



INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Healthcare Systems Protection: All-in-one cybersecurity approach

Bruno Filipe Passos Ferraz Coutinho

Master in Computer Engineering

Supervisor:

PhD Vitor Manuel Basto Fernandes, Assistant Professor with
Habilitation

Iscte – Instituto Universitário de Lisboa

November, 2021

Department of Information Science and Technology

Healthcare Systems Protection: All-in-one cybersecurity approach

Bruno Filipe Passos Ferraz Coutinho

Master in Computer Engineering

Supervisor:

PhD Vitor Manuel Basto Fernandes, Assistant Professor with
Habilitation

Iscte – Instituto Universitário de Lisboa

November, 2021

To my family, Salvador and J  ssica for their love, inspiration, unconditional support, encouragement, patience and help overcome the obstacles that come the way. This work, as well as all my love, is dedicated to you.

Acknowledgements

I would like to acknowledge my beautiful family and my mother for providing all the motivation, inspiration, and emotional support I needed in this challenge. Without them, it would not be possible to be writing this new page of my life.

I'd want to express my gratitude to Dr. Vitor Basto Fernandes for his assistance, critical thinking and supervision. Dr. João Ferreira deserves special thanks for all of his help, advice, and recommendations, which were critical to the success of this project.

To all friends and colleagues who contributed to or assisted in the preparation of this work, thank you for your patience, attention, and fortitude during the difficult times.

Finally, a note to ISCTE - Instituto Universitário de Lisboa and all the faculty and non-teaching staff for the opportunity.

To all, my sincere gratitude,

Bruno Ferraz Coutinho.

Resumo

Os riscos cibernéticos estão cada vez mais difundidos à medida que as organizações de cuidados de saúde desempenham um papel determinante na sociedade. Vários estudos revelaram um aumento das ameaças de cibersegurança no setor, o que nos deve preocupar a todos.

Quando se trata de cibersegurança, as consequências podem ser sentidas em toda a organização, desde os mais pequenos processos até à sua capacidade global de funcionamento. Normalmente, um ciberataque resulta na divulgação de informações confidenciais que colocam em causa a sua vantagem competitiva e a confiança geral. O healthcare como setor crítico apresenta, como muitos outros setores, uma aposta tardia na sua transformação para a cibersegurança de forma generalizada.

Esta dissertação reforça esta necessidade apresentando uma solução de valor acrescentado que ajuda a potenciar os processos internos das unidades de saúde possibilitando a sua missão principal de salvar vidas, aumentando a garantia de confidencialidade e segurança dos dados dos pacientes e instituições.

A solução apresenta-se como um compósito tecnológico que se traduz numa metodologia e artefacto de inovação para integração, monitorização e segurança de infraestruturas médicas críticas baseado em use cases de operação.

A abordagem que envolve pessoas, processos e tecnologia assenta num modelo que prevê a avaliação de potenciais ativos para integração e monitorização, como conta alavancar a eficiência na resposta a incidentes de segurança com o desenvolvimento formal de um processo e mecanismos para alerta e resolução de cenários de exposição e ataque.

O artefacto, a nível tecnológico, conta com a integração do sistema de arquivo de imagem médica (PACS) num SIEM para validação de logs aplicativos que estão associados a regras que mapeiam comportamentos anómalos que originam o despoletar do processo de gestão de incidentes numa plataforma IHS com funcionalidades desenvolvidas à medida.

A escolha para integração no protótipo de validação do sistema PACS tem por base não só a sua importância na orquestração de atividades na orgânica duma instituição de saúde, mas também com as recentes recomendações de várias agências e organizações de cibersegurança para a importância da sua proteção em resposta às últimas tendências de ciberataques.

Em linha com os resultados auscultados, esta abordagem terá total aplicabilidade em contexto real de operação, seguindo as mais recentes práticas e tecnologias no sector.

Palavras-Chave: Cibersegurança, Proteção de Infraestruturas Críticas, Sistemas de Informação de Saúde, Sistemas de Controlo Industrial, Ciberataque, Resposta a Incidentes

Abstract

Cyber risks are increasingly widespread as healthcare organizations play a defining role in society. Several studies have revealed an increase in cybersecurity threats in the industry, which should concern us all.

When it comes to cybersecurity, the consequences can be felt throughout the organization, from the smallest processes to the overall ability of the organization to function. Typically, a cyberattack results in the disclosure of confidential information that undermines your competitive advantage and overall trust. Healthcare as a critical sector has, like many other sectors, a late bet on its transformation to cybersecurity across the board.

This dissertation reinforces this need by presenting a value-added solution that helps strengthen the internal processes of healthcare units, enabling their primary mission of saving lives while ensuring the confidentiality and security of patient and institutional data.

The solution is presented as a technological composite that translates into a methodology and innovative artifact for integration, monitoring, and security of critical medical infrastructures based on operational use cases.

The approach that involves people, processes, and technology is based on a model that foresees the evaluation of potential assets for integration and monitoring, as well as leveraging the efficiency in responding to security incidents with the formal development of a process and mechanisms for alert and resolution of exposure and attack scenarios.

On a technical level, the artifact relies on the integration of a medical image archiving system (PACS) into a SIEM to validate application logs that are linked to rules to map anomalous behaviors that trigger the incident management process on an IHS platform with custom-developed features.

The choice for integration in the validation prototype of the PACS system is based not only on its importance in the orchestration of activities in the organization of a health institution, but also with the recent recommendations of various cybersecurity agencies and organizations for the importance of their protection in response to the latest trends in cyberattacks.

In line with the results obtained, this approach will have full applicability in a real operational context, following the latest practices and technologies in the sector.

Keywords: Cybersecurity, Critical Infrastructure Protection, Healthcare Information Systems, Industrial Control Systems, Cyberattack, Incident Response

Contents

Acknowledgements.....	iii
Resumo.....	v
Abstract.....	vii
List of Figures	xi
List of Tables	xii
Acronyms.....	xiii
Chapter 1.....	1
Introduction.....	1
1.1 Overview	5
1.2 Motivation	5
1.3 Objectives.....	7
1.4 Methodology.....	7
1.5 Dissertation Outline.....	10
Chapter 2.....	11
Related Work	11
2.1 Operational Technology	14
2.2 Industrial Control Systems	15
2.3 Cybersecurity Monitoring and Analysis	18
2.4 Intrusion Detection Systems	19
2.5 Intrusion Detection in Critical Systems	20
2.6 Protection of Health Critical Systems.....	22
2.6.1 Healthcare Landscape.....	22
2.6.2 Protecting Confidentiality of Patient Process.....	23
2.6.3 Picture Archive and Communication Systems (PACS).....	24
2.7 Incident Management.....	26
2.7.1 ISO /IEC 27035 - Incident Response Standard.....	26
Chapter 3.....	29
HSMS – Design & Development	29
3.1 Design – Healthcare Systems Integration Security Methodology.....	29
3.2 Development – Healthcare Security Monitor System.....	33
3.3 Cyber.SCuris.....	35
3.3.1 Health Critical System Simulation.....	35
3.3.2 SIEM Active Monitoring	38
3.3.3 Use Cases & Rules Check.....	40
3.3.4 Incident Management Process and Incident Resolution	43

Chapter 4.....	50
Demonstration & Evaluation	50
4.1 Demonstration Scenario	51
4.2 Evaluation.....	52
4.2.1 Expert panel.....	54
4.2.2 1 st DSRM Iteration	55
4.2.3 2 nd DSRM Iteration.....	56
4.2.4 3 rd DSRM Iteration.....	59
Chapter 5.....	61
Conclusions & Future Work	61
5.1 Conclusions	61
5.2 Future Work.....	63
References	64

List of Figures

FIGURE 1: HEALTHCARE INDUSTRY CYBERATTACK TRENDS DURING CORONAVIRUS PANDEMIC [9]..	3
FIGURE 2: INDUSTRIES TARGETED BY RANSOMWARE - Q4 2020 [9].....	3
FIGURE 3: DSRM PROCESS MODEL (PEFFERS ET AL., 2008) [17]	8
FIGURE 4: PRISMA FLOW DIAGRAM [18].....	12
FIGURE 5: APPLICABILITY AND INCLUSION CRITERIA - LIST OF PAPERS.....	12
FIGURE 6: IT VS OT: THE EVOLUTION OF THE THREAT LANDSCAPE, INSPIRED ON [20].....	15
FIGURE 7: ARCHITECTURE EXPLAINED OF ICS [23]	16
FIGURE 8: INDUSTRIAL CONTROL SYSTEMS - SCADA PROTOCOLS [21]	17
FIGURE 9: CHARACTERIZATION OF INTRUSION DETECTION SYSTEM TYPES [23].....	21
FIGURE 10: BREACH TRENDS - HEALTHCARE INDUSTRY [45].....	22
FIGURE 11: ALL-IN-ONE HEALTHCARE SECURITY INCIDENT RESPONSE METHODOLOGY.....	30
FIGURE 12: DIFFICULTY VS MATURITY DATA SOURCES DEFINITION - GARTNER [54].....	30
FIGURE 13: SYSTEM INTEGRATION ASSESSMENT.....	31
FIGURE 14: HSMS: PROCESS AND TECHNOLOGICAL MAPPING.....	32
FIGURE 15: ARTIFACT CYBER.SCURIS – DEVELOPMENT	33
FIGURE 16: INITIAL PAGE ORTHANC SERVER.....	36
FIGURE 17: WORK ENVIRONMENT - ONIS DICOM VIEWER	36
FIGURE 18: LOGIC SCHEME - COMMUNICATION	37
FIGURE 19: SPLUNK ENTERPRISE: ALERTS PANEL	38
FIGURE 20: COMMUNICATION INTEGRATION SIEM AND HEALTH PLATFORM, SELF-MADE	39
FIGURE 21: USE CASE TRIANGLE METHOD, SELF-MADE INSPIRED ON GARTNER [54].....	42
FIGURE 22: ALL-IN-ONE INCIDENT MANAGEMENT PROCESS AND INCIDENT RESOLUTION	43
FIGURE 23: ALL-IN-ONE INCIDENT RESPONSE PROCEDURE	45
FIGURE 24: NETWORK PACKET COLLECTION REPRESENTATION.....	45
FIGURE 25: TYPES OF INTERFACES TO MONITOR.....	46
FIGURE 26: NETWORK CAPTURE AND PATTERN ANALYSIS.....	47
FIGURE 27: DICOM - CAPTURE FILTER.....	48
FIGURE 28: EVIDENCE IDENTIFICATION STEP	48
FIGURE 29: DOCUMENTATION STEP.....	49
FIGURE 30: VALIDATION: DEMONSTRATION SCENARIO	51
FIGURE 31: DSRM ITERATION CYCLES.....	52
FIGURE 32: HIERARCHY OF CRITERIA: ARTIFACT EVALUATION, PRAT ET AL. [56].....	53
FIGURE 33: AUTOMATIC INTEGRATION OF INCIDENTS ALERT FROM SPLUNK	56
FIGURE 34: AUTOMATIC ASSIGNEE OF CASES RESOLUTION.....	57
FIGURE 35: INCIDENT ALERT CREATION.....	59

FIGURE 36: CHATBOT AUTOMATIC MESSAGE - REMOTE ALERT.....	59
--	----

List of Tables

TABLE 1: USE CASES DEFINITION.....	41
TABLE 2: CHARACTERISTICS OF EXPERT PANEL – RESUME	54
TABLE 3: RESULTS OF 1ST ITERATION.....	55
TABLE 4: RESULTS OF 2ND ITERATION	58
TABLE 5 - RESULTS OF 3RD ITERATION	60

Acronyms

API – **A**pplication **P**rogramming **I**nterface

CPS – **C**yber **P**hysical **S**ystems

CPU - **C**entral **P**rocess **U**nit

DICOM - **D**igital **I**maging and **C**ommunications in **M**edicine

DSRM - **D**esign **S**cience **R**esearch **M**ethodology

ENISA - **E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency

HIPAA – **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

HIS – **H**ealth **I**nformation **S**ystem

HIT – **H**ealth **I**nformation **T**echnology

HL7 – **H**ealth **L**evel **S**even – **P**rotocol

HMI – **H**uman **M**achine **I**nterface

HSMS - **H**ealth **S**ecurity **M**onitor **S**ystem

ICS – **I**ndustrial **C**ontrol **S**ystem

IDS – **I**ntrusion **D**etection **S**ystem

IHS – **I**ncident **H**andling **S**ystem

IR – **I**ncident **R**esponse

IS – **I**nformation **S**ystems

IT – **I**nformation **T**echnology

MTU – **M**aster **T**erminal **U**nit

OSS – **O**pen-source **S**oftware

OT – **O**perational **T**echnology

PACS - **P**icture **A**rchiving and **C**ommunication **S**ystems

PLC – **P**rogrammable **L**ogic **C**ontroller

PRISMA - **P**referred **R**eporting **I**tems for **S**ystematic **R**eviews and **M**eta-**A**nalyses

RTU – **R**emote **T**erminal **U**nit

SCADA – **S**upervision **C**ontrol **A**nd **D**ata **A**cquisition

SIEM – **S**ecurity **I**nformation and **E**vent **M**anagement

SOP – **S**tandard **O**perating **P**rocedure

TLS – **T**ransport **L**ayer **S**ecurity

Chapter 1

Introduction

Recent studies indicate an increase in cybersecurity threats to the healthcare industry that are alarming. Because healthcare institutions are so important, cyber threats are becoming more common [1].

It all starts with critical systems that can often be confused with common industrial control systems that are component networks such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that act in the control of field devices as sensors [2].

These two types of networks systems are the turntable for orchestrating industrial infrastructure essential for human survival: energy exploration, railways, water treatment and healthcare.

The one of the most well-known systems is Supervisory Control and Data Acquisition (SCADA) systems that monitor this type of infrastructure and combine data sensing, acquisition and proprietary communications protocols to monitor and control the equipment and processes involved are often called Cyber Physical Systems (CPS) [3].

Typically, these communication networks are isolated, distributed over a wide geographical location and are centrally controlled in corporate networks [2].

We have numerous recent examples of cyberattacks carried out in control systems as a result of the paradigm shift at the worldwide level and as a result of strategic positioning and the advancement of the lethality of cyberattacks.

In 2015 [4], we had the case of the attack on the Ukrainian public energy company that caused the service disruption to almost 250,000 customers or else the case that awakened to new reality about cyberwarfare with the Stuxnet case [5].

The worm had two functions. The first was to get the centrifuges in the nuclear park to start spinning at 40% more than the normal speed for fifteen minutes, which caused cracks in the aluminum structures. The second form initially recorded telemetric data from a typical normal operation of nuclear centrifuges, without the alarm sounding, and then reproducing this record for the equipment operators while the machines were literally detonating under the action of Stuxnet without them knowing [4].

Since the emergence of industrial control systems (ICS) between 1982 and 2012 [5], fifteen cyber-attacks against these infrastructures have been described. After the appearance of Stuxnet, there were numerous attacks or attempts to attack, using derivations of the initial code that was made available for investigation. In the last year, cases like Trickbot, Ryuk and Conti which are attacks that perpetrated as ransomware are common names among security professionals who manage healthcare infrastructures [6].

This type of attacks can be taken care of using signature-based or anomaly-based Intrusion Detection Systems [7]. Intrusion Detection Systems are security systems designed to enhance network and device security by detecting activities such as cyber-attacks on a computer system or a network. For previously reported cases of zero-day vulnerabilities, anomaly-based IDS will be more effective because they do not have a closed understanding of a possible trigger.

For example, in the case of anomaly detection, there is a common traffic analysis baseline that allows to perceive deviations from the expected pattern, indicating eventual attacks that are exploiting unfamiliar vulnerabilities, requiring investigation and corresponding countermeasures [7].

Zero-day vulnerabilities are vulnerabilities which were previously unknown, meaning no patches, or signatures of these vulnerabilities are known to the public, increasing the likelihood the vulnerabilities can be exploited [7].

By directing our work to a specific area of analysis, we can realize that the healthcare sector is one of the most affected by cyberattacks [8]. The COVID-19 pandemic has contributed to an increase in the number of cyber-attacks against healthcare organizations. Ransomware assaults, phishing exploits, false accounts, misinformation campaigns and supply chain disruptions are risks currently facing the healthcare sector [8].

According to [8], coronavirus-related cyber-attacks, disruption of the supply chain could be the next major health hazard if the manufacture and delivery of ventilators, medical supplies and medications were to be interrupted for a long period of time or become inaccessible.

As COVID-19 patient care threatens to overwhelm the healthcare system, doctors switch from in-office visits to virtual visits to protect frontline medical personnel and staff from infection and to mitigate the spread of Coronavirus [8].

Since the end of 2019 and during the 2020 years, several cyber-attacks have been carried out on healthcare and service organizations responsible for supporting people during this health emergency [9].

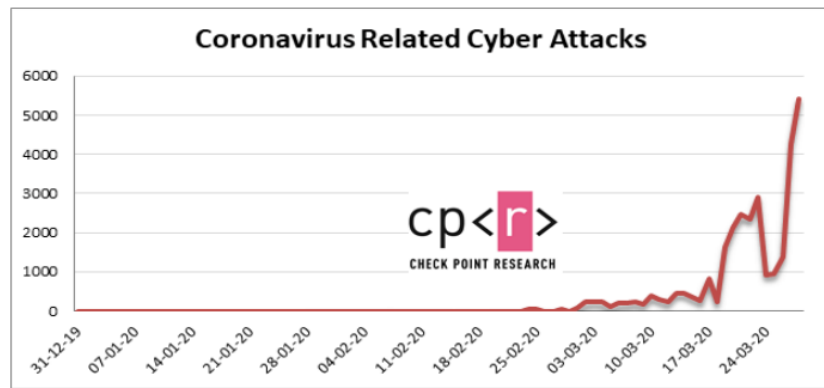


Figure 1: Healthcare industry cyberattack trends during coronavirus pandemic [9]

The main cybersecurity attack in healthcare sector is ransomware and the main cyber threat to healthcare providers are the employees caused by [1]:

- lack of training and awareness;
- no proper policies in place, particularly for those working off-site;
- insufficient secure physical access to confidential information;
- slow reporting of lost or stolen devices.

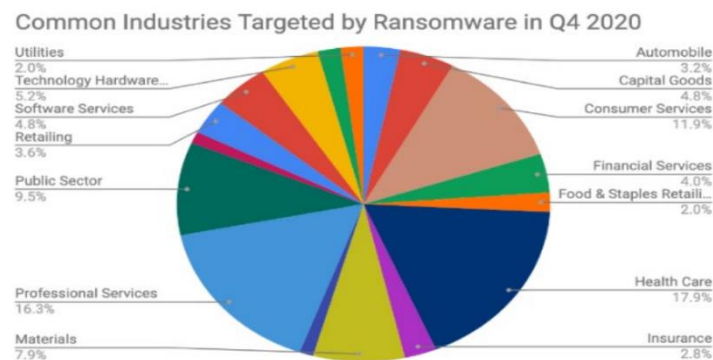


Figure 2: Industries targeted by ransomware - Q4 2020 [9]

In the field of eHealth there are many systems of technical operation and medical care that are considered critical. The criticality of these equipments are directly related with the information they hold, and the responses to business processes they support [10].

The Picture Archiving and Communication Systems (PACS) is one example of critical systems in the Healthcare domain. This type of systems allows the integration of clinical and reference data of a patient that is recorded on cross-platform in order to conserve this information for its analysis [10].

A problem that is starting to become a trend is medical fraud provided by the manipulation of fake tumor or high-profile disease. Researchers in Israel reported earlier this year that they had developed a computer virus capable of inserting tumors into CT and MRI scans – malware aimed at duping doctors into misdiagnosing high-profile patients [11].

By design, PACS cannot function in isolation. The overall PACS ecosystem consists of a range of technologies, including medical imaging equipment, patient registry systems and worklist management systems. PACS also depends on systems for storing and preserving medical image files, which may include cloud storage capabilities [12].

The primary function of PACS is to work with multiple medical imaging equipment, to interconnect with other clinical networks, and to enable a geographically and organizationally diverse team of healthcare professionals to review medical images in order to provide quality and timely treatment [12].

The threat environment is vast and allows for a large surface of attack. The PACS environment can contain vulnerabilities. Unauthorized individuals can exploit vulnerabilities and compromise or corrupt stored information. In addition, unauthorized individuals can use components known in the PACS ecosystem as pivotal points to compromise other components in the integrated health information system [12].

A Health Organization should adopt strategies, processes, techniques and tools to mitigate known cybersecurity and privacy risks [13]. A defense-in-depth approach, like network zoning, allows for granular regulation of network traffic flows and reduces exposure to the minimum required to support business functions. In other hand, assure mechanisms for access control, including multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that restrict remote vendor support for components of medical imaging.

Our approach aims to develop an artifact that provides alert and guidance features for rapid mitigation of cyberattacks. It is designed to operate in critical networks and medical context invasions, to detect unexpected behavior and prevention of security breaches in an area as sensitive as the clinical process and HIS (Health Information Systems).

In an agreed partnership with an University Hospital Center a solution that has an applicability aligned with the needs, associated technologies and respecting industry standards will be validated.

1.1 Overview

Our work aims to create technological composite that translates into a methodology and an innovative artifact for integration, monitoring, and security of critical medical infrastructures based on operational use cases.

This system is based on the references of critical systems, HIS, SIEM and IHS used in this field to enforce security controls, analyze network protocols, and strengthen their security.

The artifact will actively respond to the PACS elements of HIS's monitoring needs and trigger alerts on situations that are understood as abnormal.

It should be noted that the base open-source structure of the artifact can easily be adapt to the variants and needs of new equipment, new areas, as already happens with the detection mechanism commonly used in the industrial area.

1.2 Motivation

The world has faced many challenges over the decades of its civilization and, more recently, in its digital transformation.

As introduced earlier, the medical and healthcare sectors face two completely different types of pandemics [8].

On the one hand, we have the unpredictability of a viral enemy that is unseen and has stolen the lives of millions of people, and on the other hand an enemy also invisible for which the objective is to sabotage systems, steal data and in turn impact doubly the lives of professionals and patients [8].

Although the European Union Agency for Cybersecurity, European Network and Information Security Agency (ENISA) [13] recommends the implementation of controls and technologies that proactively seek to mitigate the exploitation of attacks, there is a determining factor, general to all economic areas, that is the lack and low priority of investment in cybersecurity [14], when compared to investment in business. However, both are essential to ensure business continuity and survival.

Since 2019 we have continuously learned that recommendations [8] should focus on the human factor, adapt the workplace to the changes concerning the place where the person is connected to the internet, promote security and educate employees in following the policies, procedures and practices that lead to the prevention, detection and mitigation of cyber-attack [8].

COVID-19 has put us all in a lively world that forces organizations to act differently. For this and all other reasons we proactively need essential services that act as a lever for global balance, such as the health and well-being of the community at large.

Critical systems are systems that support business processes that impact the business itself if they are disrupted. Since the 80's, we have followed the growth of the industry dependency from its industrial control systems.

To control and monitor industrial systems we have implemented sensor and monitoring systems that allow us to understand that everything is as expected, and the process results in the expected product or solution: ICS (Industrial Control Systems) [2].

In the healthcare field, we can consider that medical instruments or even field devices have the same importance in the development of the health business as treating the patient effectively and quickly [10].

One of the instruments that touches more parts of the process is the PACS system that works with a medical image aggregator and allows the availability in real time of tomographic exams, for example, for medical evaluation. The importance of its monitoring is increasing and a proactive response is emerging to this important need of the healthcare sector [8].

Intrusion Detection Systems can be an important tool in the sense of perceiving if the equipment that is necessary to save people is used correctly and is not tampered with or compromised, not only the well-being of the patient, but also the criticality over the medical data. Very valuable information that can establish an advantage for doing business, creating health insurance or even buying a house, must be protected with special care.

The state of the art on the ICS and IDS itself is very wide and very easy to suffer oscillations over time, as the principle is not recent and has been focused on refining methods for greater effectiveness in detecting anomalies in systems, as we can see in the following chapter. Still, the derivation for critical medical systems is still a challenge that we are committed to meeting for the enrichment of knowledge and development of more and better practices in the academic community.

Our work aims to position itself as a valid artifact with all the existing information input at the industrial level and implement it in the context of Health Information Systems (HIS). The main objective is to broaden the spectrum of action in proactive measures to include more and better methods to enrich institutions for a better positioning against attackers and a better definition of their security posture in a holistic way.

1.3 Objectives

Given the problem and the need for medical equipment monitoring, previously mentioned, the objective of this study is directly related to the construction of a conceptual model that translates into an artifact and that allows, on the one hand, to detect (from a cybersecurity point of view) an active monitoring of the critical system in clinical practice, and, on the other hand, to facilitate the detection, containment, investigation and resolution, in case of a security incident. It is intended to create an incident response methodology that will be mapped into an innovative artifact that:

is a security monitoring framework for critical operational clinical systems to enhance their monitoring and, in turn, response to cybersecurity incidents. Overall, to leverage the organization's cyberspace security posture.

Our study focuses on two main research questions:

1. Can the introduction of security incident response methodology direct towards a proactive positioning of security and enforcement of controls in the area of healthcare?
2. Can active monitoring of critical systems improve the application of more and better controls at the level and enhance the incident response process in Health Units?

1.4 Methodology

The research methodology we used in this work is the Design Science Research Methodology (DSRM). This approach is a collection of principles, practices, and procedures essential for the progress of our research.

DSRM is done in two steps: build and test. In comparison to behavior research, design-oriented research develops a conception and subsequently attempts to construct the structure according to the established model, considering limitations and restrictions (Österle et al., 2011) [15].

The methodology addresses research through the creation and evaluation of one or more artifacts designed to meet the business needs defined (Hevner et al., 2004) [11]. By also using ideas from different disciplines, such as social science, engineering, computer science, economics, and philosophy, Information Systems (IS) can benefit from DSRM to resolve issues at the intersection of IT and organizations (Hevner et al., 2004) [16]. The framework is presented in the Figure 3: DSRM Process Model (Peppers et al., 2008) [17].

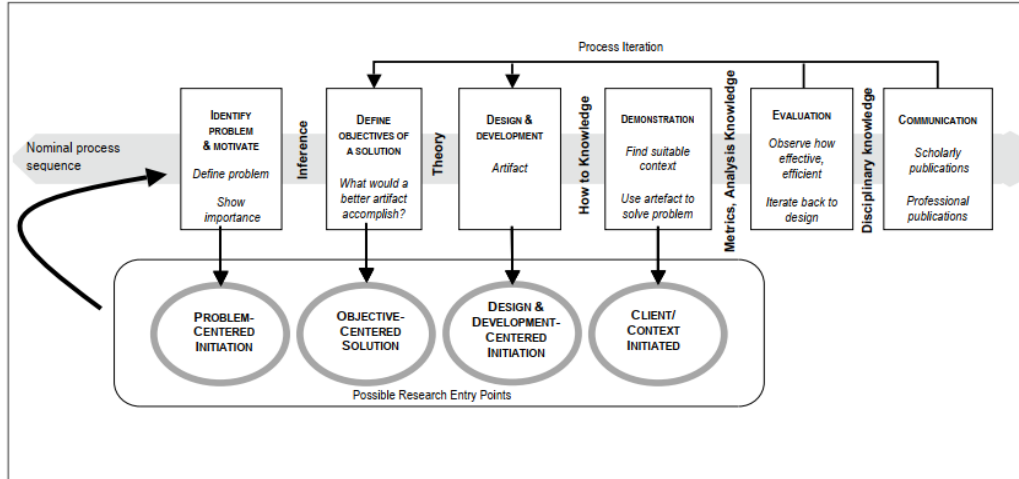


Figure 3: DSRM Process Model (Peffers et al., 2008) [17]

Our entry point into the research was problem identification. That said, we have an initial problem-centric approach to proceeding with the process. The steps are described below:

1. **Problem identification and motivation:** this step defines a challenge of study and justifies a solution's value. The definition of the problem will be used to create an artifact that can provide a solution effectively. Our research problem detects a research gap lack and makes a contribution for healthcare infrastructures to improve their security posture and monitor critical and essential instruments and medical assets.
2. **Definition of the objectives of a solution:** To infer from the problem description, related work, and knowledge of what is necessary and feasible, the aims of a solution. The objectives should be inferred rationally from the definition of the problem and can be quantitative, such as explaining how a new artifact is supposed to solve problems, or qualitative, such as terms that would be better than the existing ones for a desirable solution. In this case, the objective of our work is creating an approach that translate in a security monitoring framework for critical operating systems in order to enhance the response to security incidents and security posture in the cyberspace of the healthcare organization.
3. **Design and development:** the step to create one or more artifacts. We need to decide the desired functionality of the artifact and its design, based on related work chapter, to construct the artifact. It can broaden the knowledge base or, in new ways, apply existing knowledge.
4. **Demonstration:** justifies the decision-making process to solve the proposed problem. In this step should be involved activities like experimentation, simulation, case study approach, or others.

5. **Evaluation:** It consists of analyzing and evaluating how well a solution to the problem is assisted by the artifact. These approaches can include, among other techniques, interviews with professionals, surveys, simulations, and the scientific community's evaluation.
6. **Communication:** Corresponds to the presentation to relevant audiences of the entire study. With the public presentation of the theme in a workshop to the academic community and the presentation of the master's thesis.

A sequential order accompanies the creation and examination of the constructed artifacts and may undergo some changes throughout the process.

1.5 Dissertation Outline

The structure of this dissertation, which includes the Introduction (Chapter 1) with the objectives of the work and methodology, consists of five chapters that we describe below:

Chapter 2 situates the related work and bibliography of interest for reference of the current state of the art on the themes: Operation Technology, Industrial Control Systems, Intrusion Detection Systems, Protection of Health Systems and Incident Management.

Chapter 3 deals with the development of the artifact based on a methodology for integrating health systems and developing the framework that monitors the systems and allows for proactive response to security incidents. This part also includes the input for generating contextual use cases and an incident response process.

Chapter 4 frames, demonstrates and evaluates the context of applicability of the work developed. In the impossibility of applying the artifact in a real context, it was validated through a panel of experts with the adjustment of a demonstration scenario that depicts the process and technologies in operation. The panel was composed of experts in the field of cybersecurity and incident response.

Chapter 5 shows the results, lists the highlights that were possible to conclude with this work and projects future work and future applicability, as well as the projection of a paradigm shift in the field of cybersecurity.

Chapter 2

Related Work

The systematic literature review was carried out by crossing two methodologies in order to meet our needs. First, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology was adopted (Moher et al., 2009) [18], and then, to better define the topic of cybersecurity in healthcare field, the Snowball Sampling method [19] was used. The method consists of searching literature based on references to key documents in the area of other documents to be treated as a starting point.

Using Scopus¹ as our main research database and Google Scholar² as secondary sources for articles, we have conducted a systematic analysis, the last one needing a more stringent approach due to the range of quantity of the works it includes.

The queries involving the keywords 'protection' + 'industrial control systems' + 'health' had minimal results, after filtering studies that did not present what was intended at the level of the theme and the level of applicability of the research.

("protection" AND ("Industrial Control Systems" OR "industrial control systems") AND ("scada" OR "SCADA")) AND ("health" OR "HIS")

In the foreground was used the query directly related to the major theme and we obtained 45 studies.

That's why health was removed and the search was about 'protection' + 'intrusion detection systems' + 'industrial control systems' + 'scada'. From this research, limiting the results to the last 5 years, 2016 to 2020, written in Portuguese or English, in the field of engineering or computer science, we arrived at the result of 16 documents that were the eligibility basis for this review.

("protection" AND ("Industrial Control Systems" OR "industrial control systems") AND ("scada" OR "SCADA"))

¹ <https://www.scopus.com/>

² <https://scholar.google.com/>

We now begin to demonstrate the flow used to define literature eligibility for the course of the study.

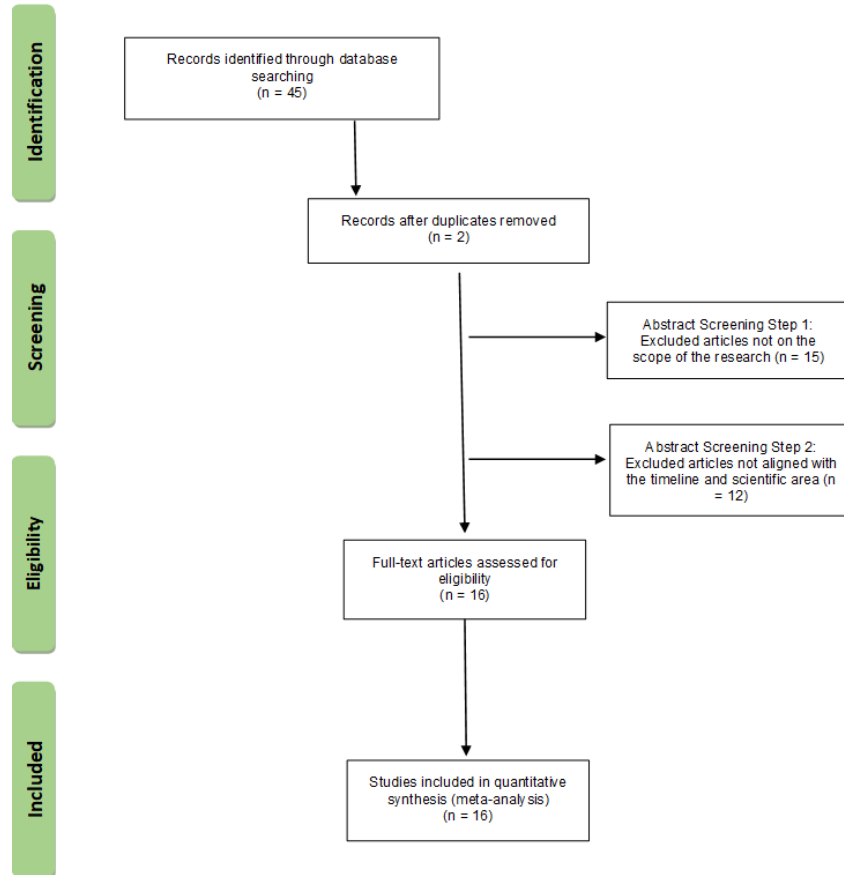


Figure 4: Prisma Flow Diagram [18]

The Figure 5: Applicability and inclusion criteria - List of papers shows the full text review listing of the reference documentation for this work. As mentioned above, a cross-referenciation method based on its highlighted references has been developed and the method for revision that we present.

Title	Year	Applicability analysis approach to this dissertation	Document Type	Source
A new perspective towards the development of robust data-driven intrusion detection for industrial control systems	2020	Intrusion Detection System	Review	Scopus
ARIES: A Novel Multivariate Intrusion Detection System for Smart Grid	2020	Intrusion Detection System; SCADA	Article	Scopus
Implementation and detection of modbus cyberattacks	2020	Intrusion Detection System; SCADA	Conference Paper	Scopus
Intrusion detection using long short-term memory model for industrial control system	2020	Intrusion Detection System	Article	Scopus
Cybersecurity for industrial control systems: A survey	2020	Industrial Control System; Intrusion Detection System	Review	Scopus
Capturing-the-Invisible (CTI): Behavior-Based Attacks Recognition in IoT-Oriented Industrial Control Systems	2020	Industrial Control System;	Article	Scopus
Detecting cyberattacks in industrial control systems using online learning algorithms	2019	Industrial Control System; Intrusion Detection System	Article	Scopus
Trends in existing and emerging cyber threat intelligence platforms	2019	Intrusion Detection System	Article	Scopus
Operational data based intrusion detection system for smart grid	2019	Intrusion Detection System; SCADA	Conference Paper	Scopus
Development of Smart Grid Testbed with Low-Cost Hardware and Software for Cybersecurity Research and Education	2018	Intrusion Detection System; SCADA	Article	Scopus
Filters based Approach with Temporal and Combinational Constraints for Cybersecurity of Industrial Control Systems	2018	Industrial Control System	Article	Scopus
Intrusion detection method for industrial control systems using singular spectrum analysis	2018	Industrial Control System; Intrusion Detection System	Conference Paper	Scopus
Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks	2017	Intrusion Detection System; SCADA	Article	Scopus
Multiattribute SCADA-specific intrusion detection system for power networks	2014	Intrusion Detection System; SCADA	Article	Scopus

Figure 5: Applicability and inclusion criteria - List of papers

All other references considered the use of the Snowball method in annual references document for the area of healthcare and the references of the elements eligible for consultation.

In the next chapters we will address the topics of industrial control systems, the particularity of the defense of ICS with Intrusion Detection Systems and, finally, we will address the challenges on critical medical equipment such as PACS systems.

2.1 Operational Technology

Most cybersecurity professionals take the information technology or IT nature of their employment for granted [20].

That example, while creating cyber defenses for a certain infrastructure, it is typically assumed that defenses are also required for software running on computers and networks [20].

The question of whether a system is digital or even computerized appears to have been the most pertinent to ask in the 80's. We all believe that everything is software running on CPUs.

The issue is that not everything is program that CPUs control. Cars incorporate mechanical parts that can get as hot as it were so hot, airplanes have wings that can twist as it were so distant, industrial facilities incorporate get together lines that can go as it were so quick, and power plants incorporate liquid channeling that can as it were handle so much. These tangible entities comprise of solids, fluids, and gases, instead of binary (1's and 0's) so their administration requires a different sort of component called an industrial control systems or ICS.

The support environment that enables industrial control is collectively referred to as operational technology or OT. As it is a part that supports the business itself, sometimes there are certain controls that are left to chance regarding cybersecurity.

OT security is particularly intense, since the physical results of compromise may be totally unsatisfactory, and because numerous of the security components that are moment nature on IT systems can in reality impair physical operations as severely as a cyberattack. This leads to both perplexes and headaches for cybersecurity engineers. Cybersecurity engineers have hence started the travel of attempting to decide how to apply the best elements of IT security, learned through down to earth encounter over the past three decades, to the OT management and observing of ICS.

In numerous cases, IT bits of knowledge are straight forwardly appropriate to OT/ICS security; but circumstances do rise where the nature of mechanical control framework presents novel malicious dangers that require inventive unused cyber arrangements [20].

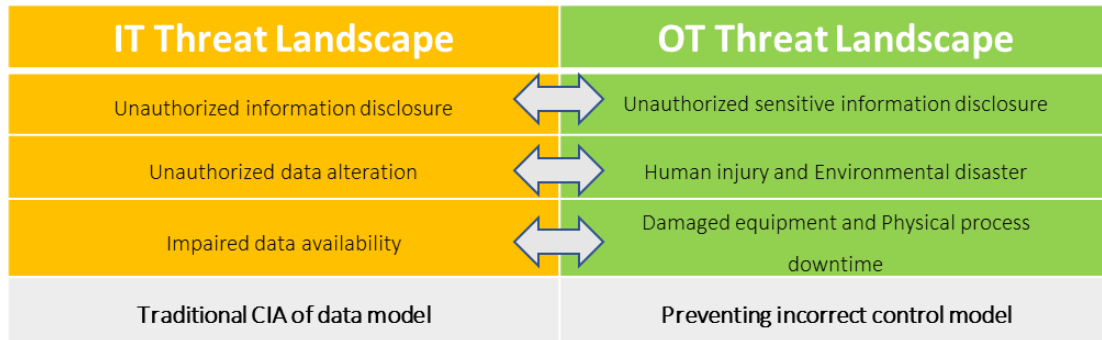


Figure 6: IT Vs OT: The Evolution of the Threat Landscape, inspired on [20]

2.2 Industrial Control Systems

An Industrial Control System (ICS) is composed of several automatic control components and real-time data acquisition components of critical infrastructures. The main aim of the ICS is to monitor and control industrial equipment to ensure the normal operation of all industrial process. The Supervisory Control and Data Acquisition System (SCADA), Distributed Control System (DCS), Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Human-Machine Interface (HMI) and several communication interface technologies are the main components of the ICS [2].

Usually, distributed control system networks are industrial control system networks in a single geographic area. In contrast, ICS/SCADA networks are usually dispersed across broad geographical areas and are used to monitor and automate industrial processes remotely [2], [21].

Pliatsios et al. (2020) [22] tell us a generic SCADA system is constituted of some components like an operator who is in charge of controlling the device, managing warnings and conducting the necessary control operations. The operator can be located on the business premises, or the device can be accessed remotely through the Internet. The Human Machine Interface (HMI) that promotes the interaction between the operator and the SCADA system. The HMI receives information from the Master Terminal Device and translates the control commands accordingly. Next component is the Corporate Network [5], this consists of components of computing, networking, and storage located within the company. It facilitates the system's operation by running analytics of data obtained from devices in the Field layer.

Already mentioned, Master Terminal Unit (MTU) is the head for collecting and transmitting data from remote terminals to the HMI, as well as sending control signals. It also provides the system with high-level control logic. The Remote Terminal Units (RTU) works as a data and commands exchange central with the MTU to send specific control signals to the field equipment. Finally, Field Devices are

used in a distributed manner throughout the company to verify, monitor and control the critical process. In the following Figure 7 we can see all this description in an integrated system.

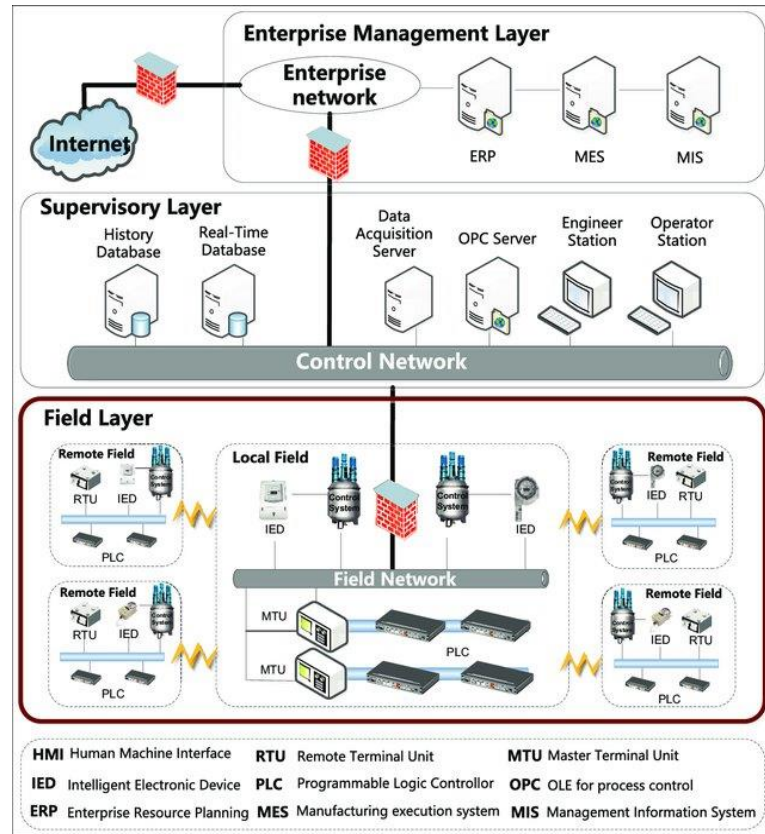


Figure 7: Architecture Explained of ICS [23]

Control messages exchanged between master and slave devices are standard communications on a SCADA network. A master device is one which can regulate another device's operation. An example of a master computer is a PC or a PLC. A slave device is typically a simple sensor or actuator that can send messages and perform actions at the behest of a master device to the command device [21].

There are numerous communication protocols for ICS/SCADA systems. According to the American Gas Association's standard, there are between 150 and 200 different protocols used in these systems device [21]. Most of these protocols were proprietary standards that individual businesses developed. The industry has moved into adopting common open standard protocols over the years. Many different technical associations are competing also with open protocols to gain greater recognition within the industry for their protocol standard.

With the introduction of 64-bit microprocessors in the 1990s, SCADA systems, along with developments in networking technology, have embraced open system architectures rather than a

supplier-controlled environment. SCADA systems have used open standard protocols that allow a wide area network to run [5].

Nicholson et al. [5] introduced that at the moment, SCADA systems can operate on several platforms and can be purchased "off the shelf" easily.

The next Figure 8: Industrial Control Systems - SCADA Protocols indicate us the available protocols and in use to critical systems.

Protocol	Network Infrastructure	Topologies	Data Rates	Maximum Distance
BITBUS	Fieldbus	Bus	62.5 Kbps, 375 Kbps, 1.5 Mbps	1200m
DC-BUS	2-wire cable	Line	115.2 Kbps up to 1.3 Mbps	100 km
Distributed Network Protocol 3	Ethernet	Line, Peer-to-Peer	100 Mbps, 1 Gbps	100m
EtherCAT	Ethernet	Ring, Line, Daisy-chain	100 Mbps	100m
Ethernet Powerlink	Ethernet	Tree, Line, Star, Peer-to-Peer	100 Mbps	100m
Foundation Fieldbus H1	Fieldbus	Point-to-point, Bus with Spur, Daisy-chain, Tree	31.25 Kbps	1900 m without repeater, 9500 m with up to 4 repeaters
Foundation HSE	Ethernet	Tree, Line, Star, Peer-to-Peer	100 Mbps	100m
HART	2-wire cable	Point-to-point, Multi-drop	1.2 Kbps	3 km
IEC 60870	Serial, Ethernet	Ring, Tree, Line, Star	N/A	N/A
IEC 61850	Ethernet	Ring, Tree, Line, Star	N/A	100m
Modbus	Serial, Ethernet	Line, Star, Ring, Mesh (MB+)	100 Mbps, 1 Gbps	N/A
PROFIBUS	Fieldbus	Point-to-point, Bus with spur, Daisy-chain, Tree	9.6 Kbps to 12 Mbps	100 to 1200m, 15km for optical channel
PROFINET	Ethernet	Ring, Tree, Line, Star	100 Mbps, 1 Gbps	100m
RAPIDnet	Ethernet	Line, Ring	100 Mbps	100m
SERCOS III	Ethernet	Line, Ring	100 Mbps, 1 Gbps	N/A
Unitronics PCOM	Serial, Ethernet	Ring, Line, Star	100 Mbps	100m
WorldFIP	Fieldbus	Bus	31.25 Kbps, 1 Mbps, 2.5 Mbps, 5 Mbps	1km

Figure 8: Industrial Control Systems - SCADA Protocols [21]

2.3 Cybersecurity Monitoring and Analysis

In computer engineering, information security allows and is responsible for defending assets such as software and hardware, as well as all resources that ensure the organization's proper operation.

This alignment is ensured through strict adherence to protocols, the adoption of appropriate security controls, and alignment with the organizations staff: the weak point of any organization.

Industrial components are composed by SCADA systems to help monitoring and controlling an industrial process.

The area of cybersecurity visualization focuses mainly on developing solutions and researching. Still, these focuses are on the technological aspects of the tools rather than considering the critical roles played by humans and that affect cyber operations. Visual analysis has benefited cybersecurity analysts by raising awareness to a more holistic approach and visually identifying problems and solutions [24].

Examples of current cybersecurity data visualization solutions are explained as follows:

- Network Analysis;
- Malware & Threat Analysis;
- Security Information and Event Management (SIEM) active monitoring.

Network Analysis maps the physical network to discover potential intrusions for security, forensics and anomalies [24].

Coudriau et al. [25] research's focused on monitoring data in the Darknet to spot dangerous activity based on traffic patterns, including generating alerts. At the end of this case study, the proposed approach analyzes malicious network packets in order to scan the activity and avoid an attack.

Malware and Threat Analysis tools can detect and delete malware and threatening communications harming enterprises in real-time, detecting cyber-attacks using maps and graphs, or evaluating threats with machine learning to find patterns for anomalous activity [26].

SIEM active monitoring are frequently used to improve system security and deal with cyber-attacks. Many practical SIEM systems use in-system agents on monitored system resources to collect state information used for incident detection and analysis [27].

2.4 Intrusion Detection Systems

The Intrusion Detection System [28], [29] is an active security technology that analyses the system's network layer data and detects unauthorized activities.

Four types of intrusion detection systems are commonly presented: wireless intrusion detection, host intrusion detection, network intrusion detection and mixed intrusion detection systems [30]. Host intrusion detection systems analyze hosts individually where systems are installed and is usually targeted at hosts that contain sensitive information that can be a desirable target. A network intrusion detection system captures and monitors network traffic and analyzes it against suspicious activity and patterns. A wireless intrusion detection system is characteristically equivalent to a network system, which is specific for detection in wireless systems such as purely wireless networks. Finally, a mixed system is defined as a system that combines at least two referred systems and has specific applicability [30]. Intrusion detection strategies occur in two groups, namely, misuse and detection of anomalies [31], [32].

There are at least two methods used in the systems described above: Signature based Intrusion Detection and Anomaly based Intrusion Detection. The first that is sometimes also characterized by Misuse based Intrusion Detection [31] looks for patterns in network data or traffic and compares them to signatures that recognize abnormal behavior. The application of signature-based mode for cybersecurity in systems requires prior knowledge of 'known cyber attacks' and/or 'abnormal behavior'. These signatures are not effective in detecting new attack trends, unknown attacks or zero-day attacks. In many other options, IDS Snort is a system that uses this method effectively [30].

In turn, Anomaly-based Intrusion Detection Systems, unlike systems that use the Signature-based method is based on statistical behavior analysis. This analysis is based on monitoring the normal operation of equipment or network and establishing a normal communication pattern on the network. When this pattern is exceeded and unexpected behavior occurs, a security anomaly is triggered in the system. A suspicious activity could be unknown with this process allowing the identification of "zero-day" or previously unknown threats [30].

In the field of Anomaly-based intrusion detection, there are three categories in the most used techniques: statistical-based, machine learning-based and knowledge-based, which includes data-mining approaches [7].

Over the years, several kind of research have been done comparing the two signature-based and anomaly-based approaches. In 2000, Axelsson [33] performed a survey about the current anomaly-based and signature-based methods. Garcia-Teodoro et al. [7] introduced the evaluation of ciphers in data, low detection rates, low throughput and high as challenges of the Anomaly-based techniques in the network. The design of a taxonomy of modern systems as a result from a review of available intrusion detection

system approaches was conducted by Liao, et al. (2013) [30]. Researches about intrusion detection methods in several areas were conducted in 2014, Butun et al. [34] presented a survey of intrusion detection in wireless networks. After, Zarpelão et al. [35] performed other surveys in the Internet of Things field. Intrusion Detection Systems new direction were introduced by Liao, et al. in [30] such as the applicability of these systems to monitor Industrial Control Systems (ICS). Ding, et al. (2018) [36] presented a survey of attack detection that identified the most common types of attacks such as Denial of Service (DDoS) or Deception Attacks, as well as methods for their detection in cyber-physical components.

As seen, Intrusion Detection Systems are divided into two types: signature-based and anomaly-based. Both solutions monitor network traffic and in one case, trigger a signature (rule) or by evaluating the deviation from a baseline considered normal. As the literature indicates, these systems are easily applicable to the security protection of critical industrial infrastructures.

2.5 Intrusion Detection in Critical Systems

For industrial control, Intrusion Detection Systems can be split into three types: content-based attack detection, network function-based detection and physical process-based detection [29], [37].

A 'state-based' intrusion detection system was proposed by Fovino et al. (2010) [38] that uses the concept of process constraints, but the approach relies on the existence of a mirrored image of the memory content of PLCs. Their method, which focuses on the Modbus and DNP3 protocols, uses a part a memory image part that periodically samples all the PLCs.

Hadžiosmanovic et al. (2011) [39] suggested monitoring solution that continuously protects the network to monitor messages that carry changes to process variables and detect them with MELISSA. Prediction models are used for each controlled process variable to measure expected values, which are then compared against observed values. The framework is like an IDS centered on anomalies because when large deviations from expected values are observed, alerts are triggered.

Erez et al. (2015) [40] suggested another mechanism for detecting anomalies in which the PLC registers are characterized as belonging to one of three classes: sensor, counter or constant. Registers containing physical process measurements have been classified as sensor registers, registers that store cyclic counter values classified as counter registers and registers whose values have not changed have been classified as constant registers.

Gao et al. [41] have proposed an intrusion detection method to detect command-and-response injection attacks and denial of service in SCADA systems. The solution keeps track of process variables

from the network. Regulated process variable values, operating under normal conditions, are used to describe the process actions. Differences in actions would imply that there may be an attack. Neural networks are equipped to learn what is "normal" and then used to identify irregular behaviors in the process. The approach was demonstrated by tracking the tank's fluid level in the SCADA network using the Modbus protocol.

The Figure 9 defines the representation of all Intrusion Detection System types to apply on Industrial Field.

Goldenberg et al. (2013) [42] introduced the IDS model for SCADA ModbusTCP networks. Their IDS system catches a large number of messages for periodic traffic.

Patterns that would imply normal activity are used to identify anomalies, and Cheung et al. [43] developed a protocol level model that characterizes Modbus requests and responses. Their approach's scope is also unaware of process level specifications, concentrating instead on network traffic inconsistencies.

Some improvements have been made available regarding SCADA rule-based intrusion detection for Snort IDS to help identify the patterns of Modbus and DNP3 control messages in a toolkit of predefined SCADA signatures as well as preprocessors. Still, using Quickdraw, it is impossible to generate rules on changes on the industrial control system monitored [44].

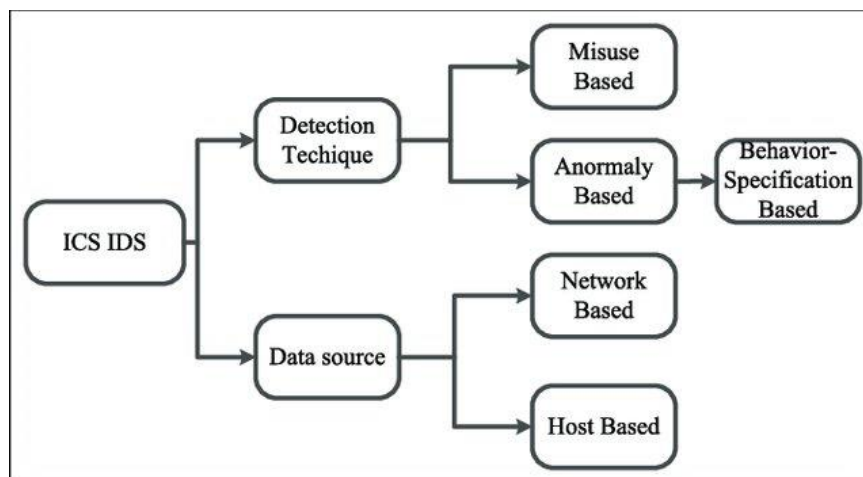


Figure 9: Characterization of Intrusion Detection System types [23]

2.6 Protection of Health Critical Systems

2.6.1 Healthcare Landscape

Even as we face a global health pandemic, cybercriminals continue to attack the healthcare business [45].

2020 will undoubtedly be remembered by COVID-19, but it will also be another year in which healthcare companies face heightened threats from these unscrupulous actors. Our adversaries mount tailored attacks to breach data and impair patient care as healthcare companies respond to the pandemic and that criminals are actively leveraging COVID-19 to their advantage [45].

The complete impact of these targeted attacks has yet to be determined, but reported breaches climbed by more than 8% in the first half of 2020 compared to the same period in 2019. According to the Office for Civil Rights (OCR) of the US Department of Health and Human Services (HHS), over 253 healthcare companies have already reported a breach this year, up from 234 in the same period last year [45].

Healthcare providers remain the most vulnerable section of the industry, accounting for over 75% of all reported breaches. The number of reported breaches among business associates increased by 46% year over year, the highest increase of any healthcare segment. Over 5.6 million people's health records have been compromised as a result of successful cyberattacks so far in 2020.

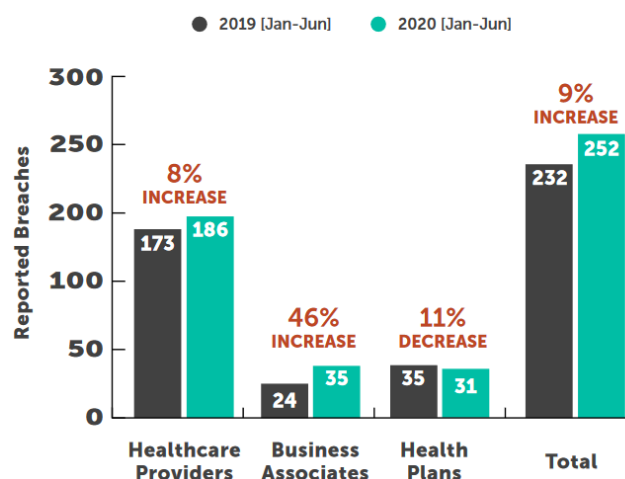


Figure 10: Breach Trends - Healthcare Industry [45]

2.6.2 Protecting Confidentiality of Patient Process

In the last two years, 89 percent of healthcare organizations have had patient data lost or stolen [1].

On the dark web market, patient health records can fetch as much as \$363, which is more than any other piece of information. The criminal community values patient data in particular [1].

EHRs (Electronic Health Records) store a variety of information about each patient, including their name, social security number, financial information, current and prior residences, medical history, and names of relatives.

Unlike credit card fraud, this type of identity theft can go unnoticed for months or even years, with no way of knowing how or when it happened. Aside from that, confidential medical histories have the potential to be utilized for extortion or smear campaigns, particularly in the case of celebrities and political leaders. The information can potentially be used by criminals to gain from bogus insurance claims.

When building software for medical equipment, manufacturers are not always security mindful. One gadget, for example, had its network password hard coded into the program, making it vulnerable to hackers. Many people utilize an insecure wireless connection, and some of them may communicate passwords and other sensitive information in plain text.

Furthermore, employees are not always aware that the device poses a security risk. Taping a password to a medical device, for example, can put a company's data at risk. Medical equipment's are, in reality, a potential entry point for a cyber-attack into the system.

Security incidents and cyberattacks can be avoided by healthcare providers by [45]:

- Implementing Security Awareness Training;
- Preventing Personal Device Use;
- Performing Comprehensive Backups;
- Creating an efficient Incident Response Policy.

2.6.3 Picture Archive and Communication Systems (PACS)

The use of technology allows modernizing the area of medicine and healthcare. In 1970, the appearance of Hospital Information Systems (HIS) was the turning point, with the inclusion of subsequent Computed Tomography (CT) magnetic resonance imaging. Then, with the Systems of Picture Archive and Communication Systems (PACS) and the sharing between hospitals of clinical information. With the growth of communication infrastructure, the challenges increased dramatically, and a term that became indispensable for hospitals was cybersecurity [10].

The most obvious degree of cyber protection is physical: technological prevention measures such as passwords, virus scanners or fine-grained user rights are of little use if an intruder can easily walk into a server room and steal computers or storage media [10].

A study from ENISA points that physical and environmental protection is the second highest safety requirement in eHealth after an incident has been identified. The most data breaches of protected health data in the USA are electronic media such as laptops or portable devices and many from theft [46].

A US Department of Health and Human Services guideline [46] recommends restricting areas and making them secure in order to mitigate the disappearance of storage devices and related data.

Even with all the controls about access to health equipment's it is still possible that a determined individual can access the information on it. The use of video recording through surveillance cameras can be understood with a possible security measure in these cases.

The PACS systems is one of many critical systems on the eHealth field. To protect this type of system, it is necessary to apply various mitigation measures in order to ensure greater security compliance.

Kruse et al. [47] conducted an analysis of security techniques for electronic health records and their conclusion shows that firewalls is one of the technological actives that are most discussed to use in this field and results in successful securing of the data on the network.

European National Information Security Agency [10] recommends out that is the most importance to separate the critical parts of the network from non-critical parts. It is highly recommended to separate medical devices to the largest possible extent from office components that are typically more susceptible to a wide range of attacks.

In addition, devices with known bugs that cannot be removed easily can either be used in a different section of the network or not connected to the network at all. In other hand, Vanickis et al. [48] describe

the approach of implementing the zero trust networks. Ultimately, the El Hajal et al. [49] describe the use of “data diodes” as a device that enforces a strictly unidirectional communication between two networks, from the highest level of security network to lowest level network in PACS network but notes this equipment cannot be used with DICOM network protocol, commonly used because it relies on bidirectional communication. Sittig et al. [50] recommend that in the device level, the Medical Organizations should disable USB ports because it is a one manner to deliver malicious code in the Medical infrastructures on-sight.

Networks monitoring and intrusion detection is highly recommended by Sittig et al. [50] where the organizations need to develop a user and activity monitoring of their networks and communications between devices that conducts proactive activities for surveillance of the systems to identify suspicious acts such as an increase of network traffic, communication not expected between devices, reception of fraudulent email messages. The purpose of monitoring approaches is to detect suspicious activities and identify and security concerns.

ENISA [10] recommends the implementation and use of monitoring and intrusion detection systems. With active monitoring on the network, we can observe abnormal system behaviors [31]. Maimó et al. [51] describes a machine-learning-based method [7] which can typify more easily a ransomware strikes that increase the reaction on the response of incidents and limit the damage.

The implementation of audit logs for imaging equipment and computer imaging systems is recommended as a standardized message format and communication protocol for audits related to PACS and medical imaging is described in the Integrating the Healthcare Enterprise (IHE) “Audit Trail and Node Authentication” (ATNA) integration profile, which is part of the IHE IT-Infrastructure Technical Framework, and in the related DICOM Audit Trail Message Format Profile [13].

Several studies have highlighted the importance of increasing the understanding and training of users of cybersecurity-related systems [10].

The recent NIST publication [12] recommends a reference architecture for a secured PACS using commercially accessible, standard-based tools and technologies and a comprehensive risk management approach. In general, with the inclusion of the various suggested measures and effective monitoring through an intrusion detection system, it will make the attack difficult even if a control fails and this would contribute to the possible non-breach of a PACS network.

2.7 Incident Management

The term incident management describes all activities performed when managing information security incidents, with activities covering the time before, during, and after an incident occurs. The main goal of an incident management strategy for many organizations is to prevent or contain the impact of information security incidents such that the direct and indirect injuries to their operations generated by the incident are minimized.

The following is how ISO/IEC 27000 defines an information security event and incident [52]:

- **Information security event:** a previously unknown scenario that can be security significant, or an identified occurrence of a system, service, or network state suggesting a possible breach of information security policy or control failure.
- **Information security incident:** a single or a series of unwanted or unexpected information security events that have a high likelihood of jeopardizing business operations and endangering information security.

2.7.1 ISO /IEC 27035 - Incident Response Standard

ISO/IEC 27035 [52] provides a method for dealing with information security incidents. The standard is divided into two sections. The first, ISO/IEC 27035-1, describes the five steps of information security management, as well as basic ideas and how to improve incident management. The second, ISO/IEC 27035-2, addresses two of the ISO/IEC 27035-1 phases, namely plan and prepare and lessons learned. It explains how to plan for and prepare for the incident response phases of Incident Management.

In this master dissertation, we will chart the timeline before, during, and after an incident using the phases as a basis [53].

- **Planning**

In the event of a cyberattack, incident response teams must function flawlessly, which requires planning. A corporate security policy often comprises guidelines for the reasonable use of company data, the repercussions of security infractions, and definitions of security incidents. As a result, businesses must create a step-by-step procedure for how the incident response team should handle incidents, including internal and external communications and incident recording.

- **Identification**

Identification is the detection of dangerous activity. This detection can be based on security and monitoring tools, publicly available threat information, or insider intelligence. The identification method includes gathering and analyzing as much data as possible about the hazardous activity. Incident response teams must differentiate between harmless user failures and harmful acts. Organizations cannot tolerate any faults in this identification process because any occurrence may threaten the organization's security.

- **Containment**

Short and lengthy containment are the two types of containment. Long-term containment restores all systems to operational status while removing the accounts and backdoors that caused the intrusion. By implementing an immediate response, short-term containment prevents the threat from spreading and causing further damage. In addition, short-term containment backs up all affected systems for further inspection.

- **Incident Removal - Eradication**

The incident removal approach includes identifying the point of breach, analyzing the scope of the attack, and eliminating any leftover back-door access. During this step, incident response personnel remove all traces of an attack. In addition, they determine the root cause of the incident and eventually comprehend how it was carried out in order to prevent similar attacks in the future.

- **Recovery**

Recovery refers to the testing of remedies from the confinement phase and the transition to regular operations. Hacked accounts are given new, more secure passwords or are replaced with other methods of access during this step. In addition, all vulnerabilities have been resolved, functionality has been tested, and normal business operations have been restored.

- **Documentation & Lessons Learned**

Mistakes are made during any event response. Learning from these mistakes and determining what went wrong is an important step in strengthening your ongoing disaster recovery plans. It comprises assembling your entire team and providing feedback on what worked and what didn't, as well as suggestions for how to improve the process.

A well-defined incident response plan should include specific details about each stage of an attack.

Preparation, identification, containment, removal, recovery, and learning from mistakes are the six important steps of incident response. This could be the deciding factor between a secured and a vulnerable infrastructure.

Chapter 3

HSMS – Design & Development

3.1 Design – Healthcare Systems Integration Security Methodology

Taking into account the defined goals, the research work was based on the development of a Health Security Monitor System (HSMS). This digital artifact is aligned with the design of a methodology for integrating medical systems in a hospital context to increase the spectrum of analysis and to provide to the healthcare institutions with active security monitoring capabilities.

Still, active monitoring should be complemented with information security investigations. Active monitoring is a process that makes use of the intelligence of monitoring systems and their interdependence of systems to be analyzed, as well as the more elementary and manual analyses, such as forensic investigation.

With this in mind, a general methodology has been formulated that is based on the ability to integrate medical practice systems into a detection system (SIEM), derive context use cases for analysis, trigger anomalous behavior detection, and ultimately cybersecurity incident resolution with integration into an incident response platform. This methodology is based on security monitoring aligned with an incident resolution process.

Incident response is the key to success in correctly positioning for managing security incidents and correctly fitting the entire life cycle of a cyber-attack into a healthcare infrastructure.

This approach focuses on increasing the capacity and security robustness of critical systems.

The security methodology is adjustable and customizable to the integration of more or different systems, based on 7 steps:

- definition of the systems to be integrated;
- integration of the systems in the monitoring platform (SIEM);
- definition of use cases and rule tuning;
- creation of information security incidents;
- definition of the incident resolution procedure;
- incident resolution;
- follow-up.

In the Figure 11: All-in-one Healthcare Security Incident Response Methodology, we can observe the methodology in the seven planned iterations.

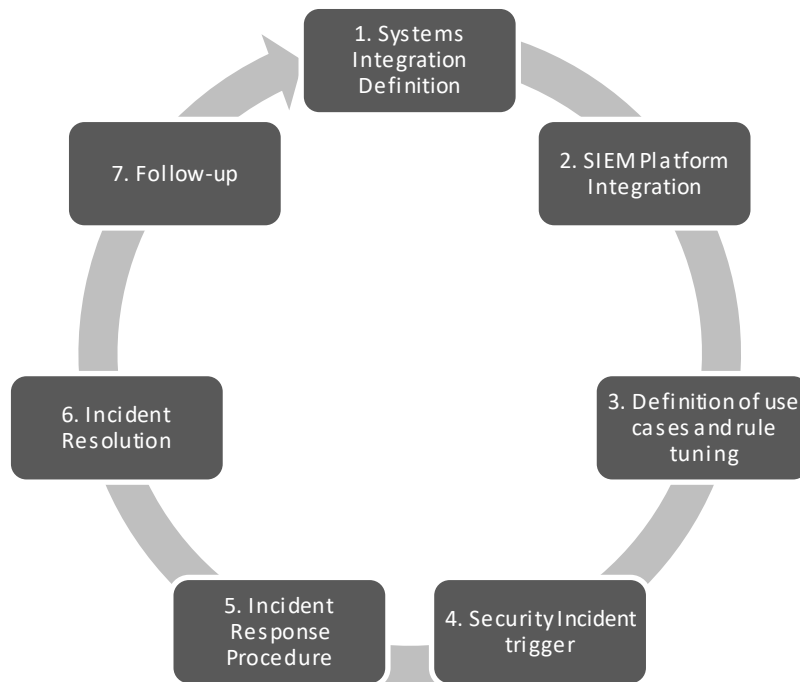


Figure 11: All-in-one Healthcare Security Incident Response Methodology

This methodology was based on the information provided in the literature review and professional experience. It is intended in a scalable manner with an easy-to-implement approach to create quick-wins for organizations that result in the implementation of cybersecurity controls.

It all starts with the need to define the systems to be integrated (critical healthcare business components, databases, active components, among others). Next Figure 12 shows a process that aims to manage the integration of data sources based on the difficulty and maturity of healthcare institutions.

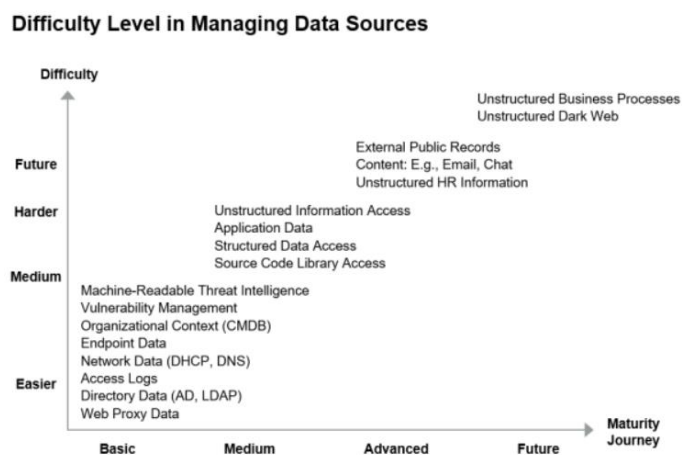


Figure 12: Difficulty vs maturity Data Sources Definition [54]

The definition is done with the assessment survey that is intended to map the criticality of the systems, their data owner, security owner and business owner. We can verify in the Figure 13 this approach.

The data owner, as the name implies, is the person responsible for the platform's information, the security owner is the person who is responsible for the platform's security and, finally, the business owner is responsible for the system within the organization.

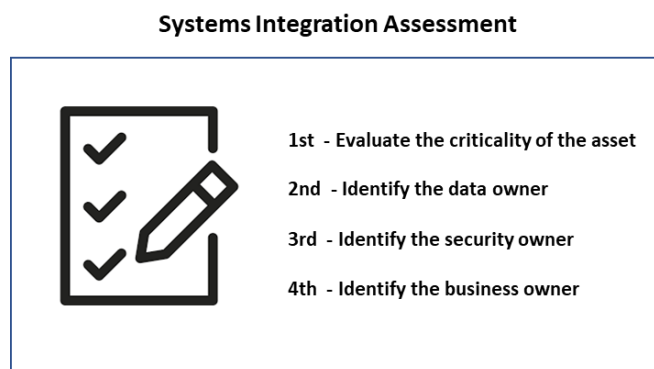


Figure 13: System integration assessment

The second step is to identify the requirements for integrating the systems into the correlation system, analysis and identification of events that may give rise to security incidents. In this step it is of considerable importance to identify the log source, the integration format and the need for manual adaptation.

The third step, integrating the systems, concerns the definition of practical cases (use cases) that match actions we want to see detected. Each healthcare facility will have its own and specific needs. Given the limitations of the protocols used in these systems, the approach to follow will be to create context and situational security. We may have situations where managers like to observe less far-fetched situations and prefer everyday cases, such as access to systems, password policy violations, and after-hours access.

Others, on the other hand, prefer to listen to the systems to understand the usage patterns or interference in their proper functioning, such as the case of ransomware or malware. This point derives directly from a procedure for defining use cases that is based on three pillars: insight that deals with part of the systems functioning, powered by data, and fueled by analytics.

The security incident triggers are aligned with the defined rules that derive from the previously defined use cases. Whenever a given event has a pattern that meets a validation threshold, an incident is created in the incident response platform for rapid resolution.

The actual incident response is based on a pre-cooked recipe dynamic that can only be deviated from that course based on intuition and experience. This procedure results in several steps that can be dynamically mapped in the platform in order to enhance the resolution and management of the cybersecurity incident in the

most pressing way. Incident handling is based on three main analysis tasks (identification, containment, and eradication & recovery), the derivation of the containment concept when further investigation is required (investigation), and finally the continuation of process tasks (documentation and lessons learned).

The investigation itself is a robust process that aims to identify additional information about a given security risk. They can range from memory analysis, data collection, and reactive network analysis.

With the definition of the methodology, the main intention of this work is that it be mapped into a technological context with the development of an innovative artifact to serve the purpose of healthcare monitoring systems (HSMS). This response anticipates the need for validation of the various steps to be taken until the resolution closure of a cyber-attack or incident based on an unanticipated situation. In the following Figure 14, we can observe the mapping between the equipment integration methodology and the instrumentation of the process itself through technology. This artifact will be described in the next section.

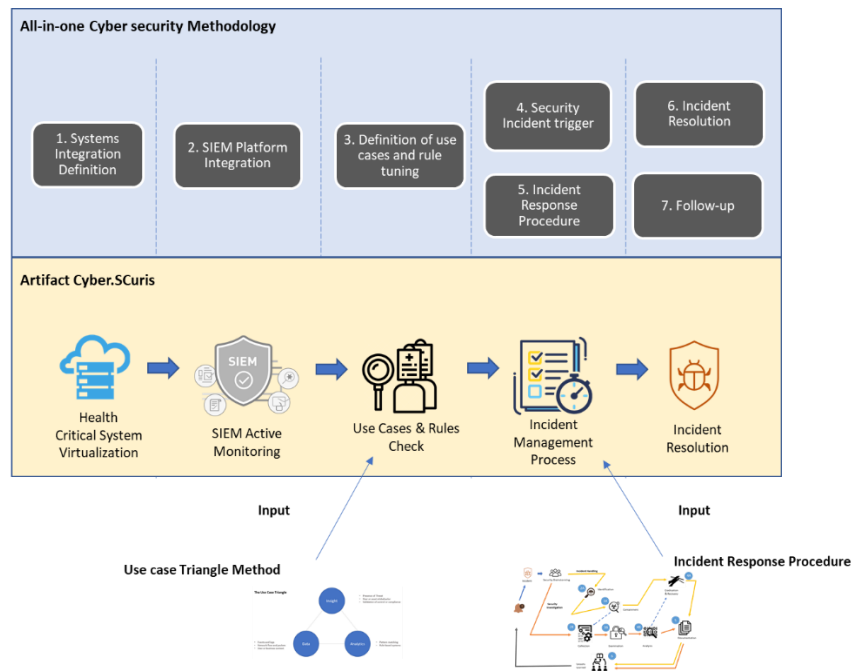


Figure 14: HSMS: Process and Technological mapping

3.2 Development – Healthcare Security Monitor System

In this subchapter we address the actual implementation of the artifact of this dissertation.

As previously represented, this artifact presents itself as the technological response to the methodology presented above with the need to simulate two virtual components that emulate the medical components of the medical image storage and the communication between them.

At this point it will be necessary to integrate their communication and monitor the network communication between both systems. This simulation validates the analysis of the systems that shows us in detail the particularities of the DICOM protocol used in the transactions between the server and the viewer created for this purpose.

Each component will be represented in the following chapters in order to give a clear understanding of how the structure works and its importance in the process, as can be found in Figure 15. The entire approach culminates in an incident response process that has a procedure outlined for operation and lifecycle management.

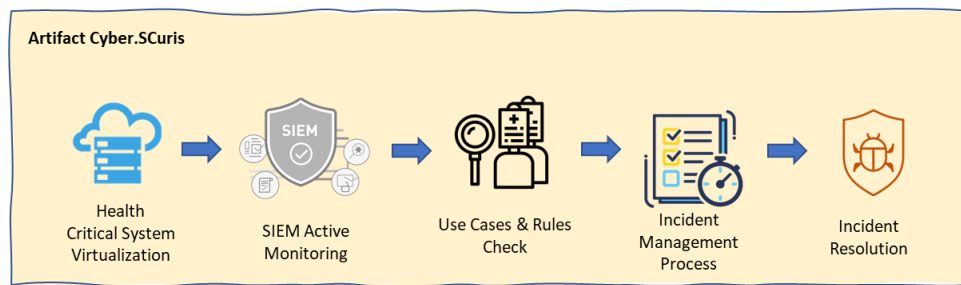


Figure 15: Artifact Cyber.SCuris – Development

For this specific use, we will monitor the behavior of a virtualized PACS infrastructure for integrated medical imaging communication, which will serve as a model of a real medical system.

Due to the constraints imposed by the COVID-19 pandemic, the cooperation agreed upon for in-person development, context, and real-world data did not materialize, thus we resorted to academic research to validate the prototype.

We will explain how to configure and create a medical imaging client-server network using a combination of open-source tools in this artifact. The emphasis in the development of this work is due to the continual attacks of hackers, who have successfully penetrated countless internal health imaging systems - a key instrument for the running of a hospital or healthcare infrastructure [7].

These forms of medical industrial component networks revolve on numerous systems and components – modalities – that serve to load, modify, save, and transport specific medical images between various equipment

and medical teams. Digital Imaging and Communications in Medicine (DICOM) is the most widely used imaging standard in the world [7].

Many Healthcare Information Technologies (HIT) system administrators must integrate the way the protocol is used in their networks various components so that they "talk correctly" to each other. Less discussed are two common standards, HL7 and FHIR, which when coupled supplement the whole patient information.

Finally, the system will be integrated with a SIEM platform for resolution of a specific use case and associated incident resolution.

One of the main platforms used in building our artifact with active monitoring framework was the Splunk Enterprise ³. The Splunk stack is a technology infrastructure that is used for searching, monitoring, analyzing and visualizing the machine-to-machine data on a real-time basis.

Most SIEM systems are unable to keep up with the sophistication and rate of modern cyber threats. This is a data-driven security system that goes beyond SIEM to handle advanced threat detection, security monitoring, incident management, and forensics in real time. This analytics-driven approach can improve your visibility across many platforms while also providing a solid security system through cross-collaboration. The tool at its genesis allows the storage of information with a strong indexing and search component for text components. With the composition of the tool with log collection, aggregation and normalization components and dynamic visualization component it was possible to combine a derivation for a free to use SIEM. Security teams use this platform for SIEM to detect threats through event analysis of network technologies, host with dedicated use cases.

³ <https://www.splunk.com/>

3.3 Cyber.SCuris

The developed artifact (HSMS) is henceforth called Cyber.SCuris which joins the cybersecurity approach in the English language plus the healthcare word derived from the Latin ‘curis’.

The global system works as a multiple integration of various open-source solutions and custom development. We highlight the integration of PACS systems (data source), integration with SIEM (Splunk) and HIS (TheHive). In addition to these points, custom development was done for the creation of alerts and incidents automatically and communication between operators and optimization of the incident management process with the following features:

- **Auto reception of alerts**
 - After defined on the SIEM platform the use case, all the cases that matches with settled rules send this Information to IR Platform automatically
- **Assignee to operators**
 - User friendly environment to assign the new cases to operators
- **Case Communication to chatbot**
 - Quick awareness of new case with Integration with collaborative chat platforms
- **Emailing from the case to the stakeholders**
 - Include and answer for more details with all stakeholders only using the platform
- **Following the process of Incident response stages and quick access to the Standard Operating Procedures (SoPs)**

3.3.1 Health Critical System Simulation

To depict this system, we shall employ two systems to simulate communication between them.

We will use anonymized test files from [dicomlibrary.com](https://www.dicomlibrary.com/)⁴ because we were unable to gather data using the genuine equipment (capture equipment).

- Orthanc Server
- ONIS Viewer 2.5 – free edition

Orthanc Server is an open-source platform designed for medical practitioners and researchers that provides a DICOM compliant server and client in a single package.

⁴ <https://www.dicomlibrary.com/>

It also has plug-ins and REST APIs, as well as the ability to secure the server using username/pass word authentication and TLS. The following Figure 16 demonstrates their presentation.

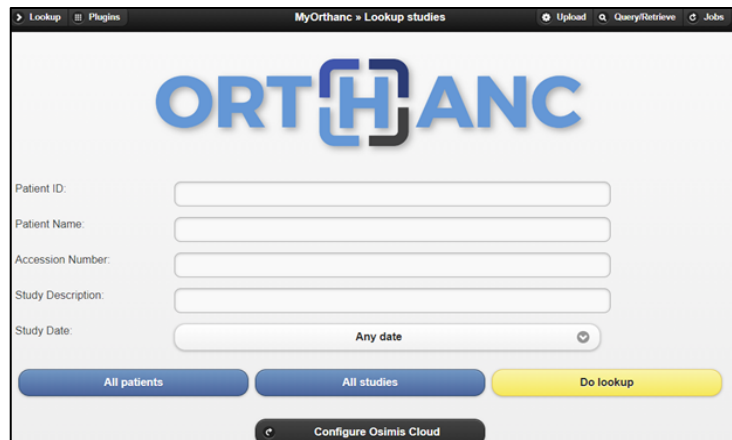


Figure 16: Initial Page Orthanc Server

In this case, we use ONIS to simulate an image provider completely apart from our primitive PACS server that is completely interoperable with Orthanc. A successful installation of this server will give rise to a presentation like what we can find below (Figure 17).

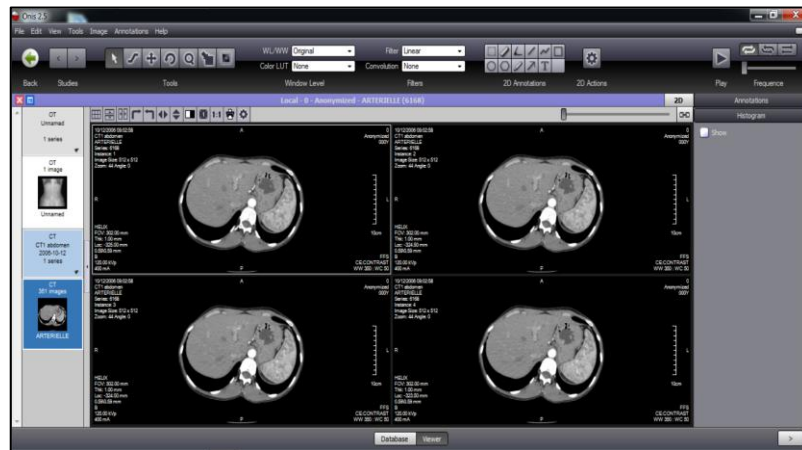


Figure 17: Work Environment - Onis DICOM Viewer

Communication between systems is achieved through the Orthanc Server which acts as the core part of the system. As previously mentioned, we do not have the possibility of acquiring images in real time and hence the archiver and the server feed themselves from an anonymized dataset of images that serves as a reference for transfers and communication.

The operation in context layer has the entire ecosystem of image capture machines (Rx, CTM, MRI, etc.), which are then captured, processed and archived in the equipment of your communication extension. Then, between what is the need for analysis in a delocalized way, medical teams or medical staff access the ability to view and medical diagnosis in a controlled access in a browser, for example.

This access is taken into account for exclusive access to healthcare professionals and in line with the clinical file of the patient under analysis. Each server has a central database that allows data to be stored in real time and allows them to be systematically saved in backup processes.

The two servers (Orthanc and Onis Viewer was deployed in the same address range) act and communicate using the DICOM standard, but given some particularities, Onis (Pacs Archiver) on port 104 and Orthanc (Server) on standard port 4242.

This framework allows for a realistic representation of the work order of a medical image acquisition procedure to be monitored, to ensure the desired improvement and control of cybersecurity.

These components have a critical position as a critical security system, since once compromised, it undermines the availability, confidentiality and integrity of medical data that could be stolen or disclosed in an unauthorized manner.

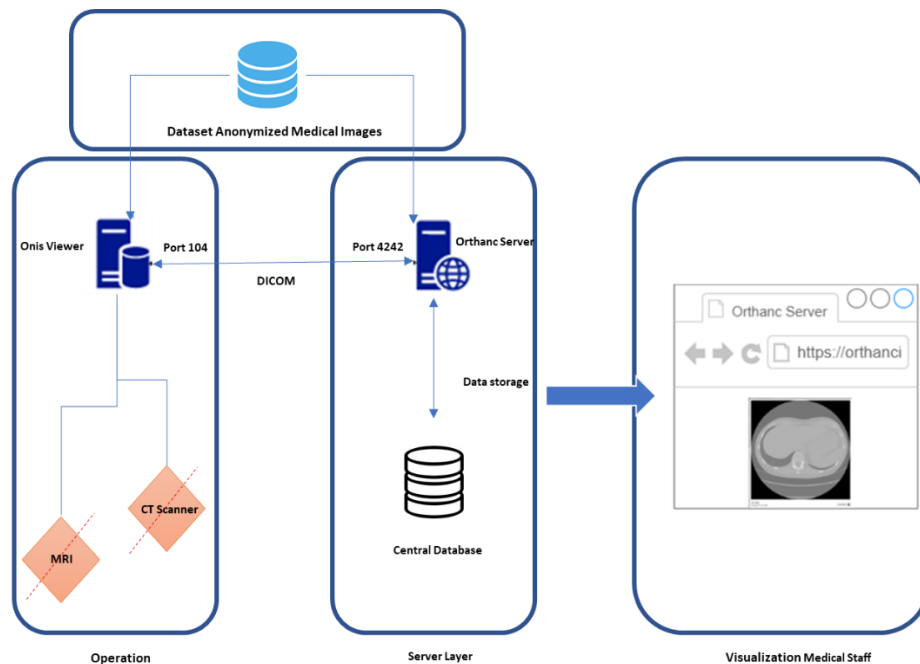


Figure 18: Logic Scheme - Communication

3.3.2 SIEM Active Monitoring

A critical system is one that must be highly dependable and maintain that reliability as it evolves without incurring prohibitively high expenses.

In this example, we will concentrate on the security crucial field, where systems cope with the loss of sensitive data due to theft or unintentional loss.

The system to monitor must send information from its core equipment to the remote communication points, which are based on monitoring through probes on the network or directly on the equipment present on the network. There are two types of network sensors: active and passive [55].

The former act actively on the network and perform queries to obtain information about the network assets. In this case we are only interested in capturing and collecting network traffic passing through a network or asset to be monitored. These types of sensors end up only collecting data that they are able to identify and collect. All out of scope networks end up having no representation in this capture and the information does not reach SIEM.

Still about the sensors we have the Network Event Sensors that are designed to detect and report relevant events that could originate an incident to a central repository (SIEM) in a timely manner. These sensors provide situational awareness of unauthorized events occurring on the network. These sensors are capable of alerting to predefined security aspects and act as assurance for compliance of network devices. The network components are configured through an audit log forwarding policy through a specific protocol (syslog, WMI, SNMP, among others). Among some of the features of a SIEM is aggregation of logs from multiple sensors to provide correlation capability among the various network devices.

Finally, we have the Endpoint-based Agents that work as software installed directly on computers (workstations or servers) and work as aggregators and collectors of information inventory related to unexpected behavior of the components and software contained in these machines and sending the events centrally to the SIEM.

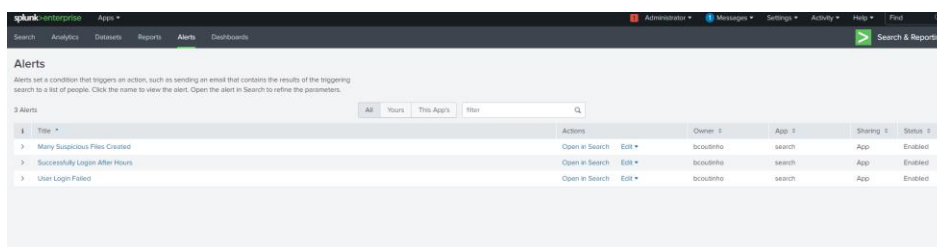


Figure 19: Splunk Enterprise: Alerts Panel

SIEM Infrastructure

At the heart of any SIEM structure is log information. Whether from servers, firewalls, databases or switches, data logs provide analysts with the raw framework to gain insight at key moments, frame them into intended use cases and put them to work in a productive environment.

Sometime recently this procedure can be turned into a resource, be that as it may, a few significant steps got to be taken. The information ought to be collected, processed, normalized, enhanced and stored. These steps, ordinarily assembled together beneath the term “log management”, are a must-have component in any SIEM framework.

For this study will be used a stack composed by a nuclear element: Splunk Enterprise.

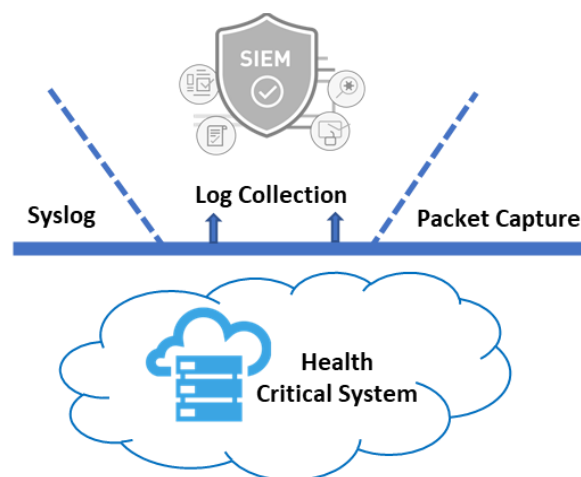


Figure 20: Communication Integration SIEM and Health Platform , self-made

3.3.3 Use Cases & Rules Check

Healthcare records have migrated from hard copy to primarily digital over the last decade. These digital pictures are easy to distribute, which speeds up the diagnostic process. Of course, the fact that healthcare pictures may now be uploaded, shared, and kept digitally on personal mobile devices such as smartphones and tablets make them a target for cybercriminals.

PACS also communicates with a variety of other systems, including electronic health records, regulatory registries, hospital information systems, and even government, academic, and commercial archives. This opens several security gaps for attackers to exploit and steal this data.

In order to mitigate possible borderline cases of information security, we will describe some use cases that will serve as a guide for the detection of unexpected behaviors that will serve as a guide for our detection in the context of responses to security incidents.

The system log information is passed to the SIEM through the Universal Forwarder that allows sending information in a directed way to a Splunk instance.

Use Cases by rules creation

To create use cases, we resorted to the definition of event detection rules in the integrated systems. Splunk allows the definition of rules via Index Patterns, Custom Queries and Query Language (QL) for compound scenarios and threshold queries.

Index patterns: WinEventLog-*

WinEventLog ships Windows event logs to Splunk Enterprise.

Custom Configuration:

Example:

```
[WinEventLog://Security]
renderXml = true
disabled = false
evt_resolve_ad_obj = true
blacklist1 = EventCode="4662" Message="Object Type:\s+(?!groupPolicyContainer)"
blacklist2 = EventCode="566" Message="Object Type:\s+(?!groupPolicyContainer)"
blacklist3 = EventCode="4688" Message="New Process Name: (?i)(?:[C-F]:\Program
Files\Splunk(?:UniversalForwarder)?\bin(?:btool\splunkd\splunk\splunk-
(?:MonitorNoHandle|admon|netmon|perfmon|powershell|regmon|winevtlog|winhostinfo|winprintmon|wmi|
OrthancService)).exe)"
```

Use cases to check

The following use cases form a set of requirements that are presented as recommendations to be carried out for monitoring in the context of protecting medical imaging platforms.

#1 Many Suspicious Files Created
#2 Successfully Logon after-hours
#3 User Login Failed

Table 1: Use Cases Definition

Based on the ransomware issue on the healthcare, the first use case is based on the creation of suspicious communication and files in specific directories that indicate the normal behavior of the attack. The second is based on successful access to critical equipment outside of normal operating hours. Finally, we will validate in the third the erratic system access during normal operating hours.

Use Case Definition

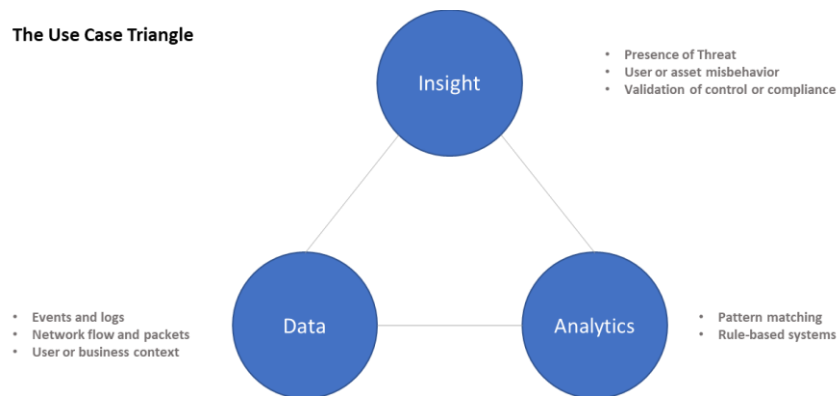


Figure 21: Use Case Triangle Method, self-made inspired on Gartner [54]

The creation of use cases is based on the definition of ideal scenarios for integrated detection of security flaws. Use cases are compositions of scenarios that may have already happened, are mapped or are intended to be triggered in an incident response process using active monitoring tools.

As you can see in the previous image, the use-case can be divided into three equal parts. The Insight layer that intends to meet a need, the data layer that concerns the data sources that feed it and, finally, the analytical capacity that is based on the trigger of a certain rule or pattern to validate and confirm the use-case set.

This triad gives the capability to effectively describe and industrialize an information security use-case.

3.3.4 Incident Management Process and Incident Resolution

The methods and actions used to respond to and resolve issues are known as incident management processes. Who is accountable for responding, how problems are noticed and conveyed to IT teams, and what technologies are used are all factors to consider.

When well-designed, incident management methods ensure that all problems are immediately addressed and that a high level of quality is maintained. Processes can also help teams improve their current operations to prevent future incidents and share this information with other reference institutions.

Incident management is a collection of techniques, processes, and tools that help teams discover, investigate, and respond to problems. It's a must-have for businesses of all sizes, and it's required by most data compliance regulations.

The process is only effective when the right incident lifecycle management tools are used.

The mapping of tools for incident resolution in the methodology presented is TheHive⁵ platform that is classified as an Incident Handling system and has the advantage of integration directly based on triggers for alerting based on use cases defined in the SIEM platform.

The resolution of incidents is based on the steps of the process and also has the precious help of Standard Operating Procedures (SoPs) that help complete each step oriented to the structure of the company and act as a guideline for a prompt response to reaction.

TheHive is connected to Splunk Enterprise via API (with specific development) and acts as a lever for triggering new alerts for resolution. The system is featured in version 4 and relies on Apache Cassandra⁶ for data storage.

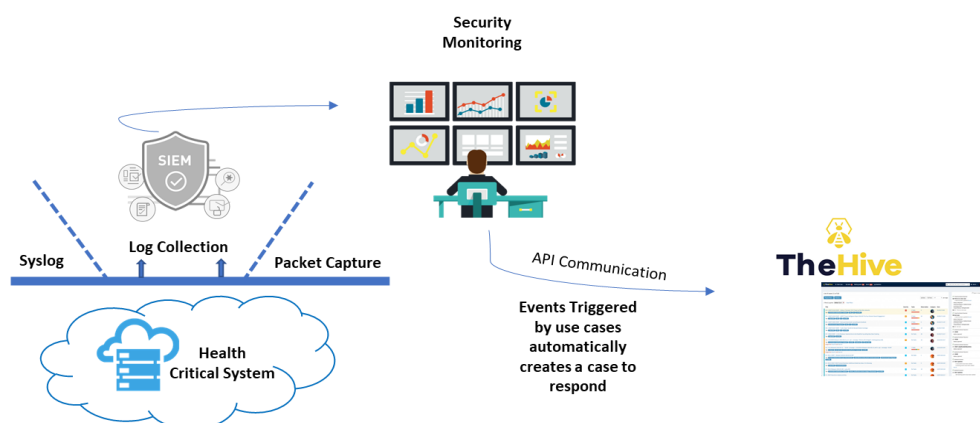


Figure 22: All-in-one Incident Management Process and Incident Resolution

⁵ <http://thehive-project.org>

⁶ <https://cassandra.apache.org>

Defining an incident response process is a core method for normative adequacy and correct incident resolution.

This procedure was created based on the information provided in the literature review and professional experience and intends to identify complementary forms of security analysis diagnosis. This procedure is an input of the Incident Management Process.

If on one hand what is Incident Management can be solved with incident monitoring and response, the investigation can happen in a complementary or parallel way in order to collect more information, better testing and analysis in order to lead us to the root cause with strong evidence for resolution of the security issue.

Looking at the yellow path in the Figure 23, the normal incident resolution process phases that intersect with the orange path are represented in a view of increasing the spectrum of analysis with activities practiced by the same team under the same conditions.

The information security investigation may occur singularly but when the incident resolution option is followed the investigation may appear as reinforcement of the first approach.

Incident handling is based on three main analysis tasks (identification, containment, and eradication & recovery), the derivation of the containment concept when further investigation is required (investigation), and finally continuity of process tasks (documentation and lessons learned).

Investigation in itself is a robust process aimed at identifying additional information about a given security risk. They can range from memory analysis, data collection, and reactive network analysis.

This procedure translates into complementarity between incident handling and security investigation. The investigation is something rawer and will be an additional route to the regular phases of incident handling, as represented in the Figure 23: All-in-one Incident Response Procedure.

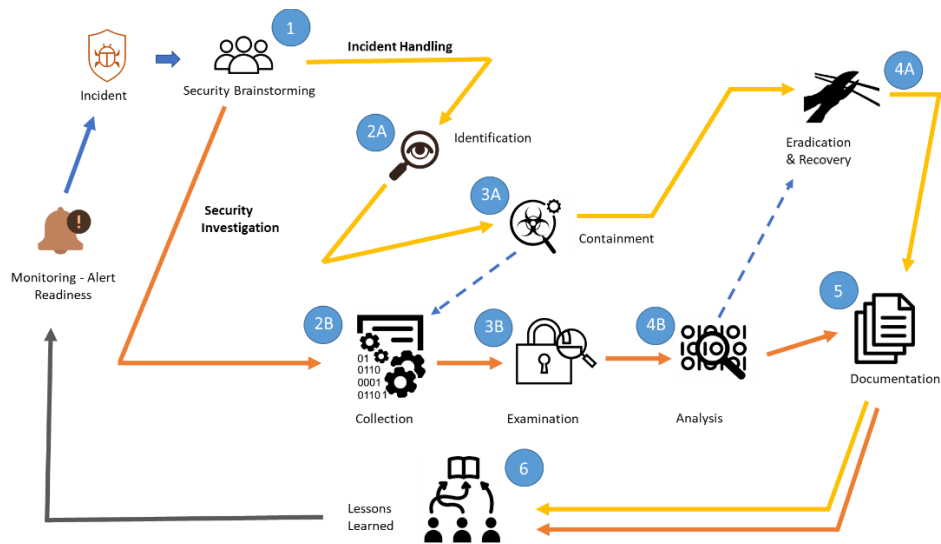


Figure 23: All-in-one Incident Response Procedure

3.3.4.1 DICOM Image Transaction - Security Investigation

Network Packet Collection

After defining the system to monitor, we must place an additional element that allows us to monitor the network communication and from there validate additional information. At the network communication level, the technique of gathering, collecting, and logging some or all packets that transit through a computer network, regardless of how the packet is addressed, is known as packet sniffing.

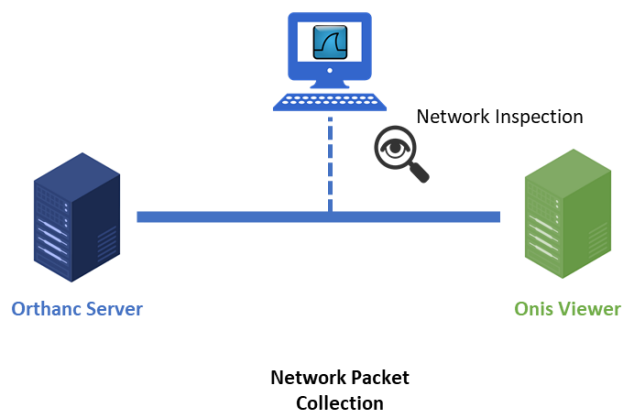


Figure 24: Network Packet Collection Representation

Every packet, or a determined selection of packets, can be gathered in this manner for subsequent analysis. As a network administrator, you may use the obtained data for a range of tasks such as monitoring bandwidth and traffic.

A packet sniffer, also known as a packet analyzer, is made up of two major components. First, a network adapter is required to connect the sniffer to the existing network. We then use the software that allows you to record, view, or analyze the data collected by it, in this case was used the network of the same machine, as we can check on the Figure 25. We then use the software that allows you to record, view, or analyze the data collected by it.

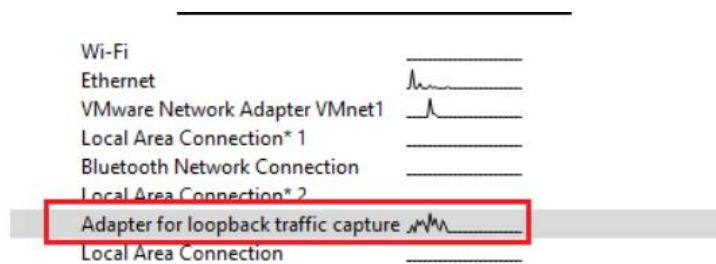


Figure 25: Types of interfaces to monitor

Wireshark has earned a reputation for being one of the most dependable network protocol analyzers on the market. This open-source application has been used as a comprehensive network analysis tool by users all around the world. Users can use Wireshark to troubleshoot network problems, investigate network security issues, debug protocols, and study network procedures. With the help of the npcap library, we will validate our loopback controller in order to validate the locally swapped packages given the installation of both servers in the same virtual machine.

Patterns and capture analysis

After capturing network data, a list of network packets is displayed on the centralized management panel or dashboard.

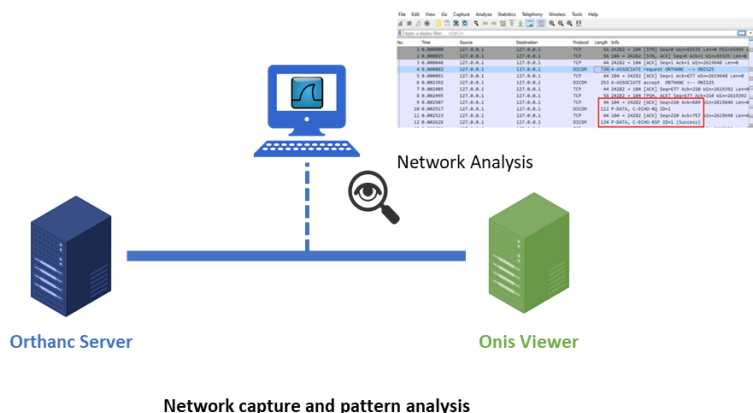


Figure 26: Network capture and pattern analysis

The screen is divided into three sections: packet list, packet bytes, and packet information. The packet list pane displays browsable captured network packets based on the timestamp to show when the packet was captured, the packet's protocol name, the packet's source and destination, and support information. The packet details pane displays information about the selected packet. Users can expand each section and use filters to find out more about specific items.

The internal data of the packet selected by the user is displayed in the Packet bytes window. By default, the data is shown in hexadecimal format.

Users must, however, click on any of the windows indicated above to obtain critical information about individual packets.

In this specific case, we will filter with the help of Wireshark the communications that we want to monitor with the help of its own syntax, in order to ensure performance and quick access in the analysis.

Show only DICOM based traffic

Filter:

dicom

In the impossibility of DICOM filtering during the capture it is possible to use the following command for inline visualization with the need with the TCP port.

Filter:

tcp port 104

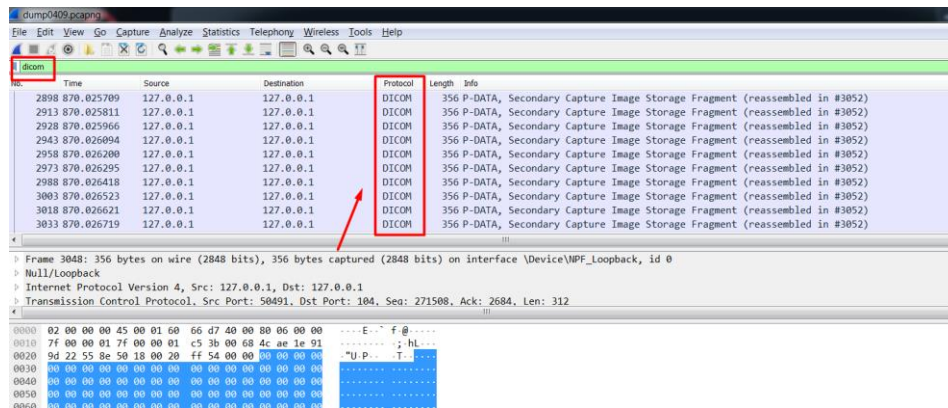


Figure 27: DICOM - Capture Filter

Evidence Identification

The identification of the evidence can be automatic or manual and can change depending on the experience of the operator. The whole procedure is based on the security investigation process in line with the incident response process. Capture, extraction and analysis are performed manually.

As a result, the communication may give us generalized hypothetical results such as malicious IPs, information about remote malicious executions, clear embedded files or execution payloads.

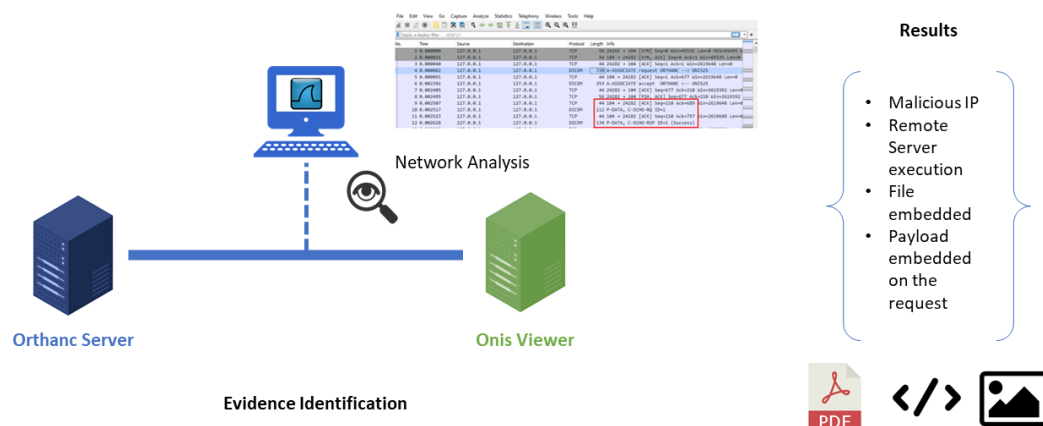


Figure 28: Evidence Identification Step

Incident Response Documentation & Recommendation

As described in the defined security monitoring methodology, after entering the security investigation line, upon completion of the analysis in the investigation phase, it should proceed to the eradication phase in order to implement permanent mitigation measures to overcome the issue security.

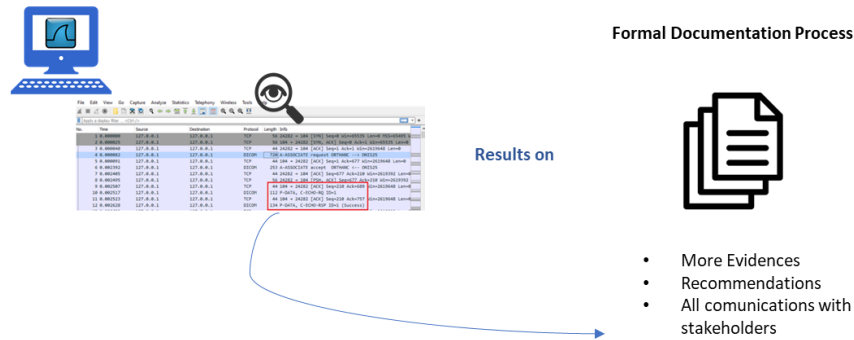


Figure 29: Documentation Step

In this procedure and on the artifact side, recommendations are given considering the investigation and alternative scenarios are suggested and all steps leading up to the resolution of the case are documented.

The procedure ends if new data is added to the incident handling path for resolution or, when separately used, causes the creation of a new security incident.

Chapter 4

Demonstration & Evaluation

In this chapter, two phases will be utilized to assess and evaluate the artifact described in the previous chapter as an integrated system.

For reference, there was a possibility of validation of the developed artifact and methodology in a real context in a Hospital, given the current conjuncture, it was not possible in time to align the work with that benefit, and we moved to the virtualization of the platform and the expert validation.

The first analysis responds with a hypothetical scenario that examines several parts of the methodology and framework. An overall scenario is offered, which constitutes the operation of the system as a whole and has been discussed in earlier chapters.

The second analysis is based on framework feedback from professionals in the field. Three experts were interviewed to discuss concerns and challenges related to and provide a comprehensive assessment of the framework components expressed in this study.

It is not the goal of contacting field specialists to produce survey results on where practitioners stand on various problems discussed in this dissertation. Experts are instead sought for their opinions on these matters, which are based on their professional expertise.

As mentioned in the methodology section, the demonstration and evaluation step had three milestone meetings for validation.

These meetings took place between July and September at the end of each iteration of the DSRM process. The meetings are based on demonstration of the scenario created, questions and answers, and interactions about how the methodology works in the different tools. The evaluators scores were collected and taken as a starting point in each iteration.

4.1 Demonstration Scenario

To demonstrate to the evaluators, what our artifacts can and do, a scenario was prepared that reflects the creation of an incident response methodology that translates into execution methods that respond in a framework artifact: an integrated automated incident monitoring and response system.

The scenario consists of the triggering of a previously defined use case that reflects the creation of a security incident case that will be analyzed. Following a direct path that previous knowledge base, it will require no further analysis and the response will be forwarded for resolution. There will be situations in which it will be necessary to evaluate initial information and start an in-depth analysis of the network assets to be monitored.

The demonstration scenario created is based on a virtualized system in a controlled environment that allows analysis to detect attempts to access the network segregated by external access and notice that the operating machines are having unexpected behavior (Successfully Logon after-hours).

The proposed scenario is triggered as follows:

- Defining the use case;
- Integration of the system(s) to be monitored;
- Trigger rules definition;
- Proactive analysis;
- Trigger for security incident;
- Automatic incident opening in the IHS platform;
- Automatic communication;
- Incident resolution procedure.

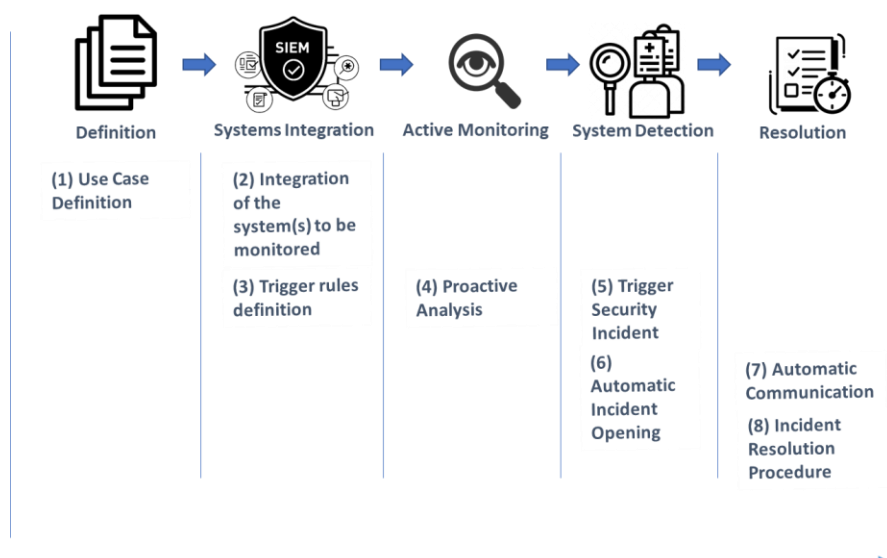


Figure 30: Validation: Demonstration Scenario

4.2 Evaluation

The assessment process following the DSRM methodology identifies the various iterations and the milestones of its execution, based on the unfolding of the process and the subtasks defined for its completion.

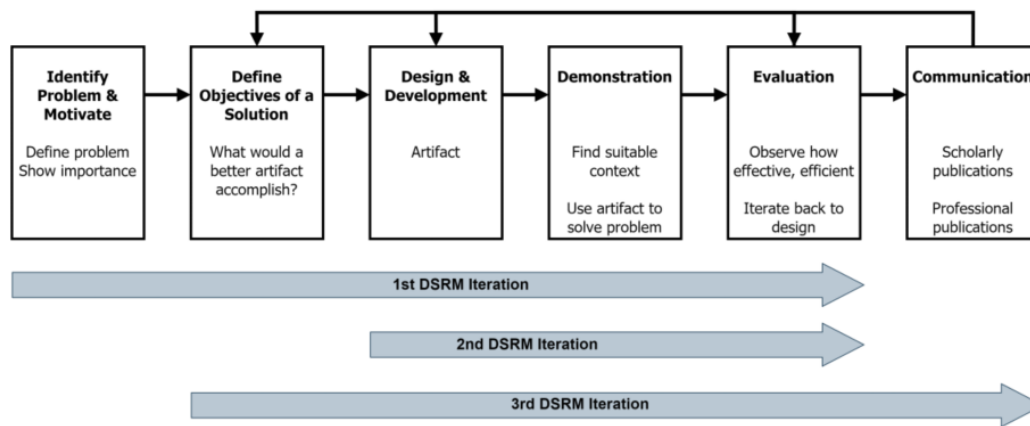


Figure 31: DSRM Iteration cycles

In line with what is written by most in the DSRM methodology community, the evaluation criteria are presented in a fragmented or incomplete manner [56]. To overcome this obstacle, it was decided to use the hierarchical evaluation criteria defined by Prat et al [56]. defined for IS artifacts. The Figure 32 presents the hierarchy and focuses on the criteria used to evaluate our artifact.

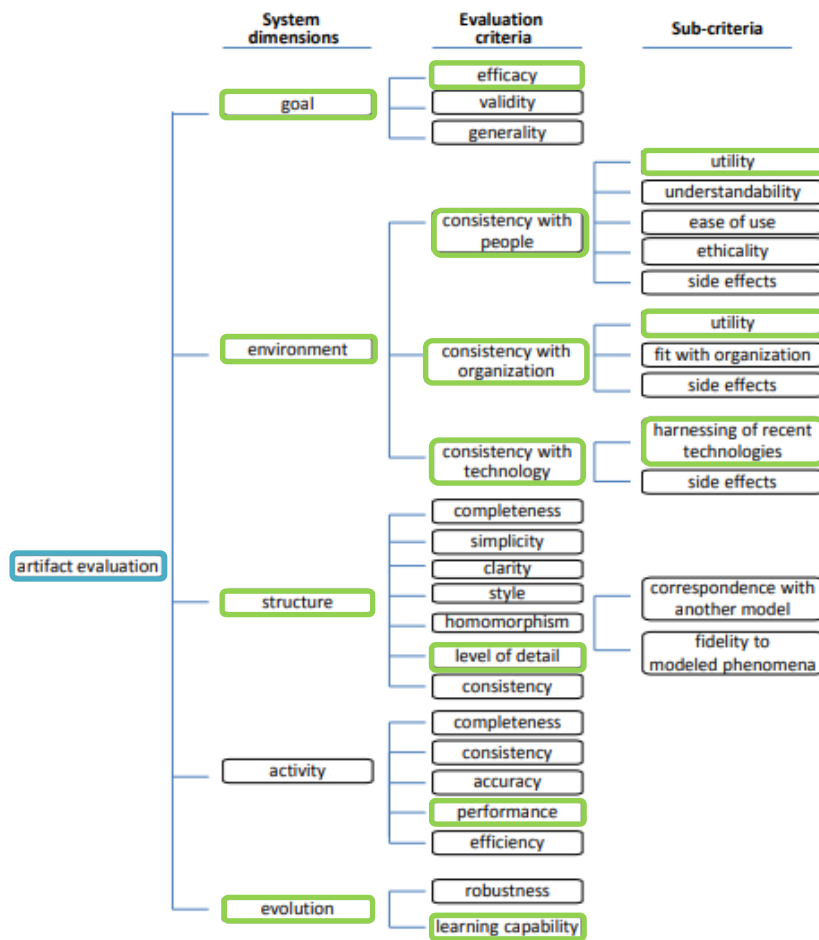


Figure 32: Hierarchy of criteria: artifact evaluation, Prat et al. [56]

Each evaluator assigns a score based on proof that the objective statement's added value has been achieved. In light of this, we've chosen to employ ISO 15504's [57] four-level NLPF scale, which includes four levels:

- Not Achieved (NA) - [0-15%]
- Partially Achieved (PA) -]15-50%]
- Largely Achieved (LA) -]50-85%]
- Totally Achieved (TA) -]85-100%]

4.2.1 Expert panel

Peers from the quorum of experts working in the fields of cybersecurity and incident response participated in this validation by answering a questionnaire aimed at evaluating the approach taken in this work.

We used the DSRM process model in three different iterations in our research. Each iteration had a distinct entry point, which varied depending on the stage of the process and the input we received after each demonstration and review.

Characteristics of expert panel, N = 3	
Gender	1 Female, 2 Males
Academic Disciplines (some with more than one degree)	1 Computer Engineering (Management Field), 1 Computer Engineering (Incident Response Specialist), 1 Computer Science (Cybersecurity specialization)
Position	1 Cybersecurity Project Manager, 1 Cybersecurity Incident Responder Specialist, 1 Cybersecurity Architect
General Work Experience	Average 33 years
Assessment instruments / process documentation	3 experts / peers
Theoretical knowledge about:	
Cybersecurity	2 experts
Networking	2 experts
Incident Response	2 experts
Forensics	2 experts
Threat Intel.	2 experts
Management	1 expert

Table 2: Characteristics of expert panel – Resume

4.2.2 1st DSRM Iteration

The first iteration turned out to be the longest. It stemmed from the initial identification of the problem and its goals to the development of the first version of the artifacts.

The evaluation of this first iteration was carried out to understand if the artifact was fit for purpose in line with the defined objectives in collaboration with the availability of the expert evaluators. The results of this first iteration are expressed in Table 3: Results of 1st iteration.

Criteria	Objective statement	Evaluator #1	Evaluator #2	Evaluator #3
Efficacy	Effectively leverage incident response in critical infrastructures to be monitored	LA	LA	LA
Consistency of created IR methodology with resources and tech. knowledge/Technology	Solution complies with the latest methods, best-practices, and tools for incident response	(Final iteration)	(Final iteration)	(Final iteration)
Consistency with critical health infrastructures needs/Utility	Targeting security incident detection, infrastructure hardening, and mitigation measures	LA	LA	LA
Consistency with organization field/Utility	The solution bring value to increase awareness and posture to monitor and solve cybersecurity incidents	PA	PA	PA
Level of detail	The solution provides the level of detail to help decision makers manage their teams and make more investment in cybersecurity	LA	LA	PA
Performance	Correctly integrate, monitor, and trigger cybersecurity use cases amongst several operational systems	PA	PA	PA
Learning capability	Automatically learn patterns about security intel amongst use cases defined	LA	LA	LA

Table 3: Results of 1st iteration

In line with the planned schedule, the evaluation relied on the three experts who validated the initial phase of the artifacts and where they were received. Some doubts were clarified, and some notes were taken into consideration for the remaining iterations. Given the maturity issue of the first version, this demo did not include many of the foreseen automations and the final definition of the use cases raised.

For our evaluators there was a note to retain regarding the integrations not being properly completed on the Consistency with organization field/Utility criterion because it should directly demonstrate what is missing for organizations where the core business is to provide medical services and only by having additional resources can they dispense or recruit more resources to deal with improvement tasks.

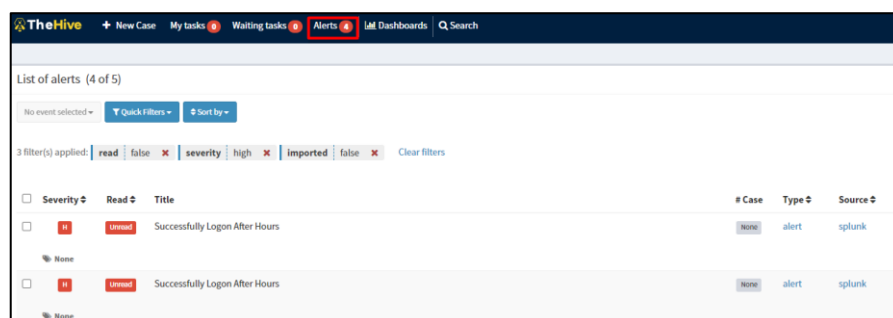
4.2.3 2nd DSRM Iteration

The second iteration of the DSRM was focused on solving the issues from the first iteration that had no integration performed: the first step of Design & Development of the artifact.

With this, the validation scenario only focused on those same integrations for their due revalidation. In this iteration some developments were finished, to highlight:

- **Automatic receipt of alerts**

The alerts that were created to trigger in the defined use cases now have automatic alarming to the incident resolution platform. Their creation is now automatic, and events do not need to be manually passed with the need for active monitoring by the operator.



The screenshot shows the 'Alerts' tab in TheHive. It displays a list of 4 alerts. The first alert is 'Successfully Logon After Hours' with a severity of 'High' and a status of 'Unread'. It is an 'alert' type from the 'splunk' source. The interface includes filters for 'read', 'severity', and 'imported'.

Severity	Read	Title	# Case	Type	Source
High	Unread	Successfully Logon After Hours	None	alert	splunk
High	Unread	Successfully Logon After Hours	None	alert	splunk

Figure 33: Automatic integration of incidents alert from Splunk

- **Assigning tasks to operators**

When an event triggers a use case rule, the operator can automatically triage the incident and classify it as an information security incident.

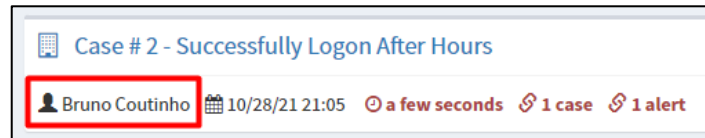


Figure 34: Automatic assignee of cases resolution

- **Document incident response process as walkthrough**

An incident can be quickly resolved based on the phases of the industrialized incident life cycle in the platform and with a procedure guide: SoPs.

Criteria	Objective statement	Evaluator #1	Evaluator #2	Evaluator #3
Efficacy	Effectively leverage incident response in critical infrastructures to be monitored	LA	LA	FA
Consistency of created IR methodology with resources and tech. knowledge	Solution complies with the latest methods, best-practices, and tools for incident response	(Final iteration)	(Final iteration)	(Final iteration)
Consistency with critical health infrastructures needs/Utility	Targeting security incident detection, infrastructure hardening, and mitigation measures	LA	LA	LA
Consistency with organization field/Utility	The solution bring value to increase awareness and posture to monitor and solve cybersecurity incidents	LA	LA	LA
Level of detail	The solution provides the level of detail to help decision makers manage their teams and make more investment in cybersecurity	LA	LA	FA
Performance	Correctly integrate, monitor, and trigger cybersecurity use cases amongst several operational systems	LA	LA	LA
Learning capability	Automatically learn patterns about security intel amongst use cases defined	LA	LA	LA

Table 4: Results of 2nd Iteration

In this iteration the existing doubts about the integrations have been overcome and it was possible to verify, not yet in their final state, the tailored developments made.

Finally, the cybersecurity profiles, more technical, on the criteria of Consistency with critical health infrastructures needs/Utility, Consistency with organization field/Utility and Level of the detail that despite the automatism and through optimization of resources and means that alarmistic should be more directed to those who respond to it and allow users not to be all day monitoring the systems.

4.2.4 3rd DSRM Iteration

In line with the notes suggested in iteration 2 of DSRM, the possibilities of giving portability to a monitoring and resource optimization requirement were evaluated.

As we are almost always connected to our smartphones or email there should be a redundancy about the communication path for opening a case. The following functionalities were developed:

- **Cases are now transcribed to a chatbot on the webchat platform**

Open cases can be tracked on their priority or urgency and which system they refer to remotely in a team communication group. From here the awareness about the systems in production is increased. The platform chosen was Telegram ⁷ to receive all the urgent information to respond to the security incidents.



Figure 35: Incident Alert creation

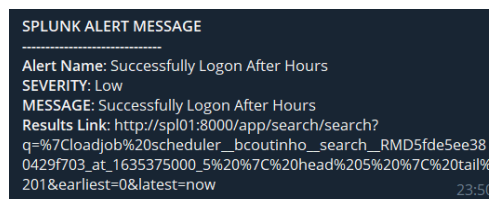


Figure 36: Chatbot automatic message - remote alert

- **Open cases are now sent to the distribution list of the responsible team**

Via email the open cases are now opened via email where they are flagged with their id and reference for treatment.

⁷ <https://telegram.org/>

Criteria	Objective statement	Evaluator #1	Evaluator #2	Evaluator #3
Efficacy	Effectively leverage incident response in critical infrastructures to be monitored	FA	FA	FA
Consistency of created IR methodology with resources and tech. knowledge	Solution complies with the latest methods, best-practices, and tools for incident response	LA	LA	LA
Consistency with critical health infrastructures needs/Utility	Targeting security incident detection, infrastructure hardening, and mitigation measures	LA	LA	LA
Consistency with organization field/Utility	The solution bring value to increase awareness and posture to monitor and solve cybersecurity incidents	FA	FA	FA
Level of detail	The solution provides the level of detail to help decision makers manage their teams and make more investment in cybersecurity	FA	FA	FA
Performance	Correctly integrate, monitor, and trigger cybersecurity use cases amongst several operational systems	LA	LA	LA
Learning capability	Automatically learn patterns about security intel amongst use cases defined	LA	LA	LA

Table 5 - Results of 3rd Iteration

These last developments in this iteration raised interest and general agreement among the evaluators.

All the points of doubt that had not been positively evaluated in the first iterations were considered as Largely Achieved (LA) and with the evolution of the evaluation, some of those that were initially mature enough to be Largely Achieved (LA) became Fully Achieved (FA), as is the case of the criteria Efficacy, Consistency with organization field/Utility and Level of Detail.

Chapter 5

Conclusions & Future Work

5.1 Conclusions

The main objective of this work was the implementation of security practices in critical healthcare delivery systems, thereby increasing resilience and health postures in scenarios of cyber-attack, fraud and data tampering in a real medical context.

The collaboration with a reference hospital lacked the feedback and spirit of collaboration needed to bring this integration to fruition. With significant enough work already in progress it was necessary to recreate the system thought out and adapt it to a methodology that is mirrored in the creation of an integrated artifact and the integration of several virtualized systems with the intended security intelligence.

The methodology ends up being the differentiating and disruptive point with the introduction of information security in a medical context and in critical instruments where cybersecurity is often despised, because it is seen as something accessory to its main mission, which is to diagnose and save lives.

With these goals and redefinition in mind an artifact was created that maps directly onto a methodology for intelligent security incident response in operational environments. This allowed to be safeguarded and derive two main research questions:

- Can the introduction of security incident response methodology direct towards a proactive positioning of security and enforcement of controls in healthcare?
- Can active monitoring of critical systems improve the application of more and better controls at the level and enhance the incident response process in Health Units?

As our work unfolded, we were able to develop a methodology that derives from related work in the field, years of experience, and specific needs of the common information security incident resolution process.

Given the impossibility of creating data in real context, we were forced to virtualize a large medical image storage system - Picture Archive and Communication Systems (PACS) - and use it to validate anonymized medical images and experiment with the effects of cross-platform communications and the particularities of the DICOM protocol for better analysis.

With the complementary path of the incident response procedure, we saw it possible to improve this protocol itself beyond what it originally provides. And we came to some conclusions in our analysis: if our

modalities do not support some controls due to construct definition limitations, you will need to abstract higher security at the OS or network level to help ensure this and opt for an approach based on real use cases.

In addition to ensuring the use of all granular controls built in, regardless of the PACS modality endpoint you should also consider wrapping all DICOM image transfers through a TLS connection tunnel. Some information capture modalities do not support encryption or only support legacy TLS v1.0 or SSLv3. To get around this, it is necessary to wrap each endpoint connection using a local port redirector.

In validating these capital points, we found that by doing so we would only get recommendations on the robustness of the controls of the protocol itself and would be downplaying the points regarding the evaluation of anomalous behavior in networks dedicated to operationalizing these types of components. As seen in 2.6 Protection of Health Critical Systems, deriving in security anomalous event detection technology is possible through behavior specification. This is where business knowledge and specific use case definition come in.

Since we need to ensure that medical images are not compromised, we needed to go deep into what concerns protecting the infrastructure and here we go to the evaluation of behaviors in the network transactions that trigger previously defined rules that will alert us about anomalous behaviors that will be the target of triage, analysis, treatment, and response, in cases of security incident.

In the basic structure of the framework, we have the integration of sources of logs in the core engine of this development. That is the SIEM infrastructure that allows us to give intelligence to the framework and be the conductor for the detection of possible cases. It gives the trigger for the resolution of incidents with the development of tools for its integration with the TheHive platform for targeted resolution of incidents.

Following the development of this work, the evaluation was based on the consultation with three experts that reinforced the possibility of answering the research questions.

Despite all the limitations assumed, the artifact together with the methodology can efficiently leverage the security posture, contribute to define successful controls in hospital environment practices and, above all, contribute to the active monitoring of operational environments. This innovative approach leverages the stated investment in cybersecurity and realizes that this same investment is our main way to protect ourselves in the cyberspace.

Despite deserving future continuation, it was possible to assess the applicability, usefulness and consistency of this development through peer reviews required from experts in the field.

The assessments were based on three experts: in the field of cybersecurity and incident response. With their experience of the factual needs of the area and the knowledge to implement it, they give us the evidence and endorsement for the evaluations went from Largely Achieved to Fully Achieved in the various criteria analysis.

As occasion makes chance, with a limited scope and the unforeseen collaboration having fallen through, we have to point out that it was through this scenario that this methodology was created, and that the artifact can be worked upon.

With this, energetically and aspiring a projection of challenging future applicability, I hope that there is the opportunity to continue this work and that it brings value to the implementation in real context in future iterations and be an asset to the safeguarding of patient data and that this is a change of mindset to effectively bet on the materialization of cybersecurity in an operational context and the criticality that the health sector holds for all of us: not being a common place for cybersecurity today.

Given the current context and challenges, change is urgent and becomes decisive.

5.2 Future Work

Despite the validations considered, we hope that the work developed can inspire future iterations for the cybersecurity area and its derivation for the practice of active monitoring in critical devices in the healthcare area.

As previously assumed, the definition of this cybersecurity approach ends up being limited by its non-application in a real context. As the great is the enemy of the good, we encourage the continuation of this work to be the application of this methodology and artifact to help in critical areas enhancing cybersecurity.

With this it can be developed a library of use cases aligned with expectations, knowledge base of previously known attacks, new trends and preventing future incidents.

The introduction of innovative approaches, as the one presented in this dissertation, must be seen as complimentary to other cybersecurity sensitive and important aspects such as aging resources, lack of training, human factor (motivation and potential to commit illegalities against the employer), security policies and planning.

In line with the work developed, it should also be accompanied by a training and awareness base at the global level of the organizations where these innovative practices will be implemented.

References

- [1] “19 Healthcare Cyber Security Statistics You Need To Know In 2020 | PurpleSec.” <https://purplesec.us/cyber-security-healthcare-statistics/> (accessed Oct. 10, 2021).
- [2] R. M. Van Der Knijff, “Control systems/SCADA forensics, what’s the difference?,” *Digit. Investig.*, vol. 11, no. 3, pp. 160–174, 2014, doi: 10.1016/j.diin.2014.06.007.
- [3] B. A. Jeffries, “TRACE : Tennessee Research and Creative Exchange INTRUSION DETECTION OF A SIMULATED SCADA SYSTEM USING A DATA-DRIVEN MODELING APPROACH,” 2017.
- [4] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *Electr. Inf. Shar. Anal. Cent.*, p. 36, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- [5] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA security in the light of cyber-warfare,” *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, 2012, doi: 10.1016/j.cose.2012.02.009.
- [6] “TAU Threat Advisory: Imminent Ransomware threat to U.S. Healthcare and Public Health Sector | Security & Compliance Blog | VMware.” <https://blogs.vmware.com/security/2020/10/tau-threat-advisory-imminent-ransomware-threat-to-u-s-healthcare-and-public-health-sector.html> (accessed Oct. 10, 2021).
- [7] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, 2009, doi: 10.1016/j.cose.2008.08.003.
- [8] M. Thomas, “2020 Global Threat Intelligence Report (GTIR),” *Ntt*, 2020.
- [9] HHS - United States Department of Health and Human Services, “2020: A Retrospective Look at Healthcare Cybersecurity,” 2021.
- [10] D. Liveri, A. Sarri, and C. Skouloudi, *Security and Resilience in eHealth*. 2015.
- [11] S. Report and C. Ventures, “The 2020 Healthcare Cybersecurity Report 2020 Healthcare Cybersecurity Report Cybersecurity Ventures,” pp. 1–5, 2020, [Online]. Available: www.herjavecgroup.com.
- [12] J. Cawthra., “Securing Picture Archiving and Communication System (PACS),” 2019.
- [13] ENISA, European Union Agency for Cybersecurity (ENISA), European Union Agency for Cybersecurity, European Union Agency for Cybersecurity (ENISA), and ENISA, “PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS Good practices for the security of Healthcare services FEBRUARY 2020,” *Baseline Secur. Recomm. IoT Context Crit. Inf. Infrastructures*, no. November, pp. 1–30, 2018, doi: 10.2824/939028.
- [14] K. Mcy, “Perspectives on transforming cybersecurity,” *McKinsey Glob. Inst.*, vol. 32, no. March, pp. 1–128, 2019, [Online]. Available: [https://www.mckinsey.com/~media/McKinsey/McKinsey Solutions/Cyber Solutions/Perspectives on transforming cybersecurity/Transforming cybersecurity_March2019.ashx](https://www.mckinsey.com/~media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx).
- [15] H. Österle, “Memorandum on design-oriented information systems research,” *Eur. J. Inf. Syst.*, vol. 20, no. 1, pp. 7–10, 2011, doi: 10.1057/ejis.2010.55.
- [16] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Q. Manag. Inf. Syst.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.
- [17] K. Peffers, “The design science research process: A model for producing and presenting information systems research,” *arXiv*, no. May 2014, 2020.
- [18] D. Moher, “Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement,” *PLoS Med.*, vol. 6, no. 7, 2009, doi: 10.1371/journal.pmed.1000097.

- [19] J. D. Lecy and K. E. Beatty, "Representative Literature Reviews Using Constrained Snowball Sampling and Citation Network Analysis," *SSRN Electron. J.*, pp. 1–15, 2012, doi: 10.2139/ssm.1992601.
- [20] E. Amoroso and A. Ginter, "OT Security for IT Professionals: An Introduction to Industrial Cyber Controls."
- [21] V. M. Ijure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, 2006, doi: 10.1016/j.cose.2006.03.001.
- [22] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1942–1976, Jul. 2020, doi: 10.1109/COMST.2020.2987688.
- [23] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," *Int. J. Distrib. Sens. Networks*, vol. 14, no. 8, 2018, doi: 10.1177/1550147718794615.
- [24] A. Sethi and G. Wills, "Expert-interviews led analysis of EEVi-A model for effective visualization in cyber-security," *2017 IEEE Symp. Vis. Cyber Secur. VizSec 2017*, vol. 2017-October, pp. 1–8, Oct. 2017, doi: 10.1109/VIZSEC.2017.8062195.
- [25] M. Coudriau, A. Lahmadi, and J. Francois, "Topological analysis and visualisation of network monitoring data: Darknet case study," *8th IEEE Int. Work. Inf. Forensics Secur. WIFS 2016*, Jan. 2017, doi: 10.1109/WIFS.2016.7823920.
- [26] K. Rieck, P. Trinius, C. Willems, and T. Holz, "Automatic analysis of malware behavior using machine learning," *J. Comput. Secur.*, vol. 19, no. 4, pp. 639–668, Jan. 2011, doi: 10.3233/JCS-2010-0410.
- [27] S. Muthuraj, M. Sethumadhavan, P. P. Amritha, and R. Santhya, "Detection and Prevention of Attacks on Active Directory Using SIEM," *Smart Innov. Syst. Technol.*, vol. 196, pp. 533–541, May 2020, doi: 10.1007/978-981-15-7062-9_53.
- [28] Y. X. Lai, Z. H. Liu, X. T. Cai, and K. X. Yang, "Research on intrusion detection of industrial control system," *Tongxin Xuebao/Journal Commun.*, vol. 38, no. 2, pp. 143–156, 2017, doi: 10.11959/j.issn.1000-436x.2017036.
- [29] H. Li, B. Wang, and X. Xie, "An improved content-based outlier detection method for ICS intrusion detection," *Eurasip J. Wirel. Commun. Netw.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13638-020-01718-0.
- [30] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.
- [31] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Comput. Networks*, vol. 136, pp. 37–50, 2018, doi: 10.1016/j.comnet.2018.02.028.
- [32] R. B. Benisha and S. Raja Ratna, "Design of Intrusion Detection and Prevention in SCADA System for the Detection of Bias Injection Attacks," *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/1082485.
- [33] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6603>. [Accessed: 30-Sep- 2016]. [16]," *Tech. Rep.*, vol. 99, pp. 1–15, 2000, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6603>.
- [34] R. S. Ismail Butun, Salvatore D. Morgera, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Commun. Surv. TUTORIALS*, vol. 16, no. 1, pp. 266–280, 2014.
- [35] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, no. February, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.
- [36] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A survey on security control and attack

- detection for industrial cyber-physical systems,” *Neurocomputing*, vol. 275, pp. 1674–1683, 2018, doi: 10.1016/j.neucom.2017.10.009.
- [37] R. Mitchell and I. R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” *ACM Comput. Surv.*, vol. 46, no. 4, 2014, doi: 10.1145/2542049.
 - [38] I. N. Fovino, A. Carcano, T. De Lacheze Murel, A. Trombetta, and M. Masera, “Modbus/DNP3 state-based intrusion detection system,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 729–736, 2010, doi: 10.1109/AINA.2010.86.
 - [39] D. Hadžiosmanović, D. Bolzoni, P. Hartel, and S. Etalle, “MELISSA: Towards automated detection of undesirable user actions in critical infrastructures,” *Proc. - 2011 7th Eur. Conf. Comput. Netw. Defense, EC2ND 2011*, pp. 41–48, 2012, doi: 10.1109/EC2ND.2011.10.
 - [40] N. Erez and A. Wool, “Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 10, pp. 59–70, 2015, doi: 10.1016/j.ijcip.2015.05.001.
 - [41] W. Gao, T. Morris, B. Reaves, and D. Richey, “On SCADA control system command and response injection and intrusion detection,” *Gen. Members Meet. eCrime Res. Summit, eCrime 2010*, 2010, doi: 10.1109/ecrime.2010.5706699.
 - [42] N. Goldenberg and A. Wool, “Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 2, pp. 63–75, 2013, doi: 10.1016/j.ijcip.2013.05.001.
 - [43] S. Cheung, “Using Model-based Intrusion Detection for SCADA Networks,” 2006. doi: 10.1136/bmj.329.7461.331.
 - [44] D. Peterson, “Quickdraw: Generating security log events for legacy SCADA and control system devices,” *Proc. - Cybersecurity Appl. Technol. Conf. Homel. Secur. CATCH 2009*, pp. 227–229, 2009, doi: 10.1109/CATCH.2009.33.
 - [45] F. H. Cybersecurity, “Horizon Report,” 2020. [Online]. Available: <http://insights.ovid.com/crossref?an=00024776-201705000-00016>.
 - [46] V. Liu, M. A. Musen, and T. Chou, “Data breaches of protected health information in the United States,” *JAMA - J. Am. Med. Assoc.*, vol. 313, no. 14, pp. 1471–1473, 2015, doi: 10.1001/jama.2015.2252.
 - [47] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, “Security Techniques for the Electronic Health Records,” *J. Med. Syst.*, vol. 41, no. 8, 2017, doi: 10.1007/s10916-017-0778-4.
 - [48] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, “Access Control Policy Enforcement for Zero-Trust-Networking,” *29th Irish Signals Syst. Conf. ISSC 2018*, 2018, doi: 10.1109/ISSC.2018.8585365.
 - [49] G. El Hajal, R. Abi Zeid Daou, Y. Ducq, and J. Börcsök, “Designing and validating a cost effective safe network: Application to a PACS system,” *Int. Conf. Adv. Biomed. Eng. ICABME*, vol. 2019-Octob, pp. 2019–2022, 2019, doi: 10.1109/ICABME47164.2019.8940252.
 - [50] D. F. Sittig and H. Singh, “A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks,” *Appl. Clin. Inform.*, vol. 7, no. 2, pp. 624–632, 2016, doi: 10.4338/ACI-2016-04-SOA-0064.
 - [51] L. F. Maimó, A. H. Celdrán, Á. L. Perales Gómez, F. J. García Clemente, J. Weimer, and I. Lee, “Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments,” *Sensors (Switzerland)*, vol. 19, no. 5, pp. 1–31, 2019, doi: 10.3390/s19051114.
 - [52] G. Østby, B. K.- ICISSP, and undefined 2020, “Maturity Modelling to Prepare for Cyber Crisis Escalation and Management,” *scitepress.org*, Accessed: Oct. 10, 2021. [Online]. Available: <https://www.scitepress.org/Papers/2020/88716/88716.pdf>.
 - [53] I. Alsmadi, “Incident Response,” *NICE Cyber Secur. Framew.*, pp. 331–346, 2019, doi: 10.1007/978-3-030-02360-7_13.

- [54] “Building a sustainable SIEM use cases. | by Olu BaBaCaMp | Medium.” https://medium.com/@olucampbell_64749/building-a-sustainable-siem-use-cases-8f58408db375 (accessed Oct. 10, 2021).
- [55] “Description of Actual State Sensor Types for the Software Asset Management (SWAM) Capability,” 2014.
- [56] N. Prat, I. Comyn-Wattiau, and J. Akoka, “Artifact evaluation in information systems design-science research - A holistic view,” *Proc. - Pacific Asia Conf. Inf. Syst. PACIS 2014*, 2014.
- [57] S. International Organization for Standardization, Geneva, CH, “Information technology — Process assessment — Part 2: Performing an assessment,” 2003.

