 25.6% among IT directors and 11.6% among system administrators are believed to be reasonable and somewhat representative of the population under study.

Second, another relevant limitation was the lack of material resources for the implementation of a more advanced laboratory, which would allow the creation of more points of analysis with a clustered SIEM Wazuh architecture. This would result in a closer approach to reality, allowing a more in-depth analysis of the data. However, it seems that the main objective proposed by the work has been achieved. The recognition of the aforementioned limitations provides an opening for future investigations capable of overcoming these restrictions and enriching scientific knowledge in this specific area.

## 7.2 Future Work

This research contributed to the increase of knowledge in information security in the hospital context, highlighting the benefits of implementing a SIEM in safeguarding sensitive patient data and controlling access to the network. The results highlight the importance of investing in security solutions, such as SIEM, in healthcare institutions, particularly in the Portuguese NHS hospitals, to prevent data breaches and ensure compliance with privacy regulations.

Future studies may evaluate the effectiveness of SIEM in different hospital contexts and propose integration with other security tools to optimize threat detection and response. A specific example may be the creation of an integrated set of tools.

The cyber security strategy known as XDR (Extended Detection and Response) is recognized for its success in mitigating advanced threats. This covers several crucial areas for incident protection and response, being made available by Wazuh, albeit with

associated costs. Some of these capabilities include:

- Behavioral analysis, which evaluates behaviors to detect anomalies, such as out-of-hours access or attempts to access unauthorized directories.
- Threat hunting, which proactively identifies suspicious network activity, enabling early detection of hazards.
- Protecting workloads in the cloud, ensuring data security in cloud environments.
- The use of threat intelligence to improve incident detection and response and make strategic security decisions.
- The generation of compliance reports to monitor security and comply with regulations.
- This combination of competencies enables businesses to meet the complex challenges of today's threat landscape, making Extended Detection and Response (XDR) a crucial strategy for ensuring the resilience and security of IT infrastructures.

# References

- [1] Maziana Abd Majid and Khairul Akram Zainol Ariffin. “Model for successful development and implementation of Cyber Security Operations Centre (SOC)”. In: *PLOS ONE* 16.11 (Nov. 2021). Ed. by Rogis Baker. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0260157. URL: <http://dx.doi.org/10.1371/journal.pone.0260157>.
- [2] Região Autónoma dos Açores - Assembleia Legislativa. “Decreto Legislativo Regional n.º 22/2015/A, de 18 de setembro”. In: *Journal Oficial Série I Número 131* (2015). URL: <https://diariodarepublica.pt/dr/detalhe/decreto-legislativo-regional/22-2015-70325360>.
- [3] Roaa Aljuraid and Taghreed Justinia. “Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review”. In: *Advances in Informatics, Management and Technology in Healthcare*. IOS Press, June 2022. DOI: 10.3233/shti220739. URL: <http://dx.doi.org/10.3233/shti220739>.
- [4] Salem T. Argaw et al. “Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks”. In: *BMC Medical Informatics and Decision Making* 20.1 (July 2020), p. 8. ISSN: 1472-6947. DOI: 10.1186/s12911-020-01161-7. URL: <http://dx.doi.org/10.1186/s12911-020-01161-7>.
- [5] Virginia Braun et al. “The online survey as a qualitative research tool”. In: *International Journal of Social Research Methodology* 24.6 (Aug. 2020), pp. 641–654. ISSN: 1464-5300. DOI: 10.1080/13645579.2020.1805550. URL: <http://dx.doi.org/10.1080/13645579.2020.1805550>.

- [6] L. Brito. *Pequeno Guiade Inquérito por Questionário*. IESE – Instituto de Estudos Sociais e Económicos, 2012. URL: [https://www.iese.ac.mz/wp-content/uploads/2015/12/IESE\\_PequenoGuia.pdf](https://www.iese.ac.mz/wp-content/uploads/2015/12/IESE_PequenoGuia.pdf).
- [7] Miguel Pinto Caldas. “Research design: qualitative, quantitative, and mixed methods approaches”. In: *Revista de Administração Contemporânea* 7.1 (Mar. 2003), pp. 223–223. ISSN: 1415-6555. DOI: 10.1590/s1415-65552003000100015. URL: <http://dx.doi.org/10.1590/s1415-65552003000100015>.
- [8] M. Carmo and A. Ferreira. “Metodologia da investigação : guia para auto-aprendizagem”. In: *Repositório Aberto* (2015). URL: <https://repositorioaberto.uab.pt/handle/10400.2/5963>.
- [9] Ransomware Center. *Infection with WanaCrypt2-pl virus*. Accessed on August 21, 2023. 2023. URL: <https://ransomware.center/virus-wanacrypt2-pl.html>.
- [10] Centro Nacional de Cibersegurança. *Guia para Gestão dos Riscos em matérias de Segurança da Informação e cibersegurança. v1.1*. 2022. URL: <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf>.
- [11] CNCS. “Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança”. In: *Observatório de Cibersegurança* (Apr. 2022), pp. 13–14. URL: <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf>.
- [12] CNCS. “Relatório Cibersegurança em Portugal”. In: (Dec. 2021). URL: <https://www.cncs.gov.pt/docs/relatorio-sociedade2021-observ-cnccs.pdf>.
- [13] European Commission. *Proposal for a Regulation of The European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. 2022. URL: [https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF).
- [14] Presidência do Conselho de Ministros. “Decreto Lei 65/2021, de 30 de Julho”. In: *Diário da República n.º 147/2021, Série I* (2021). URL: <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

- [15] C. P. Coutinho. *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática*. Coimbra: Almedina, 2011. ISBN: 9789724051376.
- [16] CVEdetails.com. *Wazuh : Security Vulnerabilities*. Accessed on August 16, 2023. 2023. URL: [https://www.cvedetails.com/vulnerability-list/vendor\\_id-19545/product\\_id-51675/Wazuh-Wazuh.html](https://www.cvedetails.com/vulnerability-list/vendor_id-19545/product_id-51675/Wazuh-Wazuh.html).
- [17] Fábio Martins Dias et al. “Risk management focusing on the best practices of data security systems for healthcare”. In: *International Journal of Innovation* 9.1 (Apr. 2021), pp. 45–78. ISSN: 2318-9975. DOI: 10.5585/iji.v9i1.18246. URL: <http://dx.doi.org/10.5585/iji.v9i1.18246>.
- [18] Marco Eichelberg, Klaus Kleber, and Marc Kammerer. “Cybersecurity in PACS and Medical Imaging: an Overview”. In: *Journal of Digital Imaging* 33.6 (Oct. 2020), pp. 1527–1542. ISSN: 1618-727X. DOI: 10.1007/s10278-020-00393-3. URL: <http://dx.doi.org/10.1007/s10278-020-00393-3>.
- [19] ENISA. *CIRAS Incident Reporting*. Accessed on August 12, 2023. 2023. URL: <https://ciras.enisa.europa.eu>.
- [20] ENISA. “ENISA Threat Landscape 2022”. In: (Nov. 2022). URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>.
- [21] ENISA. “ENISA Threat Landscape Health Sector 2022”. In: (July 2023). URL: <https://www.enisa.europa.eu/publications/health-threat-landscape/>.
- [22] ENISA. *Smart hospitals: security and resilience for smart health service and infrastructures, European Network and Information Security Agency*. 2016. URL: <https://data.europa.eu/doi/10.2824/28801>.
- [23] Jennifer K. Felner and Vida Henderson. “Practical Strategies for Health Equity Researchers to Enhance Analytic Rigor and Generate Meaningful Insights From Qualitative Data”. In: *Preventing Chronic Disease* 19 (Nov. 2022). DOI: 10.5888/pcd19.220134. URL: <https://doi.org/10.5888/pcd19.220134>.
- [24] Barbara Filkins. *SANS - SIEM NEXTGEN*. 2018. URL: <https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf>.

- [25] GARTNER. *Magic Quadrant For Security Information and Event Management*. 2022. URL: <https://www.gartner.com/doc/reprints?id=1-2BDC4CEU&ct=221010&st=sb>.
- [26] R. Ghiglione and B. Matalon. *O Inquérito: Teoria e Prática*. 4th ed. Celta editora, 2001.
- [27] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz. “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures”. In: *Sensors* 21.14 (July 2021). ISSN: 1424-8220. DOI: 10.3390/s21144759. URL: <http://dx.doi.org/10.3390/s21144759>.
- [28] M. M. Hill. *Desenho de questionário e análise dos dados - alguns contributos*. Edições Húmus, 2014.
- [29] HIMSS. *Protecting Digital Health Systems and Patient Information: Five key takeaways from a HIMSS APAC Cybersecurity and Privacy Government Virtual Roundtable*. 2021. URL: <https://www.himss.org/sites/hde/files/media/file/2022/04/25/apac-cybersecurity-and-privacy-government-roundtable-report.pdf>.
- [30] IBM. *What is EDR (endpoint detection and response)?* Accessed on July 13, 2023. 2023. URL: <https://www.ibm.com/topics/edr>.
- [31] A. LE BRIS and W. EL ASRI. *State of Cybersecurity and Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers*. Aug. 2020. URL: [https://f.hubspotusercontent00.net/hubfs/8011857/Admere\\_August2020/Images/risks-and-threats-healthcare-strategic-report.pdf](https://f.hubspotusercontent00.net/hubfs/8011857/Admere_August2020/Images/risks-and-threats-healthcare-strategic-report.pdf).
- [32] Região Autónoma da Madeira - Assembleia Legislativa. “Decreto Legislativo Regional n.º 8/2020/M, de 13 de julho”. In: *Journal Oficial Série I Número 131* (2020). URL: <https://joram.madeira.gov.pt/joram/1serie/Ano%20de%202020/ISerie-131-2020-07-13.pdf>.
- [33] Trend Micro. *O que é o Ransomware RYUK?* Accessed on August 21, 2023. 2023. URL: [https://www.trendmicro.com/pt\\_br/what-is/ransomware/ryuk-ransomware.html](https://www.trendmicro.com/pt_br/what-is/ransomware/ryuk-ransomware.html).

- [34] Matthew B. Miles, A. Michael Huberman, and J Saldaña. *Qualitative Data Analysis: A Methods Sourcebook*. 3rd ed. Sage Publications Inc, 2014. ISBN: 978-1-4522-5787-7.
- [35] Robert E. Moffit. *Health Care Data Breaches: A Changing Landscape*. June 2017. URL: [https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT\\_DataBreachesBrief\\_Brf\\_Rpt\\_090717.pdf](https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_DataBreachesBrief_Brf_Rpt_090717.pdf).
- [36] Janice M. Morse. *Essentials of Qualitatively-Driven Mixed-Method Designs*. Routledge, July 2016. ISBN: 9781315543406. DOI: 10.4324/9781315543406. URL: <http://dx.doi.org/10.4324/9781315543406>.
- [37] Sokratis Nifakos et al. “Influence of Human Factors on Cyber Security within Health-care Organisations: A Systematic Review”. In: *Sensors* 21.15 (July 2021), p. 17. ISSN: 1424-8220. DOI: 10.3390/s21155119. URL: <http://dx.doi.org/10.3390/s21155119>.
- [38] European Parliament and Of the Council. “Regulation(EU) 2016/679, April 27”. In: *Official Journal of the European Union* (2016). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
- [39] Portugal. “Regime Jurídico do Ciberespaço. Lei n.º 46/2018, de 13 de agosto”. In: *Diário da República Portuguesa* (2018), pp. 4031–4037. URL: <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.
- [40] Bernardi Pranggono and Abdullahi Arabo. “COVID-19 Pandemic Cybersecurity Issues”. In: *Internet Technology Letters* 4.2 (Oct. 2020). ISSN: 2476-1508. DOI: 10.1002/itl2.247. URL: <http://dx.doi.org/10.1002/itl2.247>.
- [41] Colin Reid. *Searching for a SIEM Solution? Here Are 7 Things It Likely Needs*. 2023. URL: <https://www.gartner.com/en/articles/searching-for-a-siem-solution-here-are-7-things-it-likely-needs>.
- [42] A. et al Richard. “CERT® Resilience Management Model, Version 1.2”. In: (Feb. 2016). Ed. by CERT Program. URL: [https://insights.sei.cmu.edu/documents/1629/2016\\_002\\_001\\_514462.pdf](https://insights.sei.cmu.edu/documents/1629/2016_002_001_514462.pdf).

- 
- [43] Nuno Saldanha. *Guia Para Uma Auditoria De Conformidade- Dados, Privacidade, Implementação, Controlo E Compliance*. FCA – Editora de Informática, 2019, pp. 131–132. ISBN: 978-972-722-905-5.
- [44] Ministério da Saúde. “Decreto Lei n.º 12/2015, de 26 de janeiro”. In: *Journal Oficial Série I* (2015). URL: <https://diariodarepublica.pt/dr/detalhe/decreto-lei/12-2015-66325236>.
- [45] Ministério da Saúde. “Decreto Lei n.º 233/2005, de 29 de dezembro”. In: *Journal Oficial Série I-A* (2005). URL: <https://diariodarepublica.pt/dr/detalhe/decreto-lei/233-2005-469067>.
- [46] Ministério da Saúde. “Decreto Lei n.º 27/2002, de 8 de novembro”. In: *Journal Oficial Série I* (2002). URL: <https://diariodarepublica.pt/dr/detalhe/lei/27-2002-425487>.
- [47] Serviço Nacional de Saúde. *Entidades de Saúde do SNS*. Accessed on April 11, 2023. 2023. URL: <https://www.sns.gov.pt/institucional/entidades-de-saude/>.
- [48] Serviço Nacional de Saúde. *História do SNS*. Accessed on April 11, 2023. 2023. URL: <https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/>.
- [49] *Security and Privacy Controls for Information Systems and Organizations*. Sept. 2020. DOI: 10.6028/nist.sp.800-53r5. URL: <http://dx.doi.org/10.6028/NIST.SP.800-53r5>.
- [50] *SIEM Architecture*. Accessed on May 5, 2023. 2020. URL: <https://www.tutorialandexample.com/siem-tools>.
- [51] A. Sousa and B. Baptista. *Como Fazer Investigação, Dissertações, Teses e Relatórios*. Vol. Número do Volume. Pactor, 2011, p. 56. ISBN: SBN: 978-989-693-001-1.
- [52] M. Swanson et al. “Contingency Planning Guide for Federal Information Systems”. In: *NIST Special Publication 800-34 Rev. 1* (2010), pp. 8–9. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>.



- [53] William Triplett. “Ransomware Attacks on the Healthcare Industry”. In: *Journal of Business, Technology and Leadership* 4.1 (Apr. 2022), pp. 1–13. ISSN: 2768-1300. DOI: 10.54845/btljournal.v4i1.31. URL: <http://dx.doi.org/10.54845/btljournal.v4i1.31>.
- [54] A. Veiga et al. “Estudo Sobre o Ensino Pós-Secundário e o Ensino Superior de Cibersegurança em Portugal”. In: *Observatório de Cibersegurança* (Apr. 2022), pp. 13–14. URL: <https://www.cncs.gov.pt/docs/estudo-ensino-ciberseg-cncs.pdf>.
- [55] Guangxu Wang et al. “An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation”. In: *Sustainability* 14.14 (July 2022), p. 8319. DOI: 10.3390/su14148319. URL: <https://doi.org/10.3390/su14148319>.
- [56] Wazuh. *Emotet Malware Detection*. Accessed on August 19, 2023. 2023. URL: <https://wazuh.com/blog/emotet-malware-detection/>.
- [57] Wazuh. *Getting started with WazuhComponents*. Accessed on June 22, 2023. 2023. URL: <https://documentation.wazuh.com/current/getting-started/components/index.html>.
- [58] Wazuh. *Wazuh Agent Architecture*. Accessed on August 18, 2023. 2023. URL: <https://documentation.wazuh.com/current/getting-started/components/wazuh-agent.html>.
- [59] Wazuh. *Wazuh Agent Package Linux*. Accessed on June 22, 2023. 2023. URL: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>.
- [60] Wazuh. *Wazuh deployment architecture*. 2023. URL: <https://documentation.wazuh.com/current/getting-started/architecture.html>.
- [61] Richard Zuech, Taghi M Khoshgoftaar, and Randall Wald. “Intrusion detection and Big Heterogeneous Data: a Survey”. In: *Journal of Big Data* 2.1 (Feb. 2015), pp. 21–22. ISSN: 2196-1115. DOI: 10.1186/s40537-015-0013-4. URL: <http://dx.doi.org/10.1186/s40537-015-0013-4>.

# Appendices

# Appendix A

## Appendices

### A Survey

List of survey questions by role:

- IT Director
  1. What is your opinion on the importance of cybersecurity for a hospital?
  2. What is the role of the IT/IS department in implementing cybersecurity measures in the hospital?
  3. How do you assess the growth of cybersecurity threats in the healthcare sector, and what measures does the IT/IS department take to protect the hospital against these threats?
  4. What is your experience implementing a SIEM in hospitals?
  5. In your opinion, do you believe that the implementation of a SIEM) can improve system security and the privacy of patient/employee data?
  6. Does your institution currently have an SIEM implemented? If not, are you planning to implement one in the short, medium, or long term?
  7. What are the main challenges you know about implementing an SIEM in the hospital?
  8. Are you aware of any cases where the use of a SIEM helped keep the hospital more cybersecure?

9. What are your expectations for the future of cybersecurity in the healthcare sector, and how is the IT department preparing for these changes?

10. With the increasing use of AI, do you believe that SIEM with AI can be an asset in the future?

- IT Director/CISO

1. How do you assess the importance of investing in cybersecurity for the hospital?

2. What is the role of the CISO (Head of Security) in planning and implementing cybersecurity measures in the hospital?

3. What is your opinion about the implementation of an Information Management System for security events in hospitals?

4. What is your experience implementing a SIEM in hospitals?

5. In your opinion, do you believe that the implementation of a SIEM can improve system security and the privacy of patient/employee data?

6. Does your institution currently have a SIEM implemented? If not, are you planning to implement one in the short, medium, or long term?

7. What are the main challenges you know about implementing a SIEM in the hospital?

8. Are you aware of any cases where the use of a SIEM helped keep the hospital more cybersecure?

9. What are your expectations for the future of cybersecurity in the healthcare sector, and how is the IT department preparing for these changes?

10. With the increasing use of AI, do you believe that SIEM with AI can be an asset in the future?

- CISO

1. How do you assess the importance of investing in cybersecurity for the hospital?

2. What is the role of the CISO (Head of Security) in planning and implementing cybersecurity measures in the hospital?

3. What is your opinion about the implementation of an SIEM system for security events in hospitals?
4. What is your experience implementing a SIEM in hospitals?
5. In your opinion, do you believe that the implementation of a SIEM can improve system security and the privacy of patient/employee data?
6. Does your institution currently have a SIEM implemented? If not, are you planning to implement one in the short, medium, or long term?
7. What are the main challenges you know about implementing a SIEM in the hospital?
8. Are you aware of any cases where the use of a SIEM helped keep the hospital more cybersecure?
9. What are your expectations for the future of cybersecurity in the healthcare sector, and how is the IT department preparing for these changes?
10. With the increasing use of AI, do you believe that SIEM with AI can be an asset in the future?

- System administrator

1. How do you assess the importance of investing in cybersecurity for the hospital?
2. What is the systems administrator's role in planning and implementing cybersecurity measures in the hospital?
3. What is your opinion about the implementation of an Information Management System for security events in hospitals?
4. Does your institution currently have a SIEM implemented? If not, are there any plans to implement it in the short, medium, or long term?
5. Have you implemented or helped to implement a SIEM in a hospital?
6. What are the main challenges you know in implementing a SIEM in the hospital?
7. Can you share any examples of how a SIEM helps or can help to detect and prevent security threats in the hospital?

8. How do you evaluate the potential of using a SIEM to improve the cybersecurity of a hospital more efficiently?
9. How do you see the future of cybersecurity in hospitals, and how is the hospital's IT/IS department preparing for new challenges?
10. Do you believe that AI will make an important contribution to SIEMs in the future?

## B Collaboration Request Email

### Collaboration requests sent by email

Para: [REDACTED]@arsnorte.min-saude.pt qui, 17/08/2023 23:46  
Cc: [REDACTED]  
Boa noite Enf.º [REDACTED].

Sou aluno do mestrado em Cibersegurança no Instituto Politécnico de Viana do Castelo, e encontro-me neste momento a terminar a dissertação subordinada ao tema: "*Analysis of Implementation of a Security Information and Event's Management System in E.P.E Hospitals*".

Venho por este meio solicitar encarecidamente a sua colaboração, em particular na realização de uma entrevista, visando colocar-lhe algumas questões sobre a cibersegurança e o setor da saúde.

Agradeço, desde já, toda a sua atenção e disponibilidade!  
Com os meus melhores cumprimentos,

Emanuel Gonçalves  
e.goncalves@ipvc.pt

Figure A.1: Email sent to ACeS Cabreira/Gerês. Source: The author

Para: [REDACTED] sex, 04/08/2023 11:41  
Bcc: [REDACTED]  
Bom dia!

Sou aluno do mestrado em Cibersegurança no Instituto Politécnico de Viana do Castelo, e encontro-me neste momento a terminar a dissertação subordinada ao tema: "*Analysis of Implementation of a Security Information and Event's Management System in E.P.E Hospitals*". Venho por este meio solicitar encarecidamente a sua colaboração, em particular na resposta a este pequeno questionário de 3 perguntas:

1. Os SPMS são responsáveis por grande parte da cibersegurança dos hospitais. Contudo, considera que os hospitais portugueses, em geral, estão com grande nível de maturidade relativamente a este tema ou ainda há muito caminho a percorrer?
2. Em seu entendimento, acredita que a implementação de um Sistema de Gestão de Informações e Eventos de Segurança (SIEM) pode melhorar a segurança dos sistemas e da informação num hospital?
3. Que conselho deixaria aos responsáveis pela cibersegurança dos hospitais relativamente a uma futura implementação de um SIEM nas organizações?

Agradeço, desde já, toda a sua atenção e disponibilidade!  
Com os meus melhores cumprimentos,

Emanuel Gonçalves  
e.goncalves@ipvc.pt

Figure A.2: Email sent to SPMS. Source: The author

Para: [REDACTED]  
Bcc: eagdpo@gmail.com

sex, 18/08/2023 18:13

Ex.º Sr. Diretor Executivo do SNS, [REDACTED].

Sou aluno do Mestrado em Cibersegurança no Instituto Politécnico de Viana do Castelo, e encontro-me neste momento a terminar a dissertação subordinada ao tema: "*Analysis of Implementation of a Security Information and Event's Management System in E.P.E Hospitals*".

O meu estudo e percurso académico tem se centrado em 3 temáticas, nomeadamente: Desenvolvimento de 'software' seguro, Privacidade/Proteção de dados, e Cibersegurança em geral e no setor da saúde.

Venho por este meio solicitar encarecidamente a sua colaboração, em particular necessitava da sua opinião enquanto Diretor Executivo do SNS, sobre as seguintes questões:

1. Considera que os meios logísticos e humanos dedicados à cibersegurança no SNS, em particular nas unidades hospitalares (hospitais, centros hospitalares, ULS e IPO) são satisfatórios?
2. As reformas que tenciona implementar no SNS contemplam medidas que procuram aumentar a cibersegurança para o setor da saúde? Se sim quais?
3. Verifica-se que muitas das ocorrências que afetam e comprometem a confidencialidade, a integridade e a disponibilidade, acontecem por falta de informação/formação dos colaboradores do SNS, sobre boas-práticas, independentemente da formação académica ou literacia informática. Existe algum plano formativo, para o futuro do SNS, de modo a melhorar esta lacuna?

O seu contributo vai servir para enriquecer o meu estudo, e penso que poderá contribuir para melhorar a cibersegurança no setor da saúde no futuro. Aproveito para pedir-lhe a devida autorização, para incluir as suas respostas na minha dissertação de mestrado.

Agradeço, desde já, toda a sua atenção e disponibilidade!  
Com os meus melhores cumprimentos,

Emanuel Gonçalves  
[REDACTED]  
e.goncalves@ipvc.pt

Figure A.3: Email sent to Executive SNS. Source: The author