INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Visualization of Security in Industrial Control Systems respecting IEC-62443

Alexandre Gil de Sá Martins

Master in, Computer Science and Management

Supervisor:
Doctor Maria Cabral Diogo Pinto Albuquerque, Assistant Professor,
Iscte-Instituto Universitário de Lisboa

Co-Supervisor:
Master Dirk Kroeselberg, Security Expert,
Siemens Technology

December, 2020

[This page has been intentionally left blank]

iscte

TECNOLOGIAS
E ARQUITETURA

Visualization of Security in Industrial Control Systems respecting IEC-62443

Alexandre Gil de Sá Martins

Master in, Computer Science and Management

Supervisor:
Doctor Maria Cabral Diogo Pinto Albuquerque, Assistant Professor,
Iscte-Instituto Universitário de Lisboa

Co-Supervisor:
Master Dirk Kroeselberg, Security Expert,
Siemens Technology

December, 2020

[This page has been intentionally left blank]

Visualization of Security in Industrial Control Systems respecting IEC-62443

[This page has been intentionally left blank]

I dedicate all this work to my dear grandfather, Manuel de Tomaz de Sá, who always encouraged me to give my best in any situation despite difficulties.

12/1/2020

[This page has been intentionally left blank]

Acknowledgements

I want to acknowledge my supervisors, Maria Pinto Albuquerque, for being present during all the process and my co-supervisor, Dirk Kroeselberg, for all the help and guidance throughout the project. I also would like to thank Tiange Zhao for being my unofficial supervisor for all the support and advice in the work developed. To all the professionals at Siemens Cybersecurity Technology Security lifecycle team for providing me a great work environment and excellent acceptance in the team, especially to Tiago Gasiba for the concern and advice during my time at Siemens.To Siemens for providing me a unique experience and for giving me this opportunity to learn every day and develop my master's thesis with professionals that help me in any need.

I want to thank my friends and my girlfriend for all the support given during the thesis. Despite the distance, their support was needed to help me focus on the thesis and encourage making my decisions right.

Finally, to my family, the most important thanks to helping in every situation in this six months adventure, especially to my aunt Paula Odete Fernandes for revising the english, for helping with statistical analysis and the elaboration of the questionnaire.

[This page has been intentionally left blank]

Abstract

The importance of visualizing security in industrial control systems respecting the IEC-62443 security standards has increased. This is due to the increase in cyber attacks, its complexity over time, and the security standards created to protect users from compromising them. Through an adequate visualization of security information, it is possible to manage and analyze information to make decisions for good management of systems' security.

In this sense, this study's main objective was to describe a possible solution to assist in security management, having been developed in partnership with Siemens Technology, based in Germany. Thus, appropriate tools were used and evaluated to model the data and create visual elements to represent the industrial control system's components. Their security attributes were chosen to be in a dashboard. Kibana was used for three case studies, the last one being the most important for Siemens. The data were obtained through the security software test tool. These were organized and treated to be in a configuration that allowed them to be imported into Kibana and create a dashboard containing the information needed to make decisions and discover gaps in the system. Subsequently, the proposed solution was evaluated through a questionnaire applied to the specialists responsible for industrial control systems security to obtain suggestions that would improve its usefulness and security management assistance.

From the results obtained, it was possible to observe the security representation using a visualization tool, demonstrate compliance with IEC-62443 security protocols, thus enabling a simplified security analysis of an industrial control system.

Keywords: Industrial Control Systems, Visualization for Security Management, Visual Data Modeling and Analysis, Security Visualization, Security Requirements, Security standards (IEC-62443 series).

[This page has been intentionally left blank]

Resumo

A importância de visualizar segurança em sistemas de controlo industrial respeitando as normas de segurança IEC-62443 tem vindo a aumentar. Isto deve-se, ao aumento dos ciberataques, da sua complexidade e das normas criadas para proteger os sistemas. Através de uma adequada visualização de informação sobre a segurança torna-se possível gerir e analisar a informação para tomar decisões e fazer uma boa gestão de segurança.

O presente estudo teve como principal objetivo descrever uma solução possível para auxiliar na gestão de segurança tendo sido desenvolvida em parceria com *Siemens Technology*, sediada na Alemanha. Assim, recorreu-se à avaliação das ferramentas utilizadas para modelar dados e criar elementos visuais para representar os componentes num sistema de controlo industrial e os atributos de segurança escolhidos para estarem num dashboard. O *Kibana* foi utilizado para três casos, sendo o último o mais importante para a Siemens. Os dados foram obtidos através da ferramenta de teste do software de segurança. Estes foram organizados e tratados de forma a criar um dashboard contendo a informação necessária para tomar decisões e descobrir lacunas no sistema. Posteriormente, a solução proposta foi avaliada através de um questionário aplicado aos especialistas de segurança de sistemas de controlo industrial, com o propósito de se obterem sugestões que permitissem melhorar a sua utilidade e assistência na gestão da segurança.

Com os resultados obtidos foi possível observar a representação de segurança utilizando uma ferramenta de visualização, respeitando os protocolos de segurança IEC-62443, possibilitando, uma análise simplificada da segurança num sistema de controlo industrial.

Palavras-chave: Sistemas de controlo industrial, Visualização na gestão de segurança, Modelação e Análise Visual dos Dados, Visualizacao de seguranca, Requisitos de segurança, Standards de segurança (IEC-62443 series).

[This page has been intentionally left blank]

Contents

[This page has been intentionally left blank]

List of Figures

List of Tables

[This page has been intentionally left blank]

Glossary

Actuators Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller.

Controllers The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators.

Elasticsearch "Open source full-text search engine written in Java that is designed to be distributive, scalable, and near real-time capable" to manage large amounts of online and schema-less data [1].

Sensors A sensor is a device that produces some measurement of some physical property and then sends this information as controlled variables to the controller.

[This page has been intentionally left blank]

Acronyms

ANSI	America National Standard Institute.
CVSS	Common Vulnerability Scoring System.
DCS	Distributed Control System.
EBSE	Evidence-based software engineering.
HMI	Human-Machine Interface.
IACS	Industrial Automation and Control Systems.
ICS	Industrial Control System.
IEC	International Electrotechnical Commission.
ISA	International Society for Automation.
OEM	Original Equipment Manufacturer.
PLC	Programmable Logic Controllers.
SCADA	Supervisory Control and Data Acquisition System.
SIG	Special Interest Group.
SPSS	Statistical Package for the Social Sciences.

[This page has been intentionally left blank]

Chapter One

Introduction

Contents

1.1 Overview

This chapter introduces the motivation and scope of this work by describing some security visualization problems and ways to visualize security about the industrial control system. Then it describes the research questions of this study and an outline of the following chapters.

This thesis was developed in the context of a partnership between Iscte - Instituto Universitário de Lisboa and Siemens Technology in Munich, Germany. Some data is sensitive and will not be displayed according to the author and the Siemens contract.

1.2 Context

"Security Visualization is a very young term. It expresses the idea that common visualization techniques have been designed for use cases that are not supportive of security-related data, demanding novel techniques fine-tuned for the purpose of thorough analysis" [2].

However, it is advancing at a fast pace. Today, the way we visualize security information is crucial for the management and business decisions that can impact industries.

The Industrial Control Systems, e.g., typically used in electrical, water, chemical, transportation, pharmaceutical, food, are facing a high demand for security. The Industrial Control Systems needs systematic methodologies and tools to support an automatic secure configuration and setting for operations, vulnerabilities in complex systems, and eventual attacks that can compromise information and jeopardize industries. Also, industry process systems are automatic and long-living systems that go through changing requirements throughout their life cycle. These also are used to control critical infrastructures and security is becoming a real issue that owners and vendors are facing. One of the gaps that this study cover is a method for security automation visualization in industrial control systems, this could be valuable as no customized security counteractive exist today. The present security solutions have not been designed and develop with the same constraints as the ones in industrial control systems [3].

1.3 Motivation

When attempting to solve the problems mentioned above, an adequate security visualization provides relevant and even crucial support. By visualizing the information that we need, together with filter and analysis capabilities, we can manage industrial assets security in an industrial control system.

Since there are many tools for that purpose, the motivation is to build a visualization panel and methodologies to support the asset's overall automation security with specific security standards. With such a tool, it will be possible to visualize the appropriate information to manage security.

1.4 Goals

The main goal is to develop a visualization solution with a tool that solves the lack of visualization techniques and methodologies to visualize industry assets' security, incorporating requirements from International Electrotechnical Commission (IEC)-62443.

This will require sub-objectives, such as to analyze visualization approaches, tools, and requirements related to a component, system, and network attributes.

It is also required to become familiar with the IEC-62443-X-X series standards, specifically with the 2-4 and 3-3 security standards, respectively. It also is needed to rate the tools on their applicability by criteria that will be defined and propose the visualization method for security blueprint.

At the end of the study, we can answer the questions in the next section 1.5.

1.5 Research Questions

The main research questions in the current study are:

- **RQ1** - "How to visualize security in industrial control systems, incorporating requirements from IEC-62443 standards?"
    - **RQ1.A** - "What would be an appropriate tool for security visualization?"
    - **RQ1.B** - "What related components, systems, and network attributes should be present?"

This study intends to research which requirements and components should be present on the chosen tool's representation panel. This panel will enable the users to see and analyze system information to make decisions regarding security.

We search for the optimal visualization tool to represent the information stored in a database about the hardware and software security components present in the industry system.

1.6 Methodology

For the objectives mentioned in section 1.4, we developed a visualization solution that was evaluated with experts from Siemens. This evaluation was performed through questionnaires to obtain feedback, allowing it to iterate over the solution development. The tool was implemented to ensure the validity and reliability of this study.

We performed a literature survey to analyze existing methods and tools to visualize security-related components, systems, and network attributes. We define a set of applicability criteria and use it to rate the methods and tools surveyfed. Further on in the course of the thesis, we will be using Siemens's internal use cases to fine-tune the prototype tool to specific industrial setups and requirements [4].

1.7 Outline

The present document is written into four chapters which contains:

- Chapter 2 explains the necessary concepts and terms to understand the present work that describes some previous work on the area and analyzes the visualization tools with the criteria defined to represent security.
- Chapter 3 describes the approaches for the different use cases, each with a distinct objective. It details the use case, the mock-ups created with an explanation for each present element, and the prototype developed as a proof of concept to visualize the data.
- Chapter 4 presents the methodology used to evaluate the solution created using a questionnaire and Hevner guidelines [5]. It describes the threats to the validity of the study. In the end, the results and improvements from evaluation results are analyzed and discussed.
- Chapter 5 concludes the present work by showing the contributions made to the research area, the difficulties that emerged during the execution to accomplish the research questions, and recommendations for future work.

Chapter Two

State of the Art

Contents

2.1 Overview

This chapter gives a comprehensive description of the necessary concepts to understand the present work and a detailed analysis of relevant work already developed in this area. It explains the methodology plan used to filter and analyze the research papers found in this area. We cover some of the industrial control system concepts briefly. Section 2.4 explains the security standards used in this work and detailed the security standard, and section 2.5 contains how security can be managed in an industrial control system and the security qualities that are more relevant. After, it presents some uses cases on security and security visualization. It discusses the tools and techniques that can be appropriate for this study and analyzes them. This chapter concludes with a general discussion of the works studied.

2.2 Methodology Approach in the Survey for the Research Papers

The keywords used to search for were: "Security"AND "Visualization"AND "Cybersecurity", "Data Visualization"AND "Information Visualization","Security Standards,""IEC-62443-2-4", "IEC-62443-3-3", "Security Requirements"AND "Security Attributes", "Industrial Control Systems", "Industrial Security", "SCADA Management", "Grafana vs Kibana", "Grafana"AND "Kibana", "Neo4j", "Dashboard in Industrial Control System". The research papers were evaluated to prevent the reading of non-appropriate content on the *SCImago Journal Rank*[1]. We considered the rating of the research papers and eliminate those whose quotation was in Q3 and Q4, some exceptions were made concerning the rating of the research papers, as their content was of great relevance.

The filters used to select the research papers:

- Inclusion filters - Read the abstract to see if the research paper was within the context, introduction, and conclusion and understand if the content was appropriate and year superior or equal to 2007.
- Exclusion filters - Read the abstract to see if the research paper was within the context, introduction, and conclusion and understand if the content was appropriate and year inferior to 2007.

Some exceptions were made concerning the year of the research papers, as their content was of great relevance. This table 2.1 summarizes the number of research papers found and read, and the selected one, for the state of the art.

Table 2.1: Research Papers Summary

Total Research Papers	49
Research Papers Excluded	16
Research Papers Included	33

[1] https://www.scimagojr.com/

2.3 Industrial Control Systems

An Industrial Control System (ICS) is a combination of various systems to describe a set of control systems and associated instruments, including the devices, systems, networks, and controls used to operate an automated industrial process. They provide automatic or partially automatic control of the equipment in manufacturing chemical plants, electric utilities, distribution and transportation systems and many other industries [6].

These systems are often composed by:

- Intelligent devices;
- Control systems;
- Manufacturing operations systems;
- Business logistics systems.

These systems are often present in industrial sectors and critical infrastructures that make synergies between systems and process to ensure the production of raw materials or products. The part of the system primarily concerned with creating the output is referred to as the process. The control part of the system includes the specification of the desired output or performance [6].

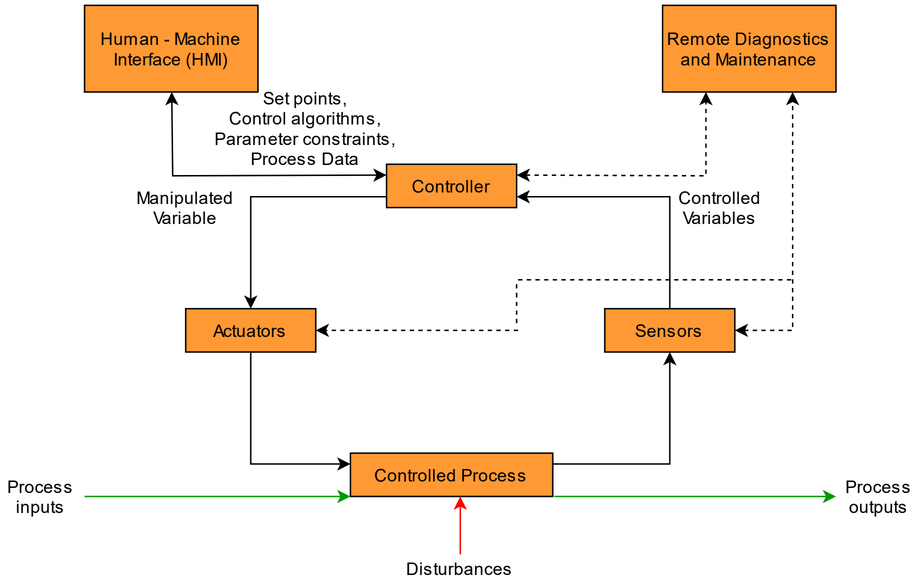

Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Controlled Process
Process inputs
Process outputs
Disturbances

Figure 2.1: Example of an Industrial Control System, Source: [6]

Figure 2.1 represents the mechanism of the essential operation of an ICS. The ICS is composed of various control loops, necessary to adjust the output with a desirable result automatically, and human interfaces to monitor and configure setpoints, adjust algorithms and establish parameters in the controller, and display the corresponding information. All these remote diagnostics and maintenance tools with network protocols based on network architectures are essential to prevent internal problems and attacks. A control loop uses Sensors, Actuators, and Controllers to manage a controlled process [6].

2.4 Security Standards

2.4.1 Security Standards ISA/IEC 62443 SERIES

The International Society for Automation (ISA) is a global nonprofit association focused on the design, development, production, and application of instruments and systems that sense, measure, and control industrial processes and manufacturing processes. ISA is known for developing security standards that match the America National Standard Institute (ANSI) requirements, through the accreditation of many security standards by ANSI [7].

International Electrotechnical Commission (IEC) is a not-for-profit, quasi-governmental organization. The members are National Committees. They appoint experts and delegates from industry, government bodies, associations, and academia to participate in the IEC's technical and conformity assessment work. The IEC is the leading global organization that publishes consensus-based International Standards. It manages conformity assessment systems for electrical and electronic products, systems, and services, collectively known as electrotechnology [7].

ISA is leading an international program called the ISA99, which focuses on developing a set of cybersecurity standards for Industrial Automation and Control Systems (IACS) and critical infrastructures that are being integrated as IEC-62443 series. This initiative can be applied to all key industry sectors and critical infrastructures because a simple system vulnerability can compromise and destroy several industries.

These standards provide a flexible framework to address and mitigate current and unforeseen security vulnerabilities in IACS. From the input and knowledge of security experts from ISA, the committee develops standards that are implemented in the industry's sectors and critical infrastructures.

The ISA99 committee essence, as mentioned before, is to develop and establish standards, recommend good practices, technical reports, and information that will define procedures for implementing security performance electronically [7].

Gilsinn et al. [7] states that collectively all this information is being delivered as the IEC-62443 series, which gives orientation to all users of this standard series. The main scope of ISA99 involves industrial automation and control systems whose compromise could provoke each or all of the following situations:

- Endangerment of public or employee safety;
- Damage to the environment;
- Loss of public confidence;
- Violation of regulatory requirements;
- Loss of proprietary or confidential information;
- Economic loss;
- Impact on national security.

The cybersecurity concept of IACS is applied by ISA99 as comprehensively as possible, e.g., facilities, building plants, industrial systems.

Industrial control and automation systems are included but not limited to:

- Hardware and software systems such as Distributed Control System (DCS), Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition System (SCADA), networked electronic sensing and monitoring and diagnostic systems;
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

In figure 2.2, describes the status of the different work outcomes in the ISA/IEC-62443 series of IACS standards and technical reports [8]. Figure 2.2 displays the framework IEC-62443. We can see that the IEC-62443 scope is organized into four categories, where each one is related to distinct purposes and responsibilities of stakeholders of the IACS.

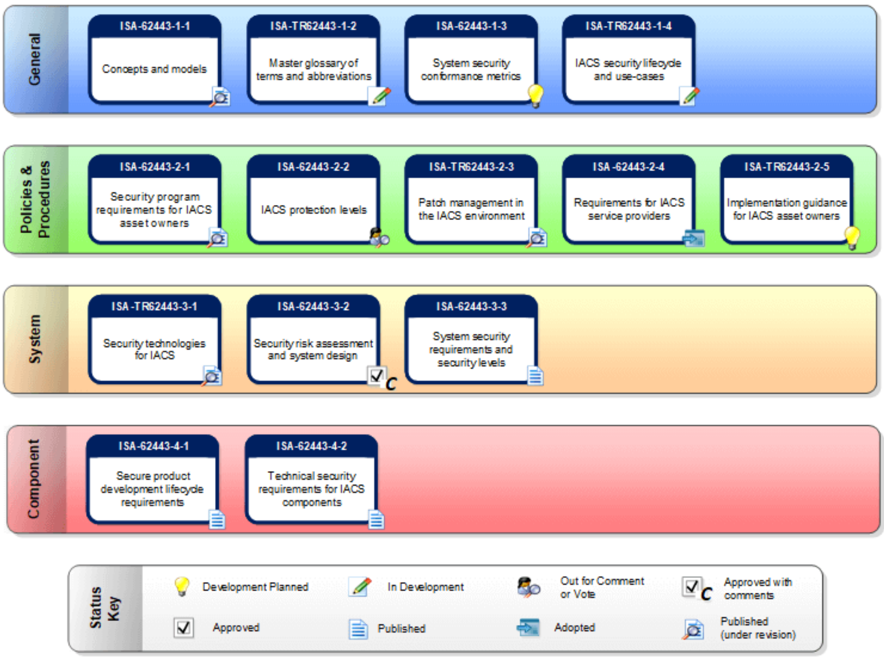

General
ISA-62443-1-1
Concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS protection levels
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment and system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Secure product development lifecycle requirements
ISA-62443-4-2
Technical security requirements for IACS components
Status Key
Development Planned
In Development
Out for Comment or Vote
Approved with comments
Approved
Published
Adopted
Published (under revision)

Figure 2.2: Framework IEC-62443 Series Standards and Thecnical Reports, Source: [8]

These categories are:

- **General Concepts** - Defines and explains the basic terminologies, concepts, and abbreviations used in the series;
- **Policies & Procedures** - Describes the policies and procedures that are required and handled to implement a cybersecurity management system;
- **System** - Describes the security requirements for a system in an IACS environment;
- **Component** - Describes the security requirement of a component in an IACS environment.

The IEC-62443 standard defines three different groups:

1. The Product Supplier;
2. The System Integrator;
3. The Asset Owner.

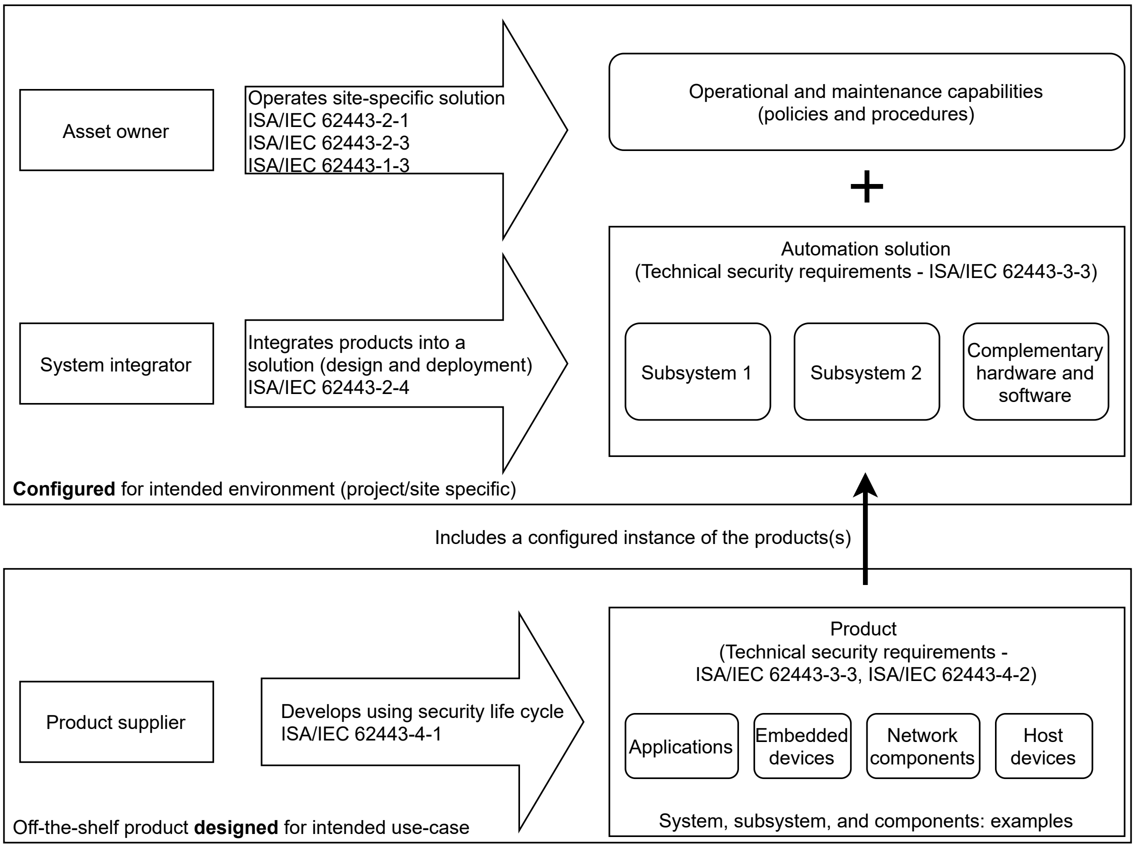

Asset owner
Operates site-specific solution
ISA/IEC 62443-2-1
ISA/IEC 62443-2-3
ISA/IEC 62443-1-3
Operational and maintenance capabilities
(policies and procedures)
+
System integrator
Integrates products into a solution (design and deployment)
ISA/IEC 62443-2-4
Automation solution
(Technical security requirements - ISA/IEC 62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software
Configured for intended environment (project/site specific)
Includes a configured instance of the products(s)
Product supplier
Develops using security life cycle
ISA/IEC 62443-4-1
Product
(Technical security requirements -
ISA/IEC 62443-3-3, ISA/IEC 62443-4-2)
Applications
Embedded devices
Network components
Host devices
System, subsystem, and components: examples
Off-the-shelf product designed for intended use-case

Figure 2.3: Scope of IACS Product Life Cycle, Source: www.isa.org/intech/20160602/

Figure 2.3 represents the process automation of an IACS that identifies the three groups. The Product Supplier, which is the Original Equipment Manufacturer (OEM) that develops individual pieces of equipment or systems/subsystems services that grouped work [9]. The second group is the System Integrator. These are responsible for taking the individual components or systems/subsystems from the product supplier, bringing together those components and subsystems into an automation solution. The standard IEC-62443-2-4 and the IEC-62443-3-3 (we will discuss both in the following sections) are included in the System Integrator [9]. The last group is the Asset Owner. It is responsible for the operation of the IACS (and includes the IEC-62443-2-4) [9].

In the next subsection 2.4.2 and 2.4.3, we will focus on the Policies & Procedures and System categories with the respective IEC references.

2.4.2 The IEC-62443-2-4

This portion of the IEC-62443 series meets the requirements for the provider's security of integration and maintenance services for the IACS [9].

There are two main types of service providers:

- The integration of service providers;
- The maintenance service providers.

IEC-62443-2-4 standard intends that both have the capabilities to understand the details of the equipment and the reference models delivered by the equipment suppliers to provide the proper security.

The OEM is a general term representing a web of relationships among IT hardware vendors, hardware component makers, software vendors, and channel partners such as resellers and distributors. These also tend to include internal service providers organizations. This standard can be applied to them, for example, to help with the reference models or architectures used to support the asset owner to use the equipment. Many OEM's have internal sections to provide integration or maintenance services for their equipment.

The standard contains maturity levels, which is how well-defined processes are and how repeatable it is to achieve that security. There are four maturity levels specified:

- **Initial or "Ad-hoc"** - Service provider's performs the service but does not have a full formal written procedure or policies for support, and when a capability is needed, it has to be done on the fly. It does not mean that they do not provide excellent service or the work result is incorrect;
- **Managed** - There are written policies and procedures, but the key element is that they are trained with specific competency requirements;
- **Defined (practiced)** - All the aspects from maturity level two have been implemented. Still, at this level, there is documentation where you can show that you have gone through and followed this for a specific project;
- **Improving** - A continuous improving-based approach is used to update the policies and procedures based on specific metrics, e.g., feedback is given.

The requirement structure of the standard has the following hierarchy:

- **Functional Area** - There are twelve different functional areas known as the security program:
  1. Solution Staffing (intent to the service provider);
  2. Assurance;
  3. Architecture;
  4. Wireless;
  5. Security Instrumented Systems;
  6. Configuration Management;
  7. Remote Access;
  8. Event Management;
  9. Account Management;
  10. Malware Protection;
  11. Patch management (intent to the service provider);
  12. Backup/restore (intent to the service provider).
- **Topic** - Forty different issues that can apply to different functional areas;
- **Sub-Topic** - Under each issue you have the last hierarchy.

In table 2.2, it is easy to explain each requirement for the standard including the hierarchy.

Table 2.2: Example Requirement from 62443-2-4

Req ID	BR/RE	Functional Area	Topic	Subtopic	Doc?	Requirement Description	Rationale
SP.03.01	BR	Architecture	Risk Assessment	Perform	No	The service provider shall have the capability to conduct a security risk assessment of the Automation Solution or contribute to (participate in) a security risk assessment conducted by the asset owner or its agent. NOTE 1:The asset owner may additionally require the service provider to documents its assessment. The "Doc?"column is set to "No"because this is a requirement to have the capability to perform the assessment and not a requirement to provide documentation.	The capabilities specified by this BR and its REs are used to ensure that the service the provider is capable of identifying and analyzing risks to support the identification and remediation of security risks to the Automation Solution. Having this capability means that the service provider has an identifiable process or performing or contributing to a risk assessment. In some cases, the asset owner will require the service provider to conduct the assessment, while in other cases, to take an active role in an assessment conducted by the asset owner or by a third party under the direction of the asset owner.

The first column represents the “Requirement Identification”. It specifies which security program element is described. In this case, the “SP.03” means we are facing the third functional area which is “Architecture”. The next “.01” from the requirement identification specifies the topic, in this example, it is “Risk Assessment”. The next column, “BR/RE”, defines that we are facing an basic requirement, “BR” means a basic requirement and “RE” means requirement enchantment. It is the initial condition that has to match the standard or a requirement enhancement and is meant to describe the requirements or modify to make them more applicable to a specific situation. The topic is risk assessment, and the sub-topic is “Performance”. It basically means the service provider has the capability to perform the risk assessment.

The next column, “Doc?”, describes if there is specific documentation that needs to be provided for this requirement. In this case, there is no documentation required. “Requirement Description” puts together all the different pieces and describes them. Summarizing the service provider for an automation solution needs to conduct a cyber risk assessment on that portion. If the asset owner chooses to complete that risk assessment, it also needs to provide inputs.

The last column “Rationale” gives a more in-depth description of the requirement. It provides additional information that can help understand the need and match the standard’s intention, here we show an example of the Architecture functional area.

This standard’s main objective is to define specific requirement subsets or profiles to focus on meeting those parts of this standard. It gives more flexibility to identify what most parts of the standard are. The cause is that not all requirements apply to service providers, and asset owners request service providers to perform only a subset of the required capabilities defined on a document.

2.4.3 The IEC 62443-3-3

This portion of the IEC-62443 series meets the system's security requirements and the security levels that define the security assurance of the IACS components.

The audience's target is system integrators, product suppliers, and service providers to evaluate whether their products and services can afford the functional security capability to meet the asset owner's target at the security level requirements [9]. System integrators are responsible assembling the different components of the overall system. Product suppliers and service providers need to understand how to fit those components on the whole system and how they perform on the overall security achievement. The asset owner understands what method is in place in the system integrator to demonstrate how it meets the security requirements. Security levels are defined by the type of threat agents systems were designed to protect against [10].

Levels of security, stated by Paper et al. [10] on this standard are:

- **SL1. Staff (Mistake)** - The intent is to design the system to be robust. It cannot be susceptible to a cybersecurity incident through unintentional internal actions, so only the necessary workers in the organization can access specific equipment. Different roles and responsibilities are designated to avoid mistakes;
- **SL2. Low-Level Hacker (Simple)** - Protection against simple attack with a low motivation, e.g., phishing campaign, or someone with considerable skills, such as a hacker, who can deploy malware. For that, additional security features will be present in the system;
- **SL3. Hacker, Terrorist-Sophisticated (Attack)** - It is a more sophisticated single attack made by a hacker or terrorist groups, who have a higher level of resources and motivation. The target can be a specific individual or organization;
- **SL4. Nation-State-Sophisticated (Campaign)** - The most sophisticated attack with the highest level of resources and motivation, e.g., extended campaign attack.

So with these security levels, we can understand the amount of time and difficulty to overcome those security features. The most rigorous set of requirements are for security level four.

Table 2.3 summarizes the levels of security and the type of possible attacks that can occur, along with the underneath motivation and resources:

Table 2.3: Levels of Security

Security Level	Skills	Motivation	Means	Resources
SL1-Staf	No Attack Skills	Mistakes	Non-intentional	Individual
SL2. Low-Level Hacker	Generic	Low	Simple	Low (Isolated Individuals)
SL3. Hacker, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Groups)
SL4. Nation-State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary Teams)

We will describe the types of security levels:

- **Security Level Target (SL-T)** - Wanted security level for a distinct zone or conduit during risk assessment (the risk assessment is present in another IEC security standard);
- **Security Level Capability (SL-C)** - Defines what features and requirements enhancements should demonstrate the capability to meet a determined level of security. Some specific zones and conduits have been evaluated and formed to be capable of providing the requisite protection;
- **Security Level Achieved (SL-A)** - Based on the performance metrics, we can identify the overall security level achieved for the system.

We will focus on the security level capability since standard 3-3 provides more guidance concerning this attribute.

The requirement structure is a hierarchy composed of three distinct parts:

- **Foundation Requirements (FRs)** - They are seven Foundation Requirements defined in the general section of the IEC standard. The 3-3 adds additional system requirements and requirements enhancements to indicate what is necessary to achieve a higher security level. These foundation requirements are:
    1. **Identification and Authentication Control** - Approaching lease privilege to ensure that specific users can only access particular devices;
    2. **Use Control** - Ensuring the communication between devices and distinct functions is executable on different machines;
    3. **System Integrity** - Ensuring the configuration of devices is maintained;
    4. **Data Confidentiality** - Specific data is invisible to those who are not supposed to have access;
    5. **Restricted Data Flow** - Learning the connection between devices within the system and subsystems;
    6. **Timely Response to Events** - Understanding the right timing to prevent events that can mitigate actions or cover reactions;
    7. **Resource Availability** - Having the resources available so as not to break the process line.
- **System Requirements (SRs)** - Identifying a functionality that is demanded for the system in order to meet the requirements;
- **Requirements Enhancements (REs)** - Changes or upgrades that increase capabilities beyond the original requirements and allow for performance scalability.

As in the previous subsection, 2.4.2, we also present an example for standard 3-3 in table 2.4.

Table 2.4: Example Requirement from 62443-3-3

SRs and REs	SL1	SL2	SL3	SL4
FR 5 - Restricted data flow (FDF)				
SR 5.1- Network Segmentation				
RE (1) Physical network segmentation				
RE (2) Independence from noncontrol system networks				
RE (3) Logical and physical isolation of critical networks				
SR 5.2 - Zone boundary protection				
RE (1) Deny by default, allow by exception				
RE (2) Island mode				
RE (3) Fail close				
SR 5.3 - General-purpose person-to-person communication restrictions				
RE (1) Prohibit all general-purpose person-to-person communication				
SR 5.4 - Application partitioning				

By looking at table 2.4, we can see that the specific system requirement present is the “Restricted data flow (FDF)”. In this case, four system requirements are represented “SR5.1”, “SR5.2”, “SR5.3” and “SR5.4”, and each one contains a specific number of requirements enhancements that constitute the additional step to be taken in order to achieve a higher security level.

“SR5.1” introduces the concept of network separation. “RE (1)” requires physical separation of the network (e.g., by a router or firewall, or physically separate Ethernet networks). “RE (2)” increases this by making the control network independent of any external services (so you can disconnect, and the automation will still control the process). “RE (3)” further increases it by additional separation of critical parts like security controllers. “SR 5.2” protects, monitors, and controls communications at the external boundary of the information to prevent and identify malicious and unauthorized communication. Protection can also be obtained resorting to gateways, routers, firewalls, guards, or encrypted tunnels. “RE (1)” has the information system managed into interfaces that denies network communications traffic by default and enables network communications to traffic by exception (i.e., deny all, permit by exception). “SR 5.3” control system provides the capability to restrict general-purpose person-to-person messages from being received from users or external systems to the control system. These can include e-mails, social media or other message systems that authorize any executable file transmission. “SR 5.4” is the partitioning application used to describe the process of developing applications that distribute the application logic with two or more devices in a network.

2.4.3.1 Security Standard Goals

IEC 2-4 and 3-3 are very closely related. The former describes the requirements for policies and procedures, and the later outlines the system’s requirements. Therefore, when applying this standard, there are vital points that we should consider:

- Providing a method to identify and evaluate the robustness of the security features provided within a zone;

- Allowing achievement of security of those integrated systems (grouping of devices) so as to be evaluated;
- Use a checklist to verify the automation solution to provide the necessary security level target defined during the risk assessment so as to meet the security level capability.

2.5 Security

Computer security is the ability to defend assets (hardware, data, software, test cases, and other parts) and resources (software and data) and property rights from misalignment and misdirection and it holds processes and policies to resolve and prevent disturbance.

2.5.1 Security Management

SCADA systems are used in ICS for monitoring and controlling a process in industrial infrastructure systems. Studies developed as research and trends on the artificial immune algorithm used in protecting the SCADA systems. Vulnerability evaluation of cybersecurity uses three models attacks and modeling to identify remotely accessible devices that were vulnerable, and vulnerability was a quantifying model. Each one improved the overview of security or created visualization patterns to increase SCADA systems' efforts. For the panorama of security or security management, it can be a win-win situation, which means a significant improvement for both sides [11].

SCADA is divided into three levels of operation, according to Ning et al. [11]:

1. **Application** - Focus on developing SCADA's security mechanism design, deployment, and updating;
2. **General Modelling, Analysing and Solution Seeking** - Features and vulnerabilities of SCADA can be explored in protocols or networks, so new security standards, new policies and architecture can be developed and accepted;
3. **Fundamental Security Issues Applicable** - Aims at the problems which can not be explained based on the current models and research.

2.5.2 Security Qualities

Security aims to guarantee safety against adversities, whether they happen intentionally or not. Information security stipulates that this protection's focus is on information, and it is a critical component, such as systems and hardware, using storage and processing the same information.

Raimundas [12] stated that information security guarantees, within the organization, that data is protected from disclosure to unauthorized users (confidentiality), from inappropriate modifications (integrity) and lack of access when required (availability). The concepts mentioned before are the following:

- **Confidentiality** - Property to withhold information or not to unauthorized individuals, entities, or processes. Also, there is a need to keep information confidential from other third parties that want to have access to it, so that only the right people can have access to it;

- **Integrity** - Prevents inappropriate modification or destruction of the information, ensuring that these acts are performed only by authorized persons, to guarantee the trustworthiness of the information in systems and resources;
- **Availability** - Capacity to access data of a resource and use information to authorized people, assuring it is well-timed and reliable.

The security requirement, in certain circumstances, needs to be present in a system in order to mitigate risks [12]. A requirement defines the levels of security expected in a system in order to prevent an attack, and the related concepts are:

- Security;
- Safety;
- Dependability;
- Privacy.

The scope of these requirements guarantees that all the participants are identified and granted access to authorized information. This way, we can detect intrusions and enable security staff to examine the security mechanism's status and regulation [12].

To obtain good requirements, we should use the following aspects:

- Asking what and not how;
- Being sharp sense and observor;
- Being clear and unambiguous.;
- Being cohesive;
- Assuring testability.

Raimundas [12] stated that some of the main roles that can be represented in security visualization software are:

- User Roles;
- Policies;
- Protocols;
- Firewalls;
- Software with versions;
- Third Party Software's with versions;
- Hardware (internal);
- Devices (external);
- Vulnerabilities.

2.6 Security Visualization

Visualizing is useful when properties of the visualization are essential for an analyst and provide conclusions of a determined area, e.g., in a display containing information about the network traffic. We can conclude that ports and users are overloading the network. The area of cybersecurity visualization focuses mainly on developing solutions and researching.

Still, these focus 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 [13].

Examples of current cybersecurity visualization solutions and issues researched are categorized in [13]:

- Network Analysis;
- Malware & Threat Analysis;
- Situational Awareness;
- Vulnerability Visualization.

However, there are other areas besides the mentioned above that are being explored. We will illustrate these concepts and describe them briefly. They can help explain how we can use visualization to aid with some examples and cases already studied.

2.6.1 Network Analysis

The function of the Network Analysis tool is to detect potential intrusions for security, forensics and irregularity by mapping the physical network [13].

We can observe the research by Coudriau et al. [14] focus was monitoring data in the Darknet to recognize malicious activities based on traffic patterns, including triggering warnings. At the end of this case study, the proposed methodology analyzes network packages that are malicious so as to scan the activity and prevent an attack.

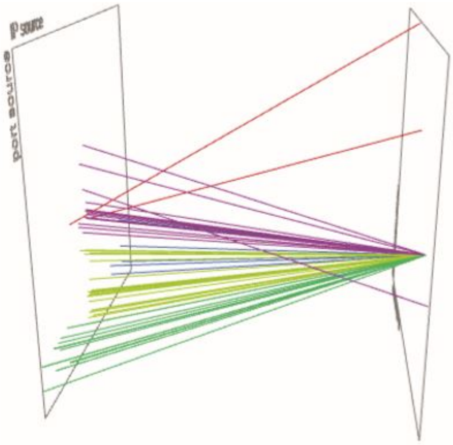


Figure 2.4: Example of visualisation of a DDoS using mapper, Source: [14]

In figure 2.4, we can see how Coudriau et al. [14] use the 3D effect to represent IP and PORT sources that suffer a denial of service attack, which gives a perception of how we can use 3D visualization to represent sources.

Another case study by Angelini et al. [15] is related to visual analytical tool relying on attack graphs. PERCIVAL, a proactive tool, was developed to help security workers manage the security of a system. It highlights possible attack vectors based on the state of the network and using attack-graphs.

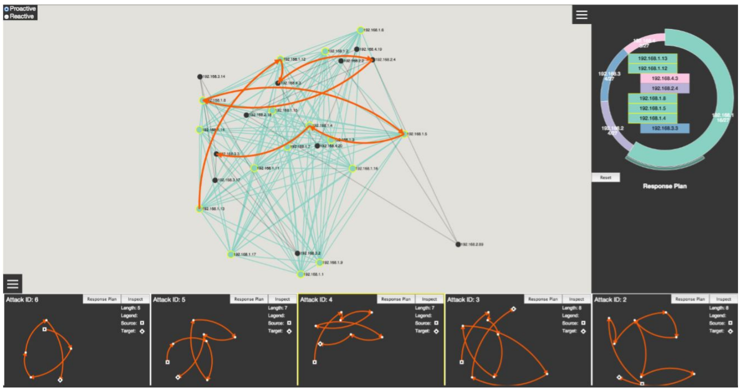
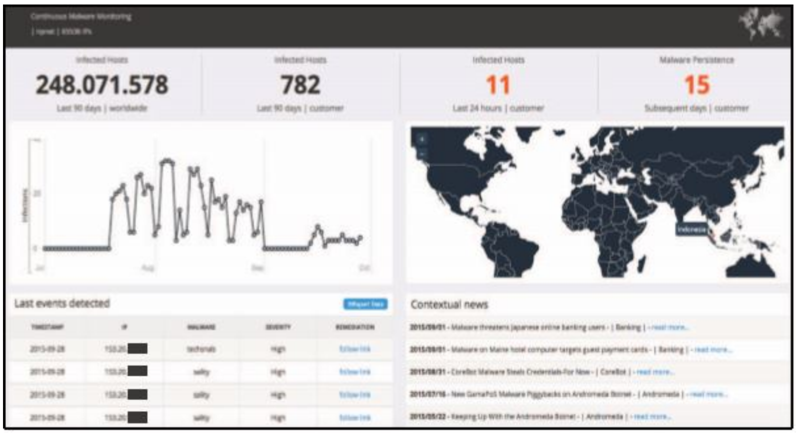


Figure 2.5: Example of the PERCIVAL system, Source: [15]

In figure 2.5, Angelini et al. [15] showed a complex network with all the connections between them with blue lines, and we can see the possible attack lines that are highlighted. This visualization is useful for showing patterns of attacks and understanding how we can represent many elements in a complex network with the connections.

2.6.2 Malware & Threat Analysis

Malware and Threat Analysis tools can detect and eliminate malware and threats communications affecting organizations. For this subsection 2.6.2, we present two developed case studies. The first one is OwlSight, which is a security platform for big data that, in real-time, detecting cyber attacks using maps and graphs or analyzing threats with machine learning to find patterns for unusual behavior [16].



Last events detected

TIMESTAMP	IP	MALWARE	SEVERITY	REMEDIATION
2015-09-28	153.20.[redacted]	techsnab	High	follow link
2015-09-28	153.20.[redacted]	sality	High	follow link
2015-09-28	153.20.[redacted]	sality	High	follow link
2015-09-28	153.20.[redacted]	sality	High	follow link

Contextual news

2015/09/01 - Malware threatens Japanese online banking users - | Banking | - read more...

2015/09/01 - Malware on Maine hotel computer targets guest payment cards - | Banking | - read more...

2015/08/31 - CoreBot Malware Steals Credentials For Now - | CoreBot | - read more...

2015/07/16 - New GamaPoS Malware Piggybacks on Andromeda Botnet - | Andromeda | - read more...

2015/05/22 - Keeping Up With the Andromeda Botnet - | Andromeda | - read more...

Figure 2.6: Example of the OwlSight system, Source: [16]

In figure 2.6, it is a dashboard visualization that has a worldwide map. It contains real-time information on where a possible attack can happen, and it has graphs and feeds that aggregate information to detect attacks in real-time.

The second study, DAVAST [17], is a system composed by two subsystems that control and breakdown, providing different design views to detect and further examine potentially malicious behavior based on patterns.

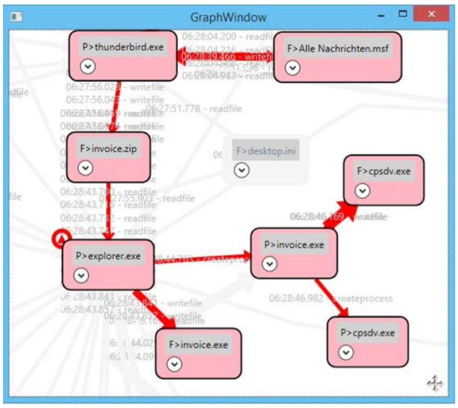


Figure 2.7: Example of the DAVAST system, Source: [17]

Figure 2.7 shows more information on this example, inside the nodes with information that can represent an attack.

2.6.3 Situational Awareness

Situational Awareness has tools that give a high-level abstract view of the systems providing benefits to experts and non-experts workers [13]. We present a tool used for situational awareness called ePSA, which engages with the network data flow analysis to learn the cybersecurity concerns by mapping data for beginner users, in order to improve their situational awareness by applying a timeline [18].

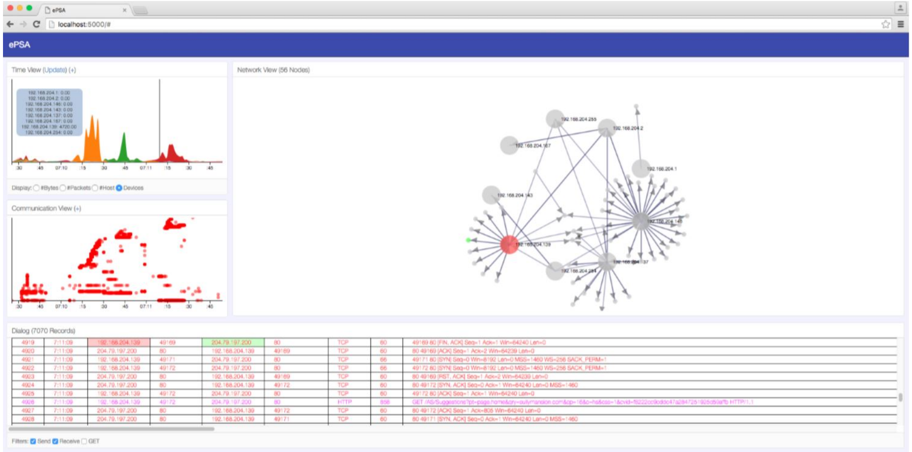


Figure 2.8: Example of the ePSA system, Source: [18]

In figure 2.8, we can see a dashboard with crucial information for situational awareness. we also have graphs and a node chart and a table with information.

There is a significant gap within solutions and research to approach problems of humans as analytic cybersecurity. As a result, it leads to low adoption rates of the visualizations solutions [13].

Another tool used, SEQUESTOR visualization (SEQViz), builds shared situational awareness and investigative skills that cybersecurity analysts must have so as to instruct with flexible models, adaptive quarantining technologies [19].

Finally, we have figure 2.9, and we can see that graphs represent the activity of the network to analyze the data flux.

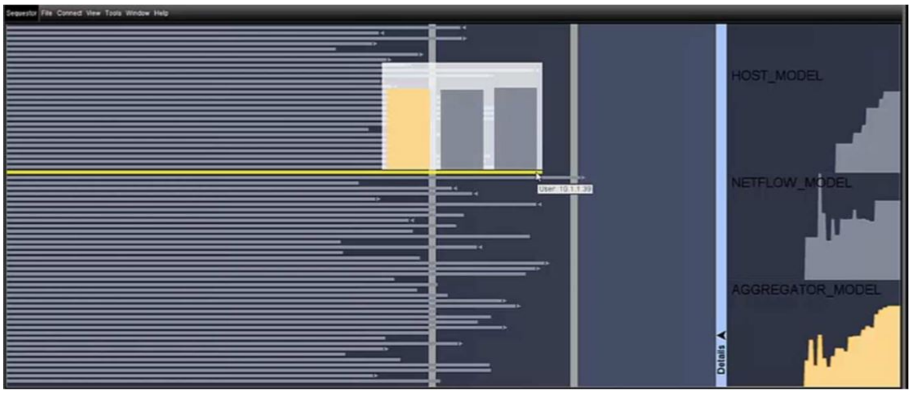


Figure 2.9: Example of the SEQViz system, Source: [19]

2.6.4 Vulnerability Visualization

This is another area that has been explored with the constant evolution of software, interfaces, hardware, services, and more technological part, and it is vulnerability visualization. Vulnerability is a weakness that attackers can exploit to perform unauthorized actions within a computer system, and it is a critical component in a system [20]. Vulnerability can be classified with a Common Vulnerability Scoring System (CVSS)[2], which provides a way to capture its principal characteristics and produce a numerical score reflecting its severity. CVSS is a published standard used by organizations worldwide, and the Special Interest Group (SIG) mission is to continue to improve it.

To monitor the vulnerability in a system there are software tools available in the market, and others are being developed. Nesus is one of those and it has been constantly development [20]. Now it has more features, but we will focus on the vulnerability scan and the main tasks that the tool is capable to perform:

- Identifying the components with more critical vulnerabilities;
- Finding services with most vulnerabilities inside a network;
- Identifying the exposure to vulnerabilities within groups of machines where those groupings reflect the analyst's mental model of their network;
- Determining the high-value machines that are vulnerable to exploitation;

[2] https://www.first.org/cvss/

- Comparing point-in-time snapshots of the security state of the machines in the network, and understanding the differences between these two points.

In figure 2.10, we can see how they divide the new, fixed, and identified vulnerabilities using a treemap, which is divided in workstations (network zone). At the bottom of the histograms, we can observe (from the left to the right) the number of vulnerabilities by severity and vulnerability type (top holes, top notes, or open port).

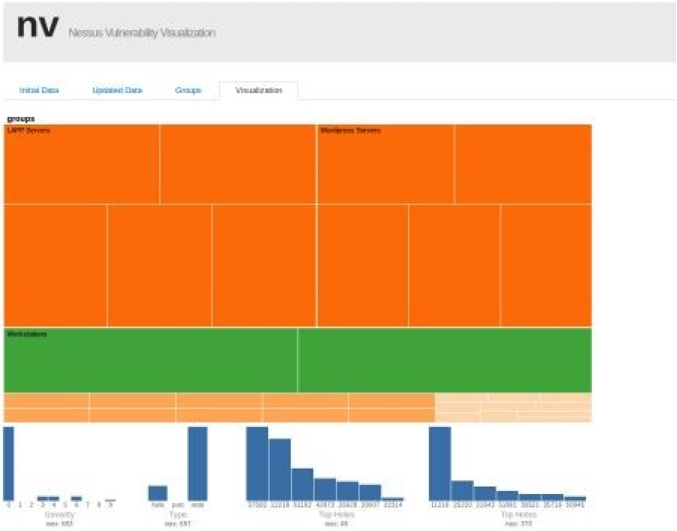


Figure 2.10: Example of results collected by the Nesus tool, Source: [20]

Another software approach for this vulnerability type of visualization is called VULNUS. It is a solution used to analyze the vulnerabilities of computer networks, providing both an overview and details of a large set of vulnerabilities spread across network nodes, combining data from vulnerabilities and network scanners [21].

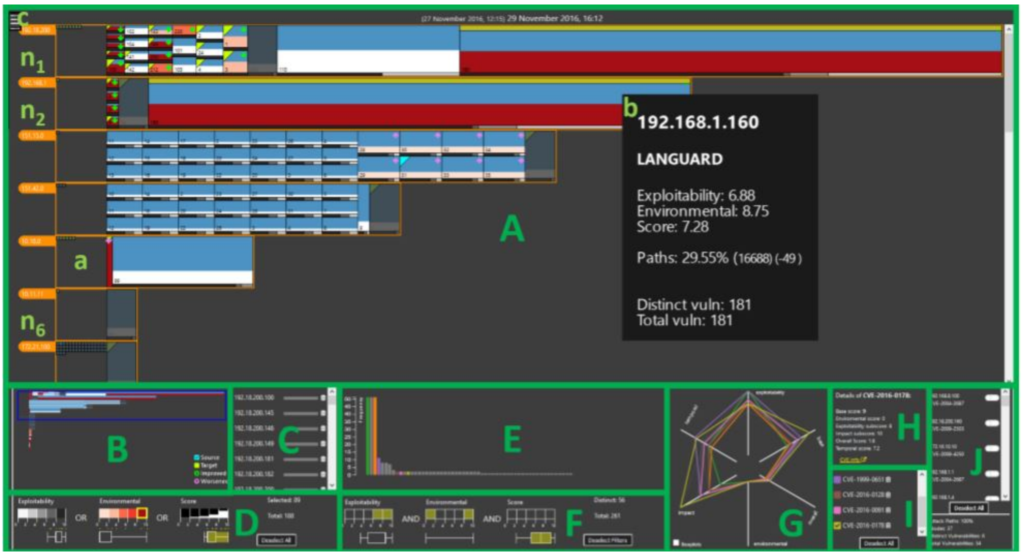


Figure 2.11: Example of the VULNUS tool, Source: [21]

VULNUS has a user-centered design approach and it consists of iterating activities in a certain context of usage, acquiring data, and extracting user and organizational requirements, composing designs and prototypes and carrying out assessment and evaluation until the system meets the needs proposed by the developers [21]. It uses cases and tasks that have been obtained requirements and assessed by users.

In figure 2.11, we are "dealing with a real network (...) Sub-networks are arranged horizontally, using a modified treemap bar chart representation. Each bar represents a sub-network (...), size, and the bar length are proportional to the total number of vulnerabilities of the element (...)" [21]. The dashboard is divided into various parts to represent the information regarding the user's needs of the various elements.

2.7 Visualization Tools

We will approach some tools available in the market to fulfill the purpose of this thesis. In the end, we will analyze how they meet the specific requirements that were derived from the purpose of visualizing information in an IACS context.

2.7.1 2D & 3D Visualization

Good animation can increase the rate of acceptance significantly. With the combination of 2D & 3D visualization capabilities, we can generate useful results with data. For instance, we can imagine a ball representing an object and inside that ball. We can create more items for relative position estimation, orientation and volume of interest tasks.

Significant factors providing display decision and usability were task features, adjustment cues, occlusion and spatial proximity of designs. This was, we present two tools, Gephi and Neo4j, used in these situations.

2.7.1.1 Gephi

Gephi is a free, open-source software, interactive and an exploration solution for graph and network analysis, which allows for real-time information. It supports dynamic and hierarchical graphs.

Users can import, visualize, spatialize, filter, manipulate and export all types of networks. It also cuts edge layout algorithms, which include force-based algorithms and multi-level algorithms, in order to give an efficient experience. The interface is organized in workspaces and each space can be applied to a specific task [22].

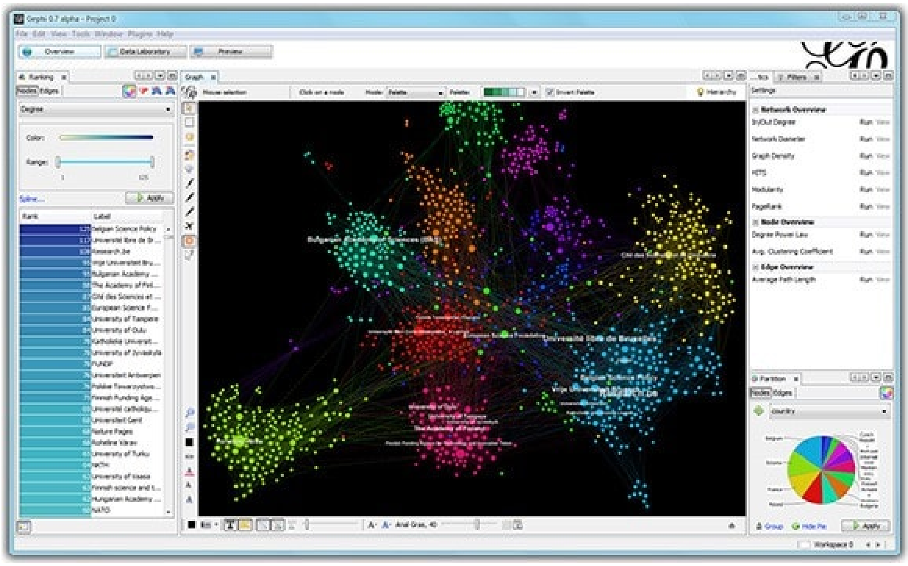


Figure 2.12: Example of the Gephi types of visualization, Source: www.gephi.org

Many types of visualization can be represented in figure 2.13.

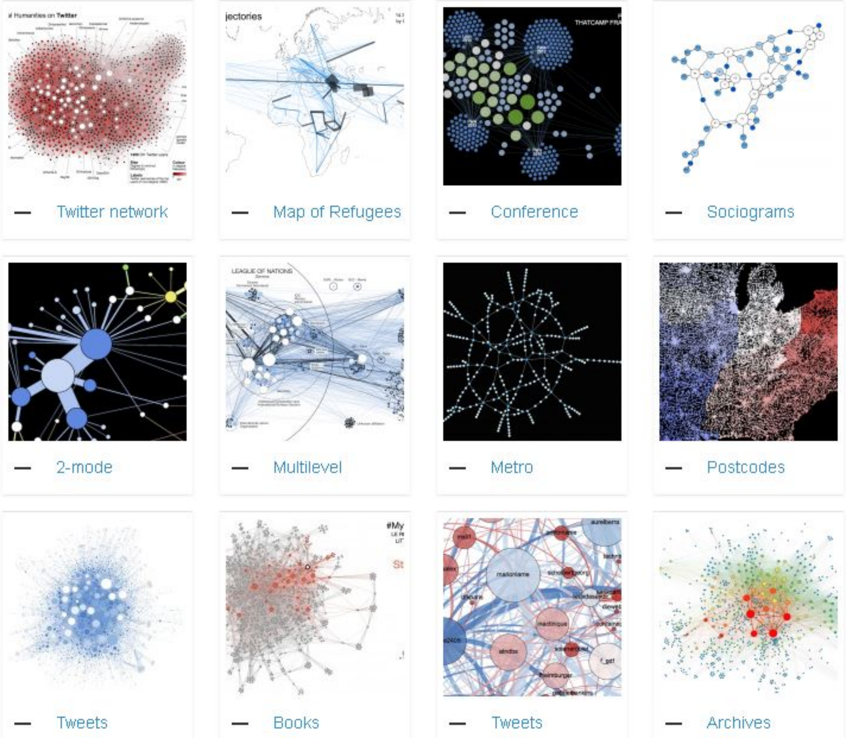


Figure 2.13: Example of the Gephi types of visualization, Source: www.martingrandjean.ch/gephi-introduction/

There are also additional plugins, like for example GeoLayout, NoverlapLayout, and Multimode Networks Transformation, which provides more features to the display.

2.7.1.2 Neo4j

Neo4j is a free, open-source, NoSQL, native graph database that implements in an efficient way a proper graph model to store data precisely as you design it, and we can navigate and traverse the graphs created. Neo4j presents full database characteristics, including ACID (atomicity, consistency, isolation, and durability), which is a set of proprieties of transaction compliance, cluster support,and runtime failover, performing it properly to do graphs for data implementation [23]. In Neo4j, we can classify three architectural category types of graph visualization. It depends on the need of the viewing, and we may establish tools to be implemented as solutions:

- **Embeddable tools with built in Neo4j connections** - Included as a dependency within an application and can easily be configured and styled for your use and Neo4j;
- **Embeddable libraries without direct Neo4j connection** - Libraries allow the capacity to set graph visualization, but without connecting directly to Neo4j;
- **Standalone product tools** - Tools and products that are intended as independent and that can combine to Neo4j and cooperate with data without requiring any code.

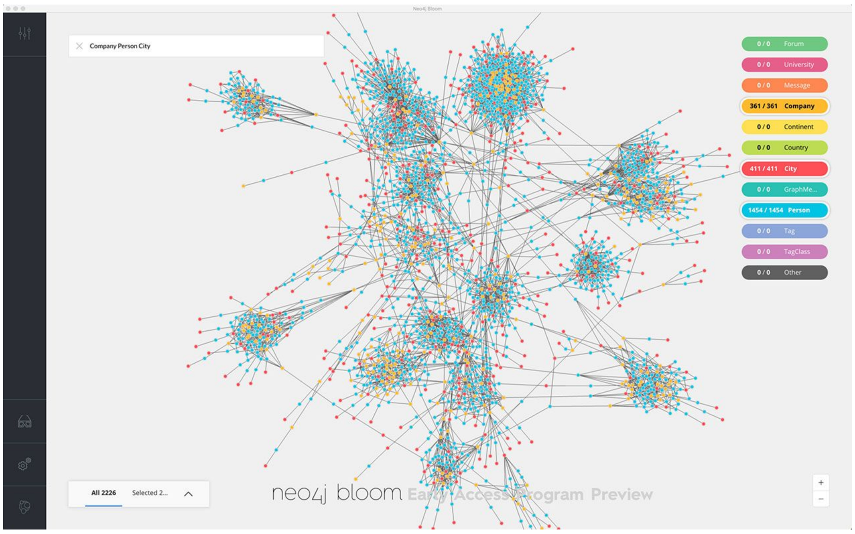


Figure 2.14: Example of Neo4j graph database, Source: www.neo4j.com

2.7.2 Dashboard

Kibana and Grafana are two popular open-source tools that help users visualize and understand trends within vast amounts of log data. We will give a short introduction to each of the tools and highlight the key differences.

The difference between these next two tools that will be presented and the others already described is the capability to create more visual elements to display data. In subsection 2.7.1, the 2D & 3D visualization tools does not have a broader range of visual elements.

They are more focused on connections between nodes, and the dashboard tools have a more customizable and more visual element to display the data.

2.7.2.1 Grafana

Grafana is an open-source software with interactive visualization and dashboard software on the browser. It provides several widgets, e.g., timelines, tables, text fields for single metrics. It also supports multiple data sources, e.g., Graphite, Elasticsearch, InfluxDB, OpenTSDB, and more than thirty open sources and type of data source.

Grafana dashboards can be easily distributed by a web address and automatically update the changes [24].

Grafana provides a range of features, e.g., selections, zoom, auto-refreshing functions, annotations. Templating is the main advantage, and we can define arrays that can be dynamically filled with specific data and use them in different places to create metrics queries, panel title, and automatic dashboard generation. This feature is useful when some events are presented in graphs [25].

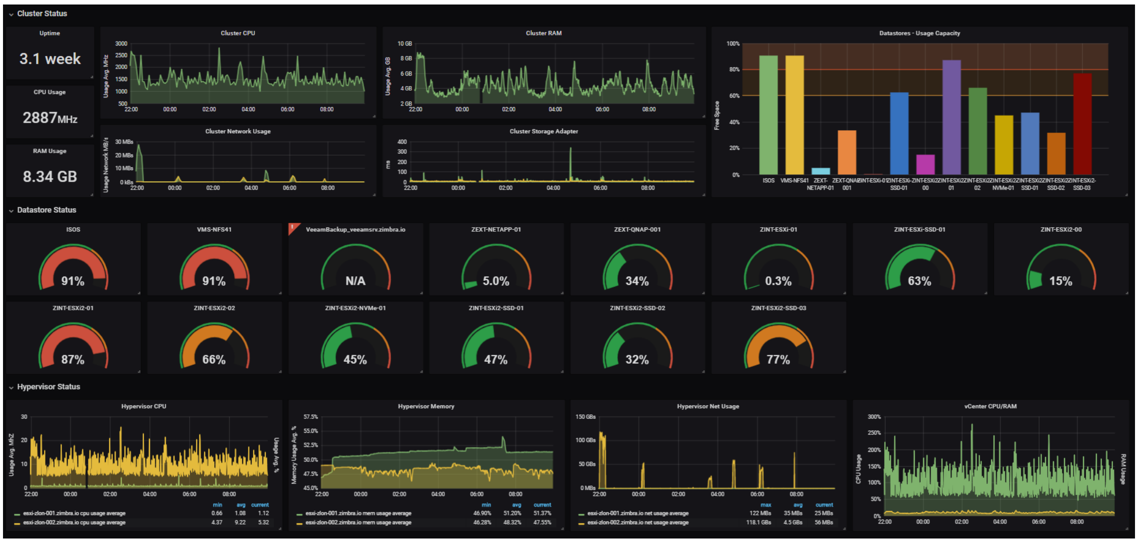


Figure 2.15: Example of Grafana dashboard, Source: www.techblog.commercetools.com

2.7.2.2 Kibana

Kibana is an open-source software for log analysis and provides the users with a tool visualization program so as to build dashboards and a search tool for timeline analytic information and Elasticsearch. Kibana's main feature is data querying and analysis [26].

It helps users analyze a considerable quantity of information based on queries by visualizing various charts, geographical maps, graphs, tables, or other types of visualizations. Also, it allows users to build dashboards and share them in real-time with Elasticsearch [24].

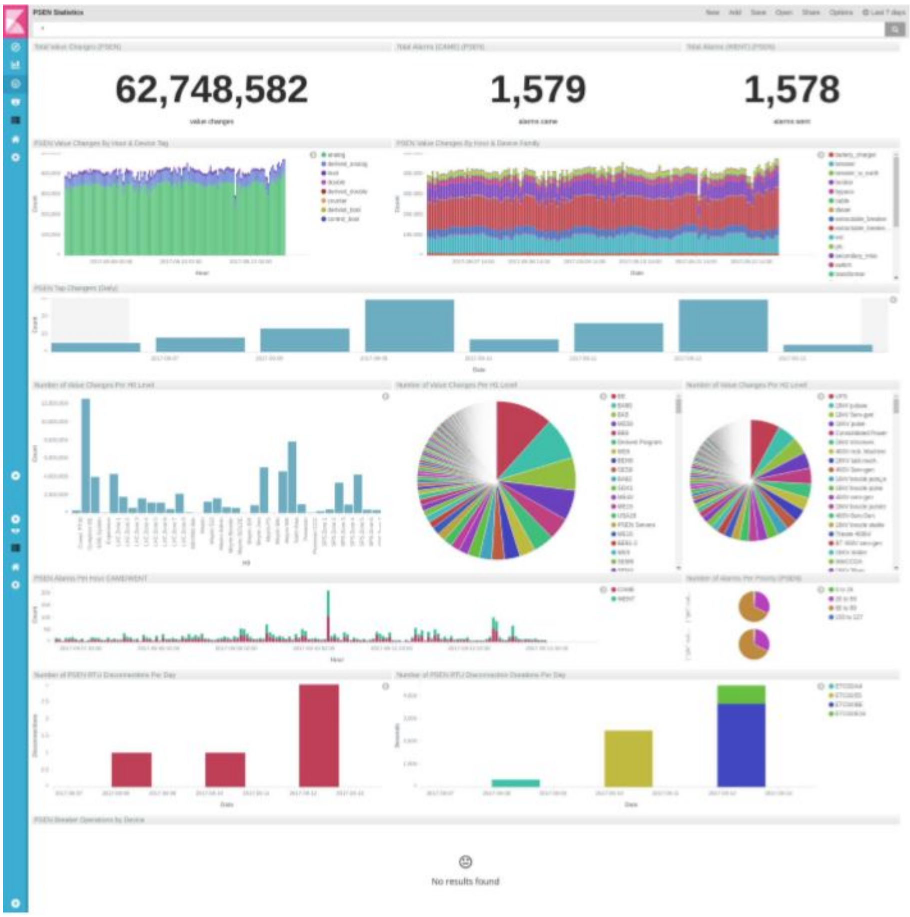


Figure 2.16: Example of Kibana dashboard, Source: [26]

2.7.2.3 Kibana versus Grafana

The research developed by Yong [24] compares the tools mentioned in subsections 2.7.2.1 and 2.7.2.2, stating that both are "visualization and monitoring tools, but they are use to handle different types of data types or user cases."

We will summarize the research on table 2.5:

Table 2.5: Grafana and Kibana Comparison, Source: [24]

Metric	Grafana	Kibana
Dashboards Editing and Visualizations	Versatile, has a greater and wider options*	Versatile but has not a greater and wider options*
Setup, installation and configuration	Easy	Difficult
Data source support	Work well with different data source	Only work well with the Elasticsearch
Querying	More intuitive and it is compatible for different data source	Not intuitive and involve certain learning curve

Note: *both are versatile, able to filter data in real-time, they support various kinds of visualization and allow the user to do editing on the dashboard. However, Grafana has a greater and wider option than Kibana in dashboard customization. In addition, it is easier to use and to make a changes.

2.7.3 Tool Discussion

Holger and Hausi [27] have stated the requirement quality attributes and functional requirements necessary for software visualization tools to build and evaluate tools. The software systems need to meet the requirements defined and that can be changed over time and meet the experts.

The surveys and reviews were based on five steps of Evidence-based software engineering (EBSE) and the methodology implemented. We can conclude that there are seven quality attributes and eight functional requirements for visualization tools, which we will explain briefly, based on the research published.

The quality attributes are:

- **Rendering Scalability** - Interactive systems capable of visualizing data have a rendering speed that should scale with the volume of data to allow direct manipulation of the visualization elements. The software needs to have an attractive performance when loading and rendering because it is essential for the usability of the visualization tool;
- **Information Scalability** - Information is increasing quickly, and having all that information in a system can cause scalability problems. The space and time with complexity are both considered by scalability, and solutions used to resolve this problem are, e.g., automatic layout. The software must provide tools to filter and display selective information;
- **Interoperability** - Capability of the system to communicate transparently with another system. Research records try to answer on how to reach interoperability without stating it as a requirement. Forcing software visualizations stress is crucial because this allows to reuse current functionalities;
- **Customizability** - Capability to change characteristics according to the user's needs, which is something that developers did not predict. Software already enables the customization of their functionalities;
- **Interactivity** - Interactivity is the skill of users to manipulate visualization elements and information to operate them. The interactivity needs to be balanced; otherwise, simple tasks can suffer from a sizeable unnecessary interaction;
- **Usability** - Focused on the evaluation of the user interface, it is a highly popular requirement, although hard to create. The quality of the interface facilitates the use of the software. By using a complex interface it can be harder to use the software;
- **Adoptability** - Divided into technical and non-technical aspects, that can change the use of the tool for a task. The tool is created for a specific problem, and its use cannot solve other issues. This was, a tool should be specialized or versatile to propose a method based on features examination to increase tool adoption.

The functional requirements are:

- **Views** - Diverse views of the software system, with multiple perspectives, integration, synchronization and navigation, can fulfill the needs of different stakeholders and maintain many dimensions of data so as to provide abstraction;
- **Abstraction** - Handle complexity by hiding unnecessary information from the user, enabling to later to execute further complex logic on top of the provided abstraction without understanding or even thinking about all the hidden complexity. Having many levels of abstraction is relevant for the availability of information so users can view the content;
- **Search** - Capability to find specific information by giving the software a query, visualization tools can be limited to these queries. The importance of this functional requirement is to obtain specific information;
- **Filters** - Visualization information filtering is a simple form of querying. This permits us to decrease the volume of data view and to confine our analysis more;
- **Code Proximity** - The user's skill provides secure and fast access to the main source code, underlying source code. Code proximity is a case of a particular abstraction mapping of the code;
- **Automatic Layouts** - An automatic layout algorithm is responsible for the automatic arrangement of visual elements already created by developers with specific rules, node positions and edge paths. It is essential to have automatic layouts to create different patterns and faster deployment of information for stakeholders with different needs. Further stakeholders can perform manual refinement, changing the visual elements;
- **Undo/History** - Users perform interactive manipulation that can change the visualization aspects of information. It is vital to have a history that saves temporary information relative to the software action and an "undo" feature. This mechanism can revert the previous status or fix minor errors made by testing features;
- **Miscellaneous** - Other requirements present on software, the use of colors, place annotations of visual elements, manipulate visual elements, e.g., moving, zooming, delete, edit, and saving.

Based on the study we present and user experience made, we perform an evaluation of set of tools for security visualization. This way, for the quality attributes, we set a score from one (poor quality) to five (excellent quality), being that one has lack of indispensable qualities and five has all the qualities. The user can add more features with ad-dons.

In figure 2.17, we can see that Neo4j has, overall, better quality attributes than Gephi. Although the rendering scalability and information scalability have the same score, the main factor for Neo4j has a better evaluation it is because the adoptability, usability, and interactivity is important for the user.

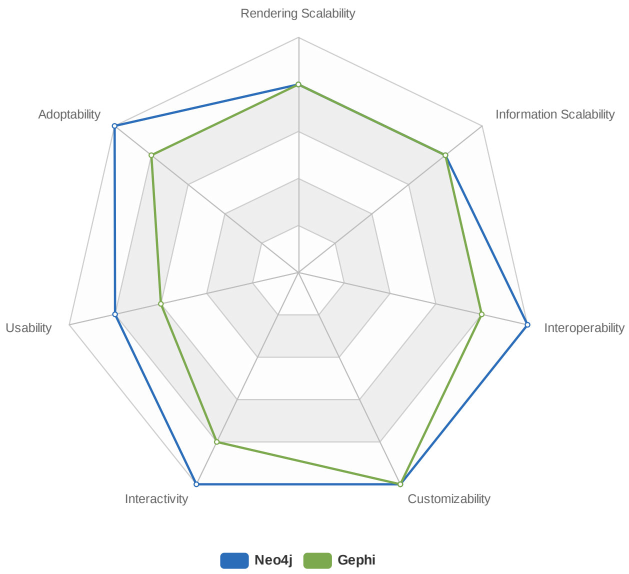


Figure 2.17: Quality Attributes for Neo4j and Gephi

As we can observe in figure 2.18, for the dashboard, Grafana, overall, has a better score than Kibana. Kibana has a greater score only in customization.

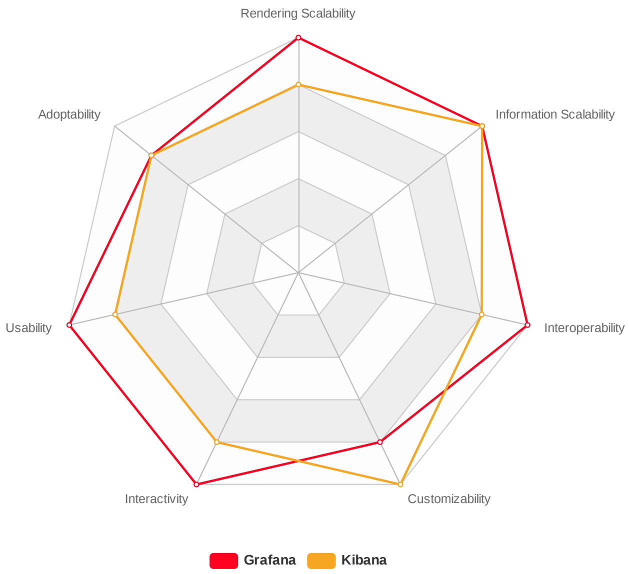


Figure 2.18: Quality Attributes for Grafana and Kibana

The same evaluation is performed for the functional requirements, a score from one (poor functionality) to five (excellent functionality), in which one has no functional requirements to define the necessary system behavior, like for example to create different views for the same data or the lack of search in the data to filter results, and to five has the functional requirements necessary to define the specific system behavior.

Observing figure 2.19, Neo4J has more multiple perspectives to see the data on the nodes than Gephi, which is more limited. Concerning code proximity, in Gephi the user does not have as much contact with the code as Neo4J.

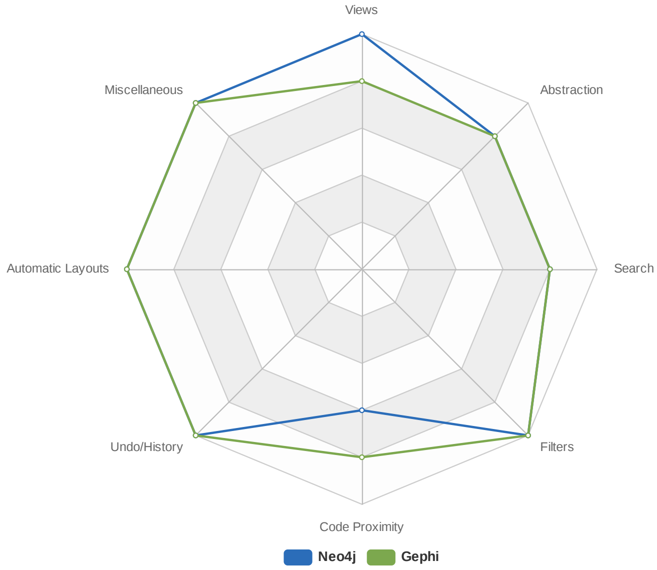


Figure 2.19: Functional Requirements for Neo4j and Gephi

In figure, 2.20, the only difference between Grafana and Kibana is the search. In fact, Kibana seems more direct in creating queries to find the specific information from different data sources in the same dashboard.

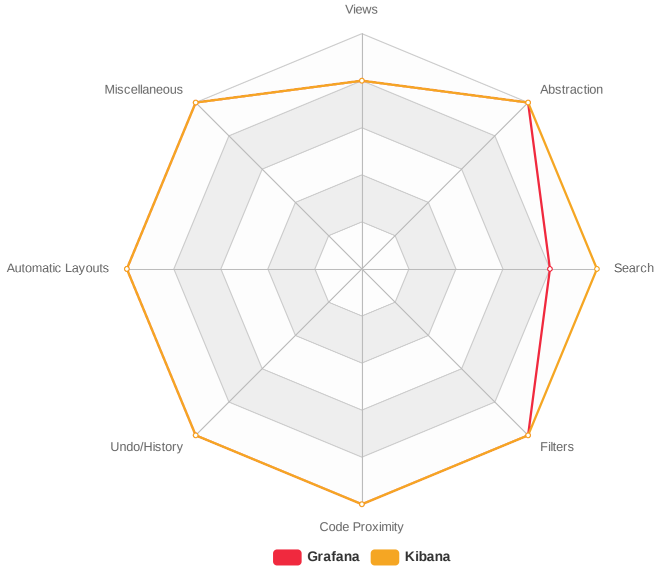


Figure 2.20: Functional Requirements for Grafana and Kibana

Now we present table 2.6, which aggregates the scores presented in the last two tables, the maximum score possible being seventy-five. From table 2.6, we can see that dashboard tools are more effective than 2D & 3D visualization tools. The cause is the possibility of processing data inserted in the tools in different ways and the main process used so as to view data.

Table 2.6: Overall Score

Tools	Overall Score
Neo4j	68
Gephi	64
Grafana	69
Kibana	69

2.8 Visualization Techniques

There are many types of visualization to represent information. One way to express it in an organization is in dashboards in order to describe critical data for decision making.

2.8.1 Visualization Requirements in Software Visualization

The scope of software visualization is to aggregate and simplify the information of a determined area or areas, which can include many components, attributes, and relationships. This need can be fulfilled with visualization elements such as graphs, charts, diagrams, etc. These interactive visualization methods contribute to support the domain expert in earning a more robust knowledge of sophisticated software and its variability [28].

Bougouffa et al. [28] proposed some visualization patterns divided in:

- Domain Experts Requirements:
  - **Requirement 1: Different usage/functionality of a visualization approach** - We should give the appropriate information to experts due to the different purposes of using the results. An expert can have different ideas of using data collected during a project phase, and modifications might occur at different hierarchical levels. It all depends on the desired outcome. Then, we need different visualization patterns that can perform distinct purposes for analysis results by different experts;
  - **Requirement 2: Different granularity levels of information in the visualization** - A granularity level needs to be considered in visualization when modification happens. Experts need to adapt the granularity level to analyze the information in a particular moment. Therefore, visualization can represent a distinct granularity level of the variability classified and thereby acknowledging a more global or close-up perspective to drill-up or drill-down the information. We need different visualizations to explain the variability in granularity levels using appropriate information details.

- Scenarios for the usage of the visualization:
  - **Scenario 1: Documentation of expected variability** - It consists of documentation stored that describes the variability of the results give an insight into the project structure and available variants that are essential for a new software developer and a detailed view of their variability in the variable declaration or on the statement level;
  - **Scenario 2: Software development of a new module variant** - Control software that implements a new variant that the expert needs to overview the existing variability. It would be of interest on a more fine-grained level, and supplementary information is required for a modification that is the most similar to the one that needs to be developed;
  - **Scenario 3: Refactoring of control software** - The software has standard components, which perform specific functions and can be reused in different softwares. Transferring these components requires an overview of these standard features and differences.

2.8.2 Best practices for Dashboard

When creating a dashboard, there are some aspects and practices that we need consider to achieve a useful view of the information [29]:

- **Awareness** - Regarded just with data that can be visualized as activity streams, tabular overviews, or other types of visualizations;
- **Reflection** - Data in themselves are not very useful. The reflection stage directs the users making questions and judging how useful and relevant data are;
- **Sensemaking** - Concerned with users answering the questions identified in the reflection process to create innovative insights;
- **Impact** - The goal is to produce distinct purposes or changes in the behavior of the user considers it beneficial.

Effectively, developing a dashboard with the best practices for dashboard design requires efforts, such as collecting elements, setting goals and designing a data model [29]. A well-designed dashboard design stands out in these areas:

1. **Get to Know Your Audience** - To have impact and success, it is important to research those that will need the information before a meeting and organizing the report to guarantee visuals and level of detail concerning their needs;
2. **Manage Goals** - Structure visualization, perform logical narrative, and drill down into relevant insights. It is critical to establish a clear-cut set of aims, purposes and goals before building your management reports, graphs, charts, and additional visuals;
3. **Choose the Correct Chart Type** - The most powerful data visualization methods. We need to select the right charts taking into consideration a specific project, audience, and purpose;

4. **Use the Advantage of Color Theory** - You should choose the correct color design so as to improve your applications significantly;
5. **Handle Big Data** - You should know the right data to display on the dashboard;
6. **Ordering, Layout and Hierarchy To Prioritize** - It is not recommended to use more than five elements in a dashboard, so users will spend one second per each element;
7. **Use Word Clouds and Network Diagrams** - More comfortable to the eyes to have a panorama of the most common events in a system;
8. **Include Comparisons** - The most pointed of our data visualization methods, but the knowledge and insights need to incorporate as many real comparisons;
9. **Tell Your Tale** - Present the data in a visual setup to communicate an essential purpose. By telling the history, we can engage the audience and make it easy for people to understand and requiring a minimal effort to respond, which will result in long-term growth, development, and progress;
10. **Use Visualization Current Tools** - Use the current tools to make the best possible judgments while collecting your data in the most efficient, effective way. A task-specific, interactive dashboard or tool offers an edible, intuitive, comprehensive, and interactive means of collecting, collating, arranging, and displaying data with ease.

To have a purpose for the view, we need to create them. By designing a model, we decide which subjects we want to aboard and which data we have to collect to satisfy the model. To achieve this, we adopted the Goal-Question-Measurement plus the Strategies approaches, which are based on Goal-Question-Measurement models [30].

1. **The Goal** — Conceptual Level — sets what we need to study and why. The object of study is examined, as well as specific products, processes, and resources, and the reason why something is being studied;
2. **The Questions** — Operational Level — defines what elements of the object of study are appropriate and what features of such parts are used to characterize the goal's assessment or achievement;
3. **The Measures** — Quantitative Level — defines which data need to be gathered to answer the questions in an objective quantitative way.

2.8.3 Color Theory

The role of colors in the dashboard is crucial to make it engaging, easy to use and easy to read. Color theory is a terminology that describes a collection of rules and guidelines regarding the use of color in art and design, and it is developing with the new technologies. The color theory describes color schemes' design, and effectively communicating a design purpose at visual and psychological levels.

Currently, the Modern Color Theory is based on Isaac Newton's color wheel. It displays three categories of colors:

- Primary colors (red, blue, yellow);

- Secondary colors (created by mixing two primary colors);
- Intermediate or tertiary ones (created by combining primary and secondary colors).

Color temperature is different considering the design, distinguishing between warm, cold, and neutral colors and evoking people's emotional responses. Warm colors are those with yellow and red. Cold colors have a blue, green, or purple tint. Neutral colors include brown, gray, black, and white. Consequently, studying the traits and expectations of target viewers is vital for fine-tuning the actual impact of color use in design and stopping design failure [29].

2.9 State of Art Discussion

We can conclude that all the software tools presented have the same essence: representing information with visualization capability for a specific area. With all the aspects considered, all the tools can handle the requirements and qualities needed to represent security in the visualization dashboard or 2D & 3D visualization.

Kibana has a poorest performance due to of less quality in rendering scalability and interactive qualities. Kibana was the hardest to install and configure. When it is used to represent many visual elements (e.g., graphs, tables, charts), it has a performance penalty, but, overall, it has an excellent capability to represent information.

Gephi is a great tool. It is a more complex tool with a big learning curve, so we need to spend more time to understand his complexity.

Neo4j is a powerful tool to complete many types of tasks with a lot of plugins to supplement the information. The menus software, in the beginning, was a little confusing, but after some research, it was easy to manage.

Grafana is an intuitive tool. However, it needs the variable time to perform the graphs. The menus are organized, and the tested was perform smoothly. Nevertheless, pop-up alerts for errors in queries are also limited, what happens when using Kibana.

Grafana, Gephi and Neo4j were the most accessible tools for the installation process and to feed them with information to create visualization elements.

Concluding, with the evaluation in the subsection 2.7.3, we can recommend that Neo4j for the 2D & 3D visualizations tools.

Grafana or Kibana, are the most acceptable tools to fulfill the goals proposed in the section 1.4.

[This page has been intentionally left blank]

Chapter Three

Proposed Approach and Solution

Contents

3.1 General Approach and Solution

This chapter describes each case's details and shows all the work done to build the dashboards to solve the problem stated, and in particular, to answer the research questions presented in the section 1.5. The proposed approaches present are for individual use cases, each with a security proposal but with a different objective of what information should be relevant to an industrial control system.

In figure 3.1, presents the general architecture for the use cases and is observable of the general concept for implementing the dashboard visualizations. The input sources are where the data will be processed and analyzed from diverse scan data with specific objectives. It is a continuous source of information that keeps feeding the system with reliable data. For example, with the vulnerability data sources with new information for each release or update of new software or program, they can be uploaded to the system security database to keep it more complete and updated. All information is centralized on the system security database with the main core. The data can be disseminated if only a certain amount of data is necessary for a use case after making tests with a relevant purpose for the industrial necessity.

Figure 3.1, also contains a cloud with some security automation use cases that can be developed to create use cases. That is what we will be doing in the next sections of this chapter.

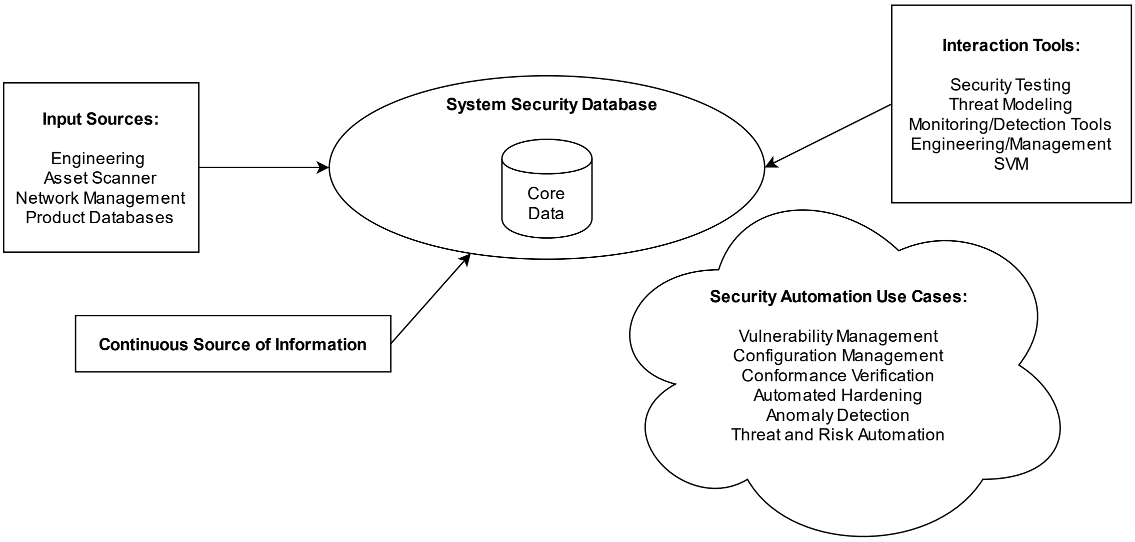


Figure 3.1: General Model for Use Cases

For each use case, there is a description explaining the details to understand the possible information that should be displayed on a dashboard and its relevance. Using the Goal-Question-Measurement model, we can see the topics we require and which data we have to collect. The second part contains information regarding the data workflow and explains how the data was processed to be imported to Kibana successfully. The third part focuses on building a mock-up, choosing what information should be present in each dashboard element, and explaining each aspect to comprehend if it fits the initial proposal. The fourth part contains the prototype dashboards and the final dashboards to show that information can show each case's information.

Table 3.1: Design-Science Research Guidelines by Hevner, Source: [5]

Guideline	Description
Design as an artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Research contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Research rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

The proposed approach reveals to develop industrial security dashboard visualization solutions regarding the conducted background research and literature review, where the decision of tool was base on the specified requirements and the elements were analyzed and categorized.

3.2 Digital Twin Motors

3.2.1 Case Description

In this first use case, we will observe the velocity of two independent motors connected with an axis. It is essential to observe the momentum of both because if they do not have the same velocity, an accident in an industrial domain could happen, e.g., destroy the assembly line, provoke injuries. By observing the velocity (the motors' vibration is calculated through a program), we can determine if there is a malfunction on the motors and the necessity to stop them if needed or adjust the velocity.

In figure 3.2, we can observe the main objective with the questions needed to give context and relevance with the proposed elements displayed in the mock-up.

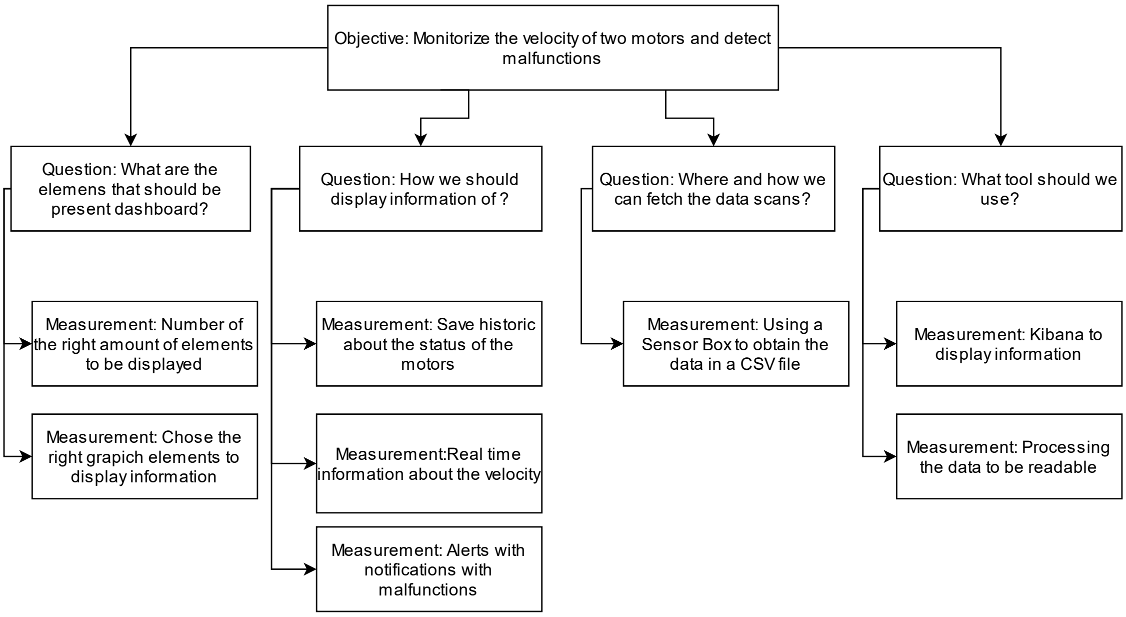

Objective: Monitorize the velocity of two motors and detect malfunctions
Question: What are the elemens that should be present dashboard?
Question: How we should display information of ?
Question: Where and how we can fetch the data scans?
Question: What tool should we use?
Measurement: Number of the right amount of elements to be displayed
Measurement: Chose the right grapich elements to display information
Measurement: Save historic about the status of the motors
Measurement:Real time information about the velocity
Measurement: Alerts with notifications with malfunctions
Measurement: Using a Sensor Box to obtain the data in a CSV file
Measurement: Kibana to display information
Measurement: Processing the data to be readable

Figure 3.2: Goal-Question-Measurement for Digital Twin Motors

In figure 3.3, represents the motors system's architecture and how the user interface and controllers control them are connected. The input action, e.g., the velocity of the motors, is inserted by a Human-Machine Interface (HMI), and next, there is an option to store data into a local database. The input continues passing by the PLC that has a connection for each motor, and after this process, the engines start to work at the speed defined by the user. The information is saved in the "Sensor Box" storing the motor's information.

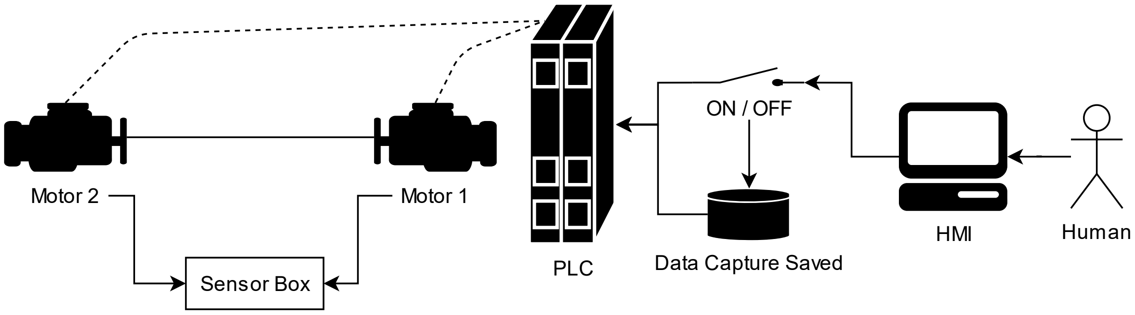


Figure 3.3: Digital Twin Motors Architecture

3.2.2 Data Workflow

The information regarding the rotations is gathered from the sensor box that records the two motors' information. The data capture saved records information relative to the human interface machine, and then the data comes in a CSV file. Then it is imported into Kibana with some data processing, so Kibana does not have trouble handling the data, as shown in figure 3.4.

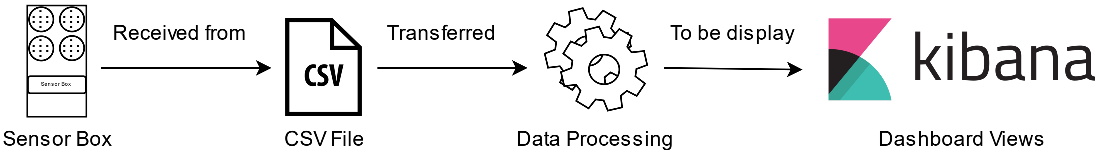
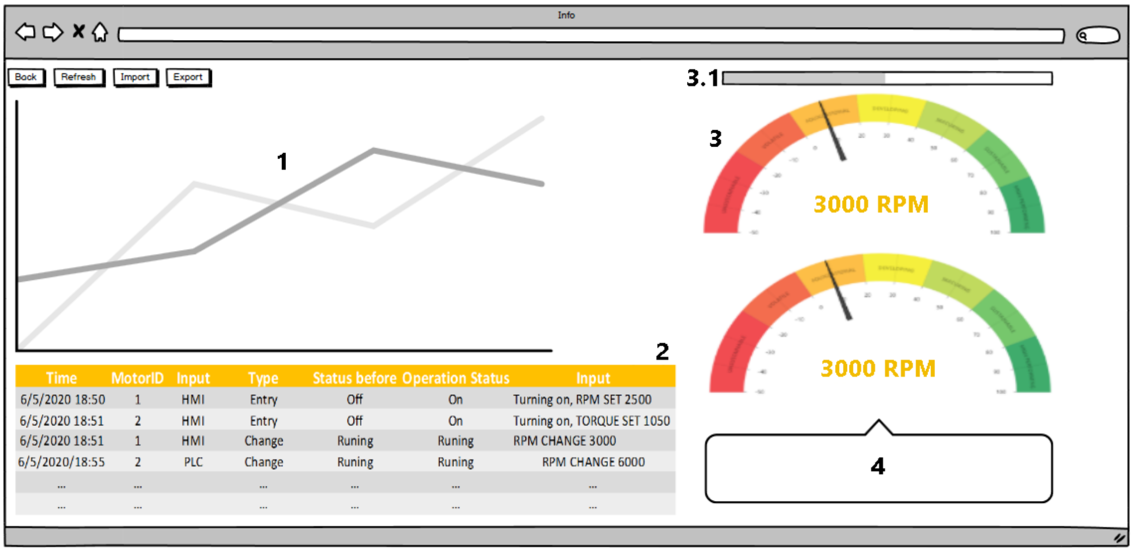


Figure 3.4: Data Workflow from Sensors

3.2.3 Mock-up Design

The mock-up created for this purpose of security monitoring is based on the two motors' velocity compared with each and the input from the HMI and in the PLC. The mock-up for the digital twin motor is represented in figure 3.5.



Time	MotorID	Input	Type	Status before	Operation Status	Input
6/5/2020 18:50	1	HMI	Entry	Off	On	Turning on, RPM SET 2500
6/5/2020 18:51	2	HMI	Entry	Off	On	Turning on, TORQUE SET 1050
6/5/2020 18:51	1	HMI	Change	Runing	Runing	RPM CHANGE 3000
6/5/2020/18:55	2	PLC	Change	Runing	Runing	RPM CHANGE 6000
...	...		...	...	...	...
...	...		...	...	...	...

Figure 3.5: Mock-up for Digital Twin Motors

Describing the numbers present in the mock-up to understand the concept easily:

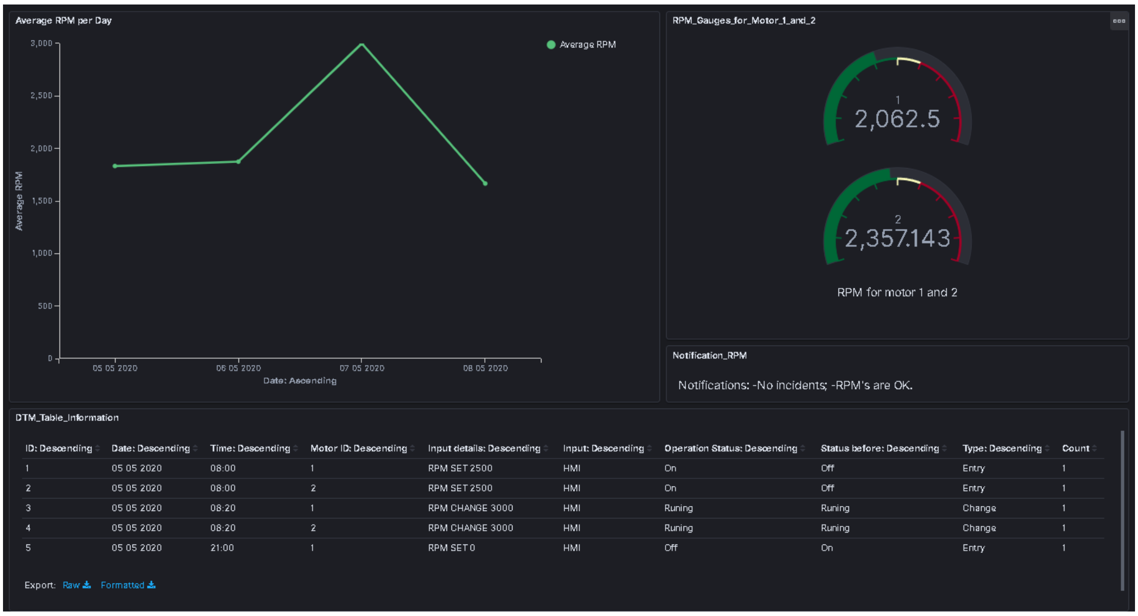
- 1 - Saves historical information about the rotations per minute and vibration of the two motors to see in detail when happened differences. It is important to analyze the uptime and the differences over time;
- 2 - The table that saves all the inputs inserted in the HMI. It displays the commands received by the PLC and delivered to the motors and it is they were successfully introduced in the motor operation. So we can recognize faster if someone is trying to inject incorrect data in the engines;
- 3 - Real-time rotations per minute meter for both motors. The real-time information displayed about the rotations per minute or other stats that may be relevant;
- 3.1 - A progress bar that translates the % difference, for example, a maximum of 3%. With this, we observe in seconds the changes in real-time of the RPM's between the motors;

- 4 - Display the alerts with sound notification if something is not right. By notifying the users of any problem that can also display the alerts generated by anomalous in the regular operation, it is possible to solve a particular problem.

3.2.4 Dashboard Development

Figure 3.6 represents the final dashboard for the digital twin motors case. The data imported was dummy data, and it was used to create this dashboard, more details in section 5.2.

On the top left corner, we have the historical information about the rotations per minute on average for the motors by day in a line chart. On the right is represented with gauges, the real-time information for the rotations per minute for both motors. Each gauge has the identifier on the center and above the rotations to identify each motor. The progress bar could not be created due to Kibana limitations. There has not any element that could represent this progress bar with success. Underneath the gauges, there is a text box with information regarding the notification of the system. It contains the alerts notifications about the operation status focusing on the rotations of the motors. The last element present in the dashboard is the table. It contains information from the inputs made on the human interface machine, the time information (date and time), and information about the input.



Notifications: -No incidents; -RPM's are OK.

ID: Descending	Date: Descending	Time: Descending	Motor ID: Descending	Input details: Descending	Input: Descending	Operation Status: Descending	Status before: Descending	Type: Descending	Count
1	05 05 2020	08:00	1	RPM SET 2500	HMI	On	Off	Entry	1
2	05 05 2020	08:00	2	RPM SET 2500	HMI	On	Off	Entry	1
3	05 05 2020	08:20	1	RPM CHANGE 3000	HMI	Runing	Runing	Change	1
4	05 05 2020	08:20	2	RPM CHANGE 3000	HMI	Runing	Runing	Change	1
5	05 05 2020	21:00	1	RPM SET 0	HMI	Off	On	Entry	1

Figure 3.6: Digital Twin Motors Dashboard

This first use case's primary goal is to explore the Kibana features and capabilities, which is a mock-up scenario, and the data tested is not real data from the motors.

3.3 Vulnerability Scan Monitoring

3.3.1 Case Description

This second use case has the objective to show from a SiESTA scan results the vulnerabilities found in a system and then display the information to make decisions that will impact the system.

SiESTA is a hardware and software developed by Siemens to scan vulnerabilities on products in the development stage to remove security gaps. After configured, it can run automatically to test the products based on existing security software (e.g., Nmap, Nessus, Kali). It can be used in an industrial environment to scan network security, discovering which assets exist within the network, open ports and services running, check if they are appropriately configured. We present the developed mock-ups in a dashboard format to visualize security vulnerability.

In figure 3.7, we can observe the main objective with the questions needed to give context and relevance with the proposed elements displayed in the mock-up.

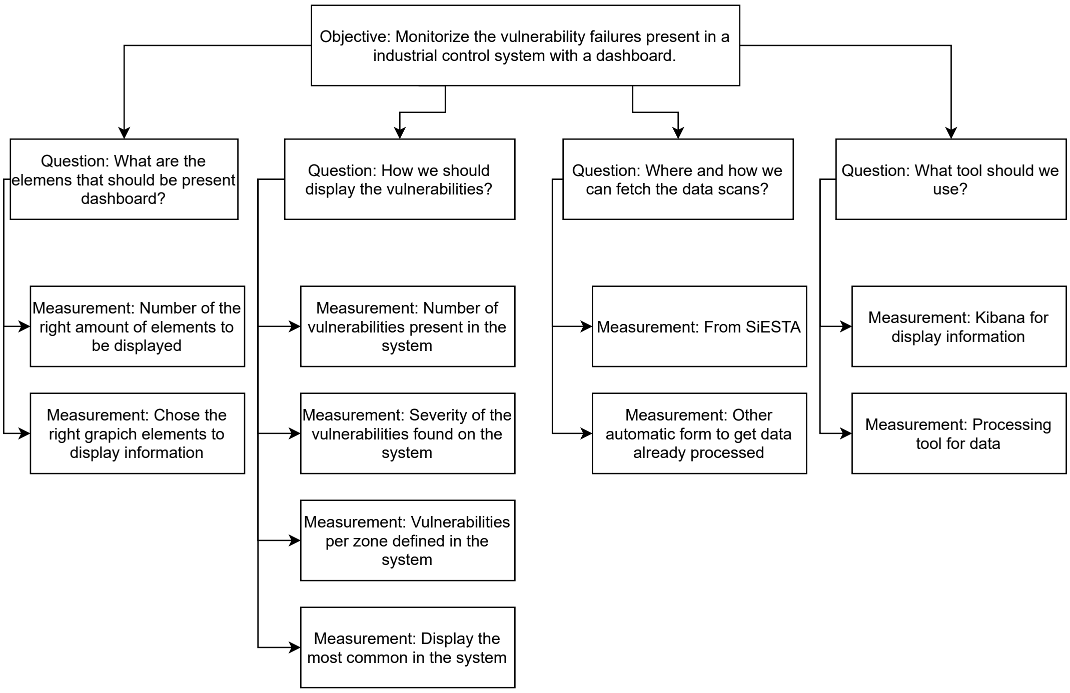

Objective: Monitorize the vulnerability failures present in a industrial control system with a dashboard.
Question: What are the elemens that should be present dashboard?
Measurement: Number of the right amount of elements to be displayed
Measurement: Chose the right grapich elements to display information
Question: How we should display the vulnerabilities?
Measurement: Number of vulnerabilities present in the system
Measurement: Severity of the vulnerabilities found on the system
Measurement: Vulnerabilities per zone defined in the system
Measurement: Display the most common in the system
Question: Where and how we can fetch the data scans?
Measurement: From SiESTA
Measurement: Other automatic form to get data already processed
Question: What tool should we use?
Measurement: Kibana for display information
Measurement: Processing tool for data

Figure 3.7: Goal-Question-Measurement for Vulnerability Scan

3.3.2 Data Workflow

The method to fetch data in this use case is straightforward, after a SiESTA scan, we compile the files output, and then we process the data to put it online on Kibana represented in figure 3.8.

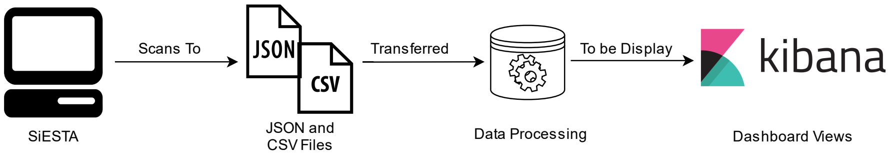


Figure 3.8: Data Workflow from Vulnerability Scans

3.3.3 Mock-up Design

The general concept for the mock-up in figure 3.9 has all the elements. Still, the bar chart represented can have three different types of data displayed. The letters (X, Y, Z and K) present in figure 3.9 are nonrepresentative values. For that bellow the general concept, we have defined the possible bar charts, each with specific information.

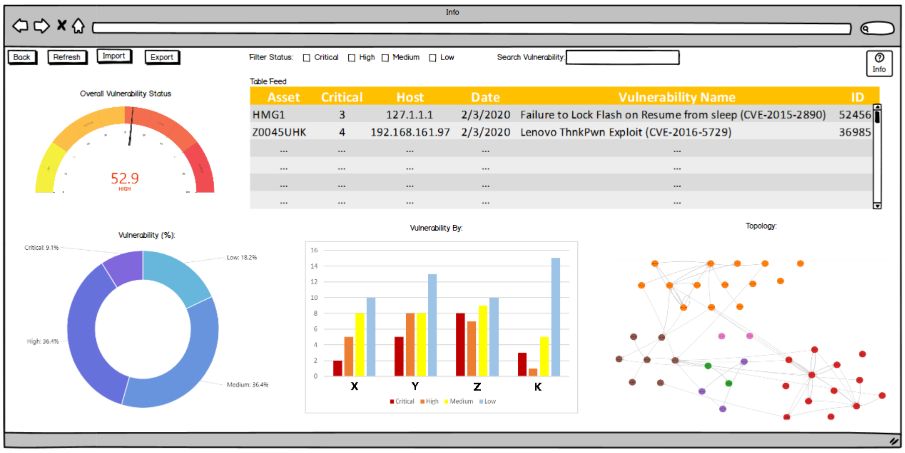


Table Feed

Asset	Critical	Host	Date	Vulnerability Name	ID
HMG1	3	127.1.1.1	2/3/2020	Failure to Lock Flash on Resume from sleep (CVE-2015-2890)	52456
Z0045UHK	4	192.168.161.97	2/3/2020	Lenovo ThnkPwn Exploit (CVE-2016-5729)	36985
...	...	...	...	...	
...	...	...	...	...	
...	...	...	...	...	
...	...	...	...	...	

Figure 3.9: Mock-up with vulnerability General

In figure 3.10, shows the vulnerabilities numbers by subnets in the system.

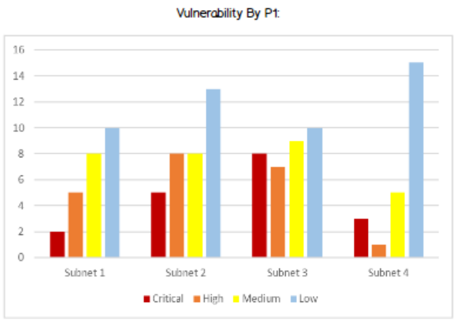


Figure 3.10: Bar chart with vulnerabilities numbers by subnets

In figure 3.11, shows the vulnerabilities numbers by the type of asset.

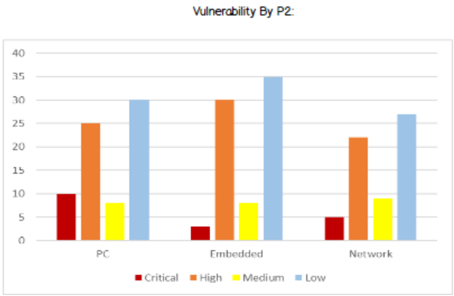


Figure 3.11: Bar chart with vulnerabilities numbers by the type of asset

In figure 3.12, shows the vulnerabilities numbers by each subnets asset type in the system.

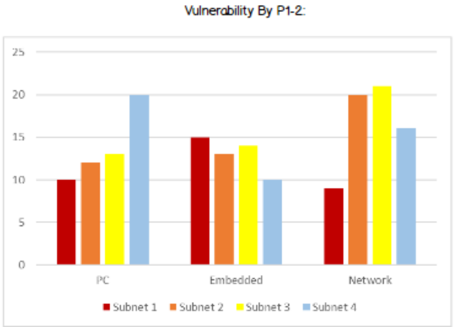


Figure 3.12: Bar chart with vulnerabilities numbers by the asset type of each subnet

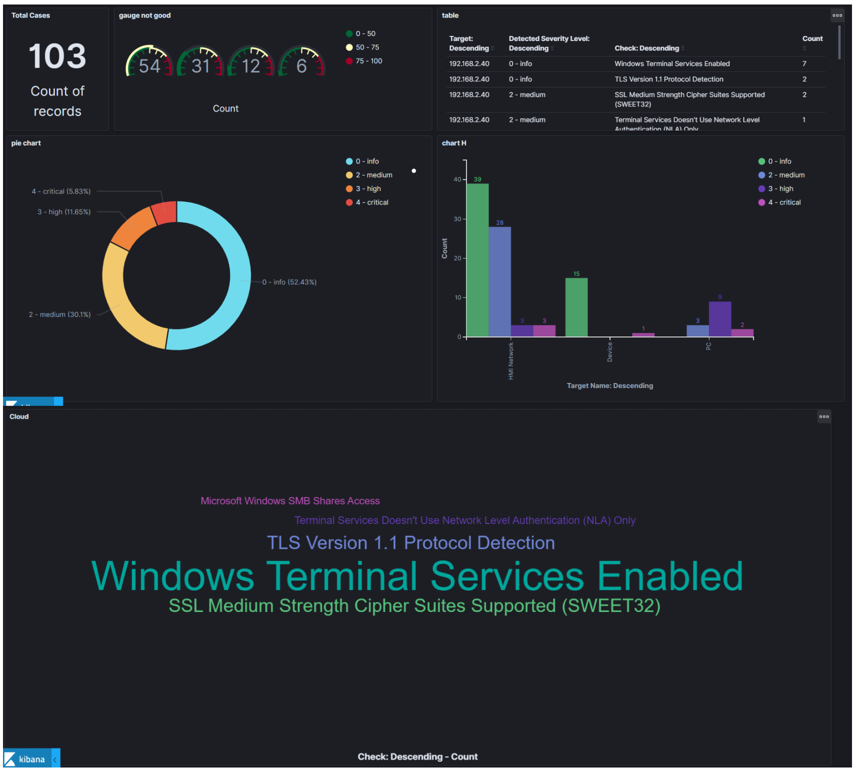
After visualizing the mock-up, we will now explain:

1. **Gauge** - With this, we can observe the general stability of the system with the present vulnerabilities, so with this is easier to keep the system more healthy, we used this element because it provides a measurement with colors to represent what is the condition of a system;
2. **Table** - Summarizes the information about the vulnerabilities with the area, IP address, name of the asset affected with specific vulnerabilities, and the date of detection and is easy to understand and read what is displayed in this element;
3. **Pie Chart** - Categorize the severity of the vulnerabilities by percentage. This element separate by color each severity. It is easy to see large disparities in data, but the problem with the pie charts is that they are unhelpful when observing trends over time because the number of data increases, creating a wrong view on this element;
4. **Bar Chart** - Shows the vulnerability number by subnets in the system or shows the vulnerability number by the type of asset or shows the vulnerability number by each subnets asset type in the system. Bar chart summarizes a large data set in visual form and permit a visual check of the accuracy and reasonableness of calculations but they can require additional explanation;
5. **Network Diagram** - Shows the system's network map with different colors symbolizing the different subnets presents in the system. They provide a good view of the

overall network with separated areas, but network diagrams can sometimes be too complex and challenging to discern visualization.

3.3.4 Dashboard Development

So with these elements present in the mock-ups, we consider that it should be necessary to show the system's vulnerabilities. In figure 3.13 is represented the dashboard prototype. We can observe the top left corner a counter with all the vulnerabilities found in the network. Next to it, we have gauges that display the system's health. The number of vulnerabilities found in the system should be green for a healthy system and red for an unhealthy system for each severity detected with conditions created to support this aspect. Still, these gauges were not working correctly on this prototype because Kibana did not recognize the data for each type of severity. This problem was further fixed by adding conditions to the gauges and visualizing each severity by seeing one by one. The table has information relative to the IP address with the vulnerability with the severity and the name of the vulnerability found. We have two graphs, a pie chart just with simple information relative to the severity for each vulnerability found and the graph bars that contain the severity by the type of asset present in the subnet. We add the cloud counter at the end of the dashboard to visualize what vulnerabilities are more common to find in a particular network. This feature could provide an additional value to the person viewing the dashboard. Kibana has not the feature to create network diagrams in the free version, so we preferred to use this visual element.

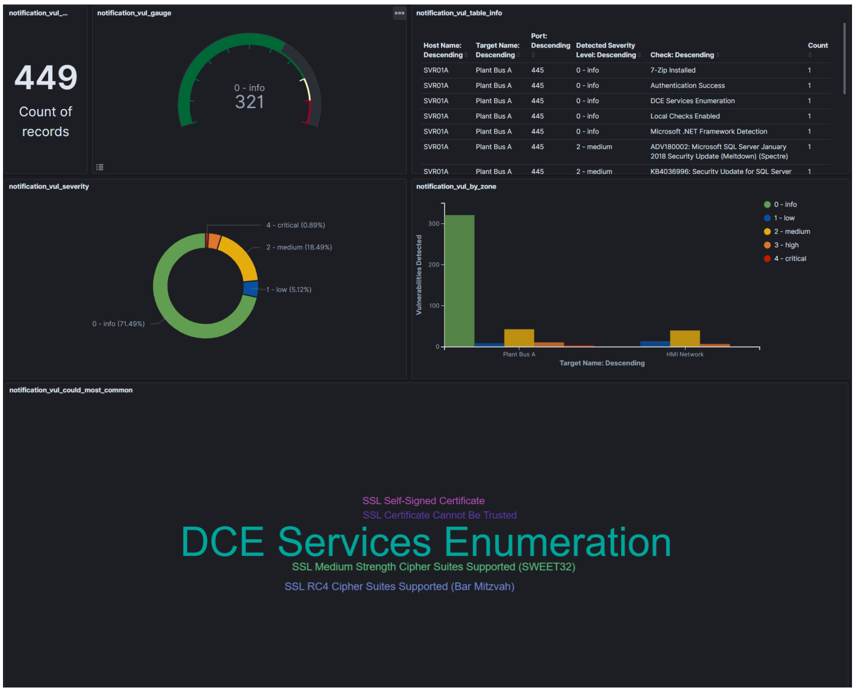


Target: Descending	Detected Severity Level: Descending	Check: Descending	Count
192.168.2.40	0 - info	Windows Terminal Services Enabled	7
192.168.2.40	0 - info	TLS Version 1.1 Protocol Detection	2
192.168.2.40	2 - medium	SSL Medium Strength Cipher Suites Supported (SWEET32)	2
192.168.2.40	2 - medium	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	1

Figure 3.13: Vulnerability Scan Monitoring Prototype Dashboard

In figure 3.14, we can observe the final prototype after some analysis to better meet the requirements for a good visualization. Some changes were made to the dashboard. From the mock-up, the element that was not possible to create was the topology map because on Kibana to in the list of visual elements to add on the dashboard, there was not any type that could recreate the visual topology element, so for this, we ignored, and the only possibility was to create in a different ambient inside Kibana. Considering the security standards in this dashboard, there is no sensitive data displayed (data confidentiality). The tool provides the capability to report the current list of vulnerabilities found in components and their associated properties about security (resource availability). These are some of the security standards that have been applied to the development of this dashboard. Another's security standard also were considered.

Summarizing also what is displayed on the dashboard, figure 3.14, we have an in the top left corner a counter for the number of vulnerabilities found in the network, on the right the gauge show health of the system for the vulnerabilities that are "info", and with the metric created, we can see that the system is healthy. For example, if we filtered for the critical vulnerability, the metric would be a different color. The table contains the hostname in a determinate area, which is the "Target Name" with the communication endpoint "Port", the severity of the vulnerability found, and the name of the vulnerability. In the middle section, the pie chart has the percentage of severity present in the system. At the bar chart, the vulnerabilities are divided by the subnets in the system.In the end, a word cloud that shows the most commons vulnerabilities found in the network.


notification_vul_table_info

Host Name: Descending	Target Name: Descending	Port: Descending	Detected Severity Level: Descending	Check: Descending	Count
SVR01A	Plant Bus A	445	0 - info	7-Zip Installed	1
SVR01A	Plant Bus A	445	0 - info	Authentication Success	1
SVR01A	Plant Bus A	445	0 - info	DCE Services Enumeration	1
SVR01A	Plant Bus A	445	0 - info	Local Checks Enabled	1
SVR01A	Plant Bus A	445	0 - info	Microsoft .NET Framework Detection	1
SVR01A	Plant Bus A	445	2 - medium	ADV180002: Microsoft SQL Server January 2018 Security Update (Meltdown) (Spectre)	1
SVR01A	Plant Bus A	445	2 - medium	KB4036996: Security Update for SQL Server	1

Figure 3.14: Vulnerability Scan Monitoring Final Dashboard

3.4 Vulnerability Scan Rating

3.4.1 Case Description

The third use case is a risk-based vulnerability classification to classify the vulnerabilities for a specific system based on the scale for each aspect:

- Exposure;
- Exploitability;
- Impact.

We can calculate the system's overall risk threat in a matrix combining all those aspects, exposure, exploitability, and impact.

This use case aims to simplify the process of the overall rating vulnerabilities in software and hardware present in a network to provide the fastest reaction to problems that can appear by attackers that can damage specific processes in a network. This use case is important also for the same reason was the use case in section 3.3, but this one has a different purpose with the classification and to find and display only the system's vulnerability per zone in a network.

This use case's main difference is that it is used to display vulnerability information with emphasize since the new input data also considers system-specific information.

In figure 3.15, we can observe the main objective with the questions needed to give context and relevance with the proposed elements displayed in the mock-up.

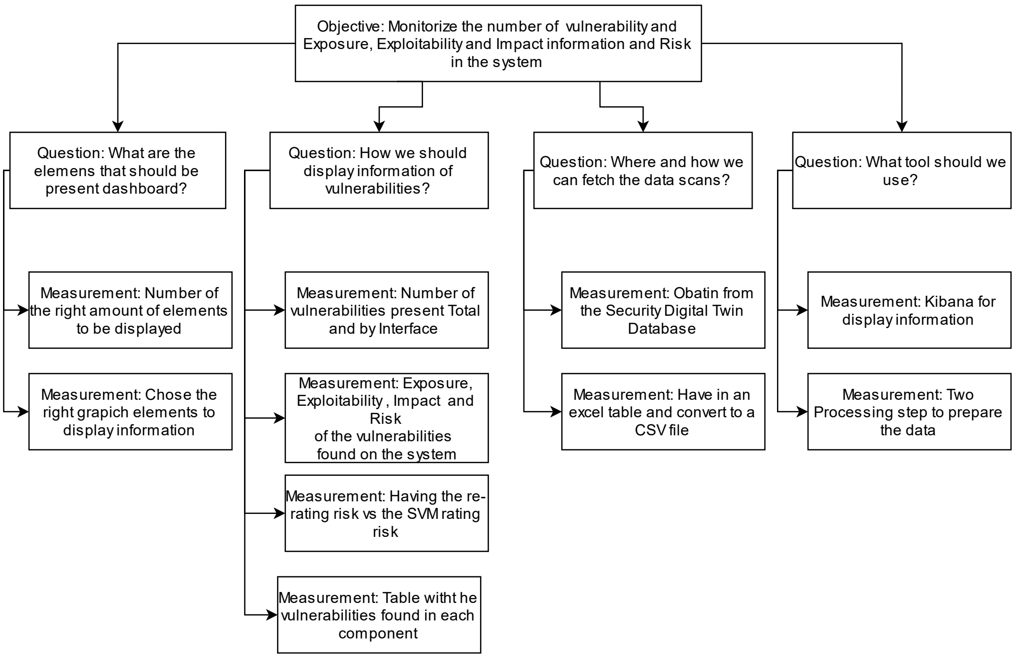

Objective: Monitorize the number of vulnerability and Exposure, Exploitability and Impact information and Risk in the system
Question: What are the elemens that should be present dashboard?
Question: How we should display information of vulnerabilities?
Question: Where and how we can fetch the data scans?
Question: What tool should we use?
Measurement: Number of the right amount of elements to be displayed
Measurement: Chose the right grapich elements to display information
Measurement: Number of vulnerabilities present Total and by Interface
Measurement: Exposure, Exploitability , Impact and Risk of the vulnerabilities found on the system
Measurement: Having the re-rating risk vs the SVM rating risk
Measurement: Table witht he vulnerabilities found in each component
Measurement: Obatin from the Security Digital Twin Database
Measurement: Have in an excel table and convert to a CSV file
Measurement: Kibana for display information
Measurement: Two Processing step to prepare the data

Figure 3.15: Goal-Question-Measurement for Vulnerability Scan Rating

The description of the elements used risk-based vulnerability classification to classify are:

- The exposure is the level of access for the attacker to exploit the system [31];

- The exploitability is the simplicity to perform a successful attack [32]:
  - With these two, they are combined to create a likelihood scale in a matrix to calculate the likelihood score for the system. They are rated in high, medium or low scales [31].
- The impact scale is more based on the protection goal of the vulnerability that can be confidentiality, integrity, or availability, each one. The scale for impact is categorized as disastrous, critical, moderate, or negligible [32]:
  - The risk is a combination of the consequences of an event and the associated likelihood of occurrence and has four scales, major, significant, moderate, minor the represent the level of priority to act for a certain vulnerability found in the system [32].

The global risk classified in the security vulnerability monitoring that monitors the information reported from new vulnerabilities found in new releases is an internationally standardized scoring system for vulnerabilities [1].

In this case, we have two different types of risk. For the global risk is displayed in a Siemens website [2] and the risk with a re-rating that includes some system-specific configuration and the risk are recalculated.

With all this information and data, we will create a dashboard to view the vulnerability risk.

3.4.2 Data Workflow

The vulnerability information that is present in the security digital twin database is firstly aggregated in an excel table with threat and risk analysis information from a data base, which needs to be converted into a CSV format (Data Processing I). After conversion, CSV data is pre-processed (Data Processing II) and imported into Kibana to create dashboard as show in figure 3.16.

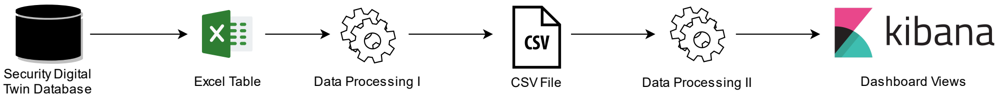


Figure 3.16: Data Workflow for Vulnerability Scan Rating

3.4.3 Mock-up Design

In figure 3.17, it is easy to see the information regarding the description of the use case. Describing the mock-up we have:

1. The number of overall vulnerabilities found in the system;
2. A bar chart is divided by exposure, exploitability, and impact rating of the overall file imported in the Kibana;

[1] https://www.first.org/cvss/

[2] https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

3. A graph with information regarding the interface that was the vulnerability that can be attacked;
4. Table with the components found and for each vulnerability present.

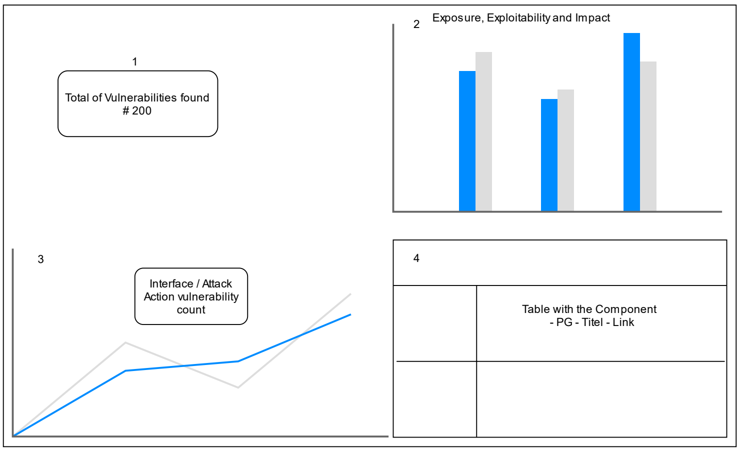
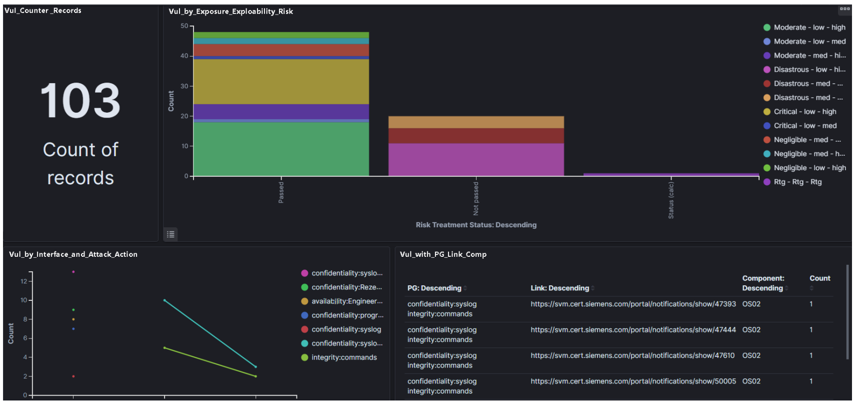


Figure 3.17: Mock-up for Vulnerability Scan Rating

3.4.4 Dashboard Development

Applying the mock-up structure on the data given to create the dashboard, this is the result in figure 3.18. After analyzing the data to segregate the visual elements and making a more superficial view and more comfortable to understand, this view was hard to know with any background of the use case and data used on the dashboard. We can observe the number of vulnerabilities found on the systems on the top left corner. On the top right corner is the number of vulnerabilities found separated by the risk status (on the x-axis), each with the exposure, exploitability, and impact associated. On the bottom left corner in the number of vulnerabilities found separated by the type of interface (on the x-axis) with each interface's protection goal. On the bottom right is the table that contains the protection goal for each component and the link that describes the vulnerability found on each element.

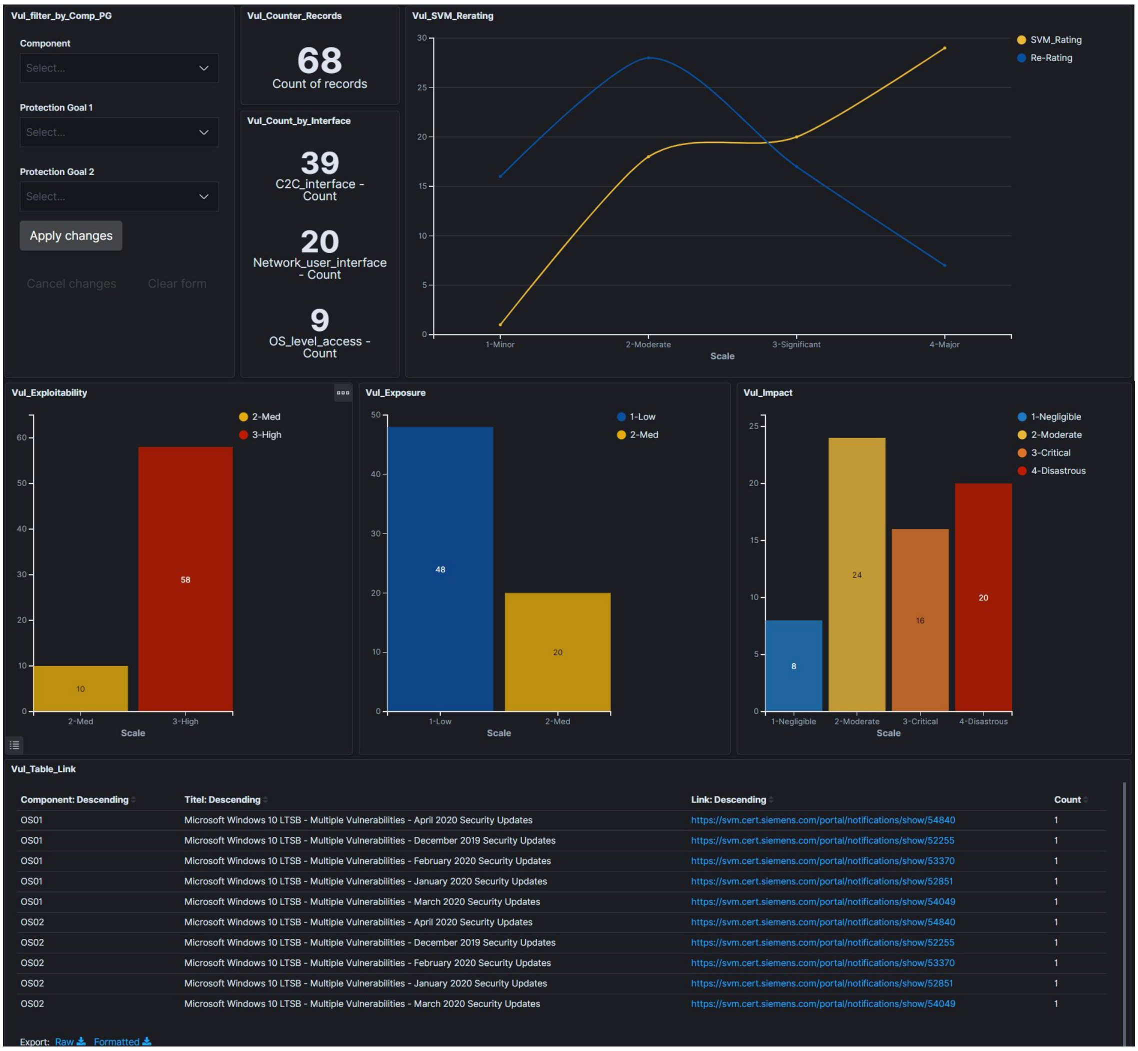


PG: Descending	Link: Descending	Component: Descending	Count
confidentiality:syslog integrity:commands	https://svm.cert.siemens.com/portal/notifications/show/47393	OS02	1
confidentiality:syslog integrity:commands	https://svm.cert.siemens.com/portal/notifications/show/47444	OS02	1
confidentiality:syslog integrity:commands	https://svm.cert.siemens.com/portal/notifications/show/47610	OS02	1
confidentiality:syslog integrity:commands	https://svm.cert.siemens.com/portal/notifications/show/50005	OS02	1

Figure 3.18: Dashboard Prototype for Vulnerability Scan Rating

Considering the security standards in this dashboard, there is no sensitive data displayed (data confidentiality). The tool provides the capability to report the current list of vulnerabilities found in components and their associated properties about security (resource availability). These are some of the security standards that have been applied to the development of this dashboard. Another's security standard also were considered.

After some analysis to better meet the requirements for a good visualization, a new concept for the dashboard is created to mitigate the previous dashboard's problems. In general, this dashboard in figure 3.19, is easier to understand. The data is separated on each visual element. The differences between these two dashboards are the layout and the elements used. For instance, comparing the overall cases found in the dashboard in figure 3.18 with the dashboard in figure 3.19 is due to some processing data that eliminated missing values and reorganized the data to be more consistent and reliable.



Vul_Table_Link

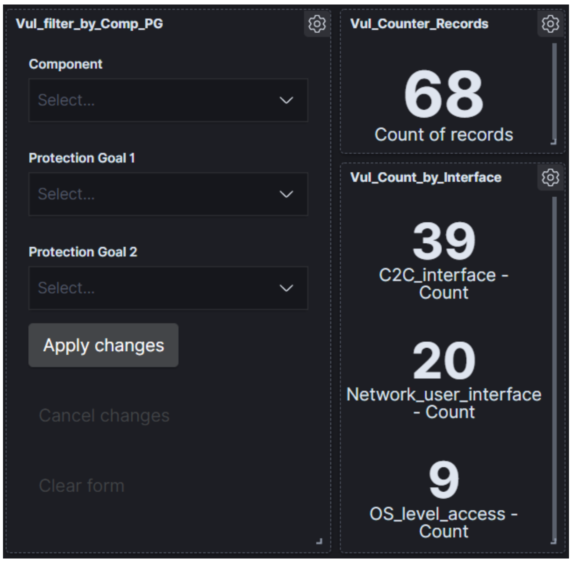
Component: Descending	Titel: Descending	Link: Descending	Count
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1

Export: Raw Formatted

Figure 3.19: Dashboard for Vulnerability Scan Rating after analysis

Describing the dashboard in figure 3.24, we separated into four areas to be easier to understand when explaining.

In Area 1, figure 3.20, we have the filters and the counter, the filters can be applied to the components and the protection goal for each component, there are two protection goals because exist components that have two different protection goals and when uploading the file to the Kibana it automatically separates the protection goal column into two other protection goals. The counters have information relative about the number of vulnerabilities found after the scan and the total of vulnerabilities found divided by interface. This element's main objective is to observe the vulnerabilities found after the scans in global and by an interface and can apply filters.



Vul_filter_by_Comp_PG

Component

Select...

Protection Goal 1

Select...

Protection Goal 2

Select...

Apply changes

Cancel changes

Clear form

Vul_Counter_Records

68
Count of records

Vul_Count_by_Interface

39
C2C_interface - Count

20
Network_user_interface - Count

9
OS_level_access - Count

Figure 3.20: Dashboard for Vulnerability Scan Rating - Area 1

Area 2, figure 3.21, is the line chart relative to the SVM and the re-rating considering a system-specific configuration like explained before in the difference between the two risk present. On this chart, the main goal is to see the difference of vulnerabilities taking into account also the scale after the re-rating and the SVM scans.

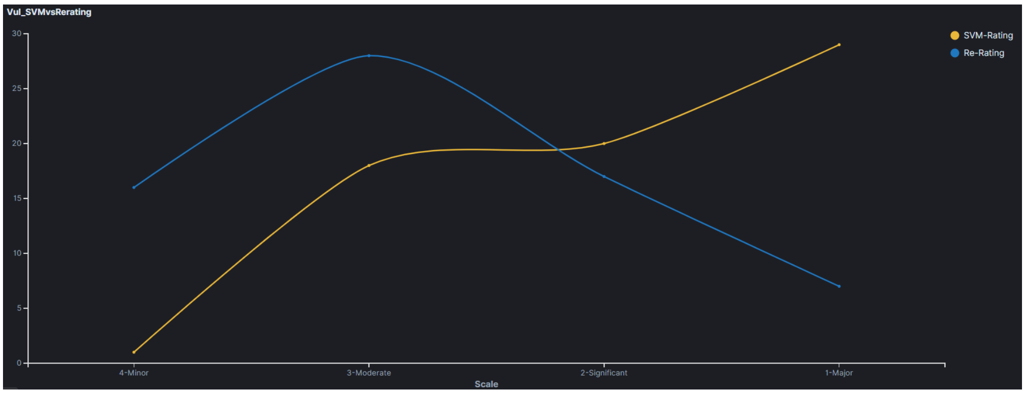


Figure 3.21: Dashboard for Vulnerability Scan Rating - Area 2

Area 3, figure 3.22, has three different bar charts. Each one is a dimension used to calculate the risk, the main goal is to overview how each factor influences the risk.

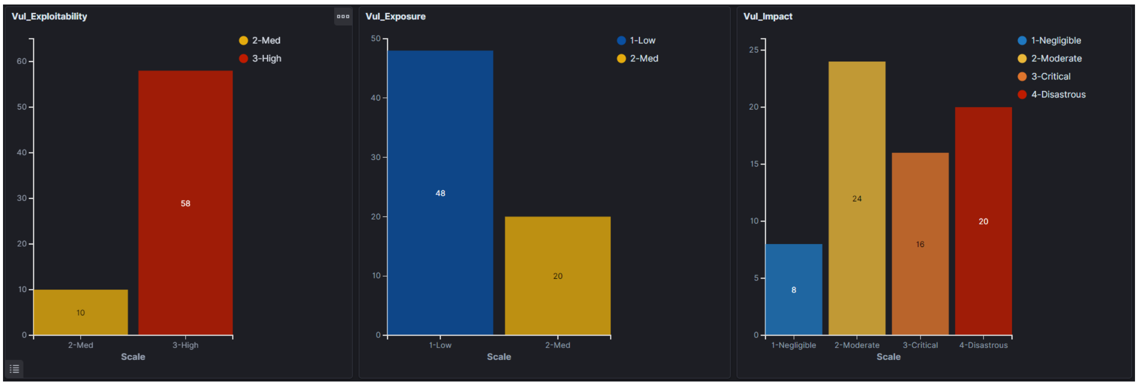
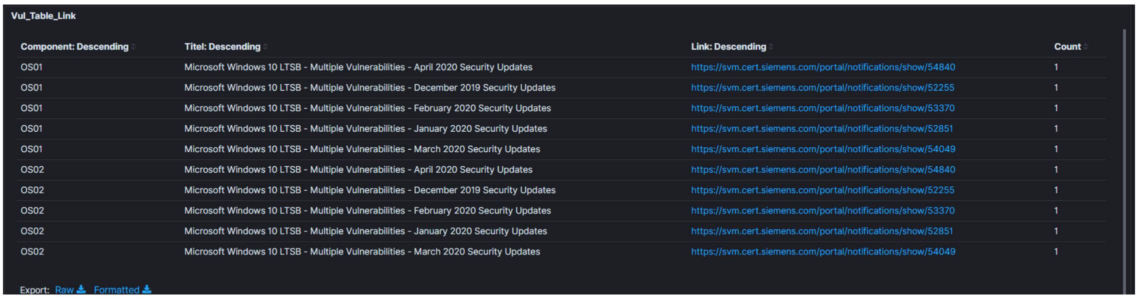


Figure 3.22: Dashboard for Vulnerability Scan Rating - Area 3

Area 4, figure 3.23, is a table that contains a component, that vulnerability found in that component, and the link that is redirecting to the SVM portal that contains information relative to the vulnerability found, such as the description, what can affect, solutions to resolve, or mitigate the vulnerability.

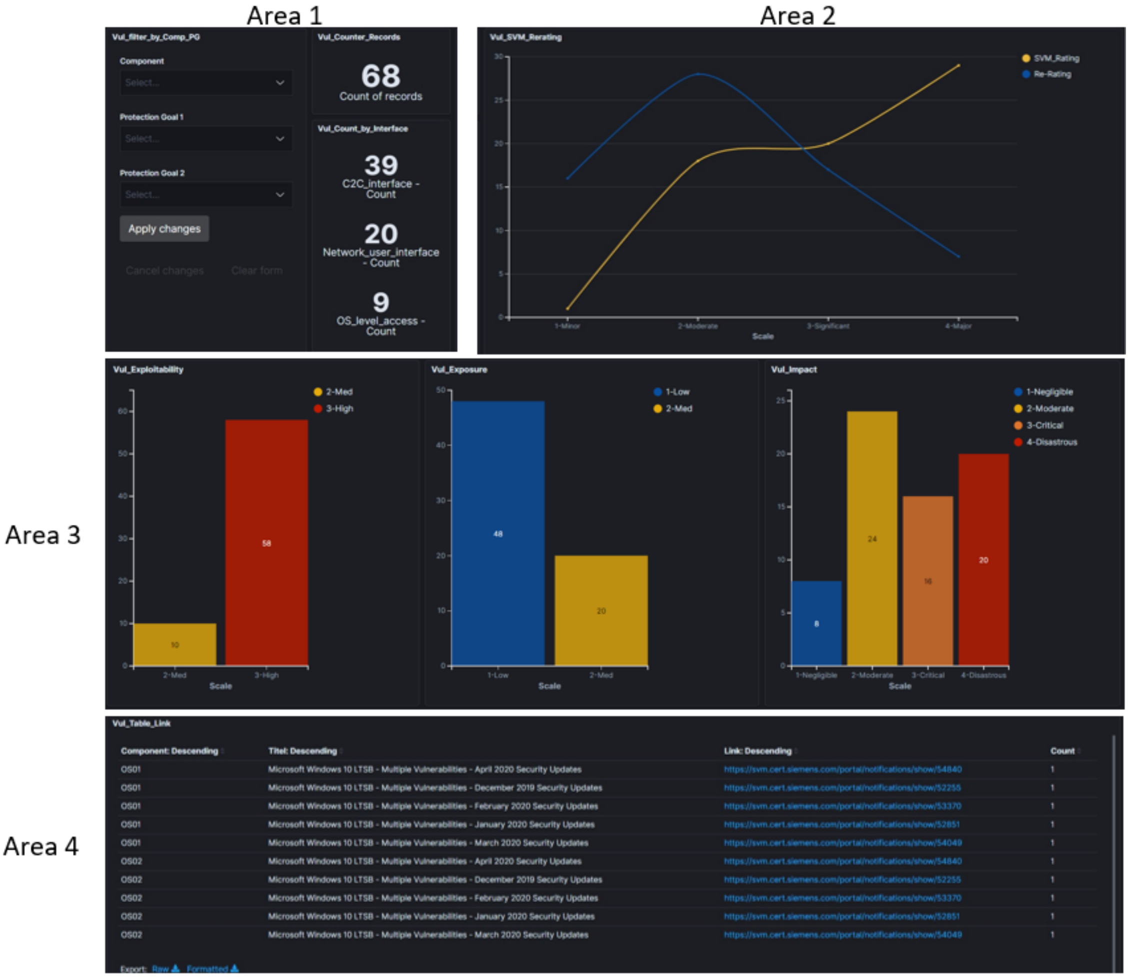


Vul_Table_Link

Component: Descending	Titel: Descending	Link: Descending	Count
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1

Figure 3.23: Dashboard for Vulnerability Scan Rating - Area 4

Figure 3.24 is the aggregation of all areas to have the overall perspective of the dashboard.

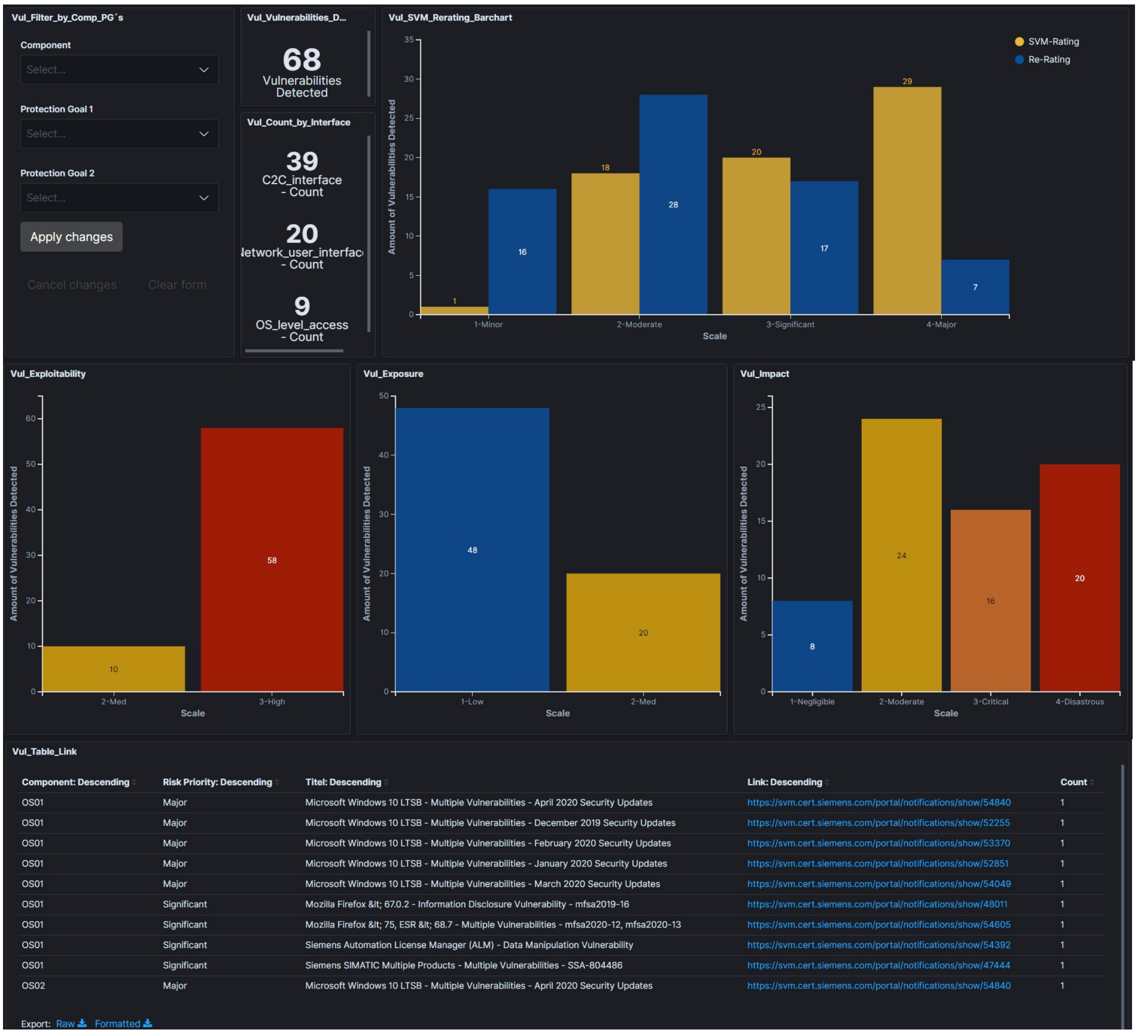


Component: Descending	Titel: Descending	Link: Descending	Count
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS01	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS02	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1

Figure 3.24: Dashboard for Vulnerability Scan Rating all areas

After the questionnaire and the presentation applied in an online meeting with Siemens Cybersecurity Technology Security lifecycle team, nine changes were made to the dashboard, taking into account the questionnaire answers for each area.

The final result is the figure below 3.25. The changes will be explained in the next section 4.5, to be easier to understand the differences and use the questionnaire responses to support those changes.



Vul_Filter_by_Comp_PG´s

Component: Select...

Protection Goal 1: Select...

Protection Goal 2: Select...

Vul_Vulnerabilities_D...

68 Vulnerabilities Detected

Vul_Count_by_Interface

39 C2C_interface - Count

20 Network_user_interface - Count

9 OS_level_access - Count

Vul_Table_Link

Component: Descending	Risk Priority: Descending	Titel: Descending	Link: Descending	Count
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1
OS01	Significant	Mozilla Firefox &lt; 67.0.2 - Information Disclosure Vulnerability - mfsa2019-16	https://svm.cert.siemens.com/portal/notifications/show/48011	1
OS01	Significant	Mozilla Firefox &lt; 75, ESR &lt; 68.7 - Multiple Vulnerabilities - mfsa2020-12, mfsa2020-13	https://svm.cert.siemens.com/portal/notifications/show/54605	1
OS01	Significant	Siemens Automation License Manager (ALM) - Data Manipulation Vulnerability	https://svm.cert.siemens.com/portal/notifications/show/54392	1
OS01	Significant	Siemens SIMATIC Multiple Products - Multiple Vulnerabilities - SSA-804486	https://svm.cert.siemens.com/portal/notifications/show/47444	1
OS02	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1

Figure 3.25: Dashboard for Vulnerability Scan Rating after questionnaire

[This page has been intentionally left blank]

Chapter Four

Evaluation

Contents

4.1 Overview

This chapter is meant to describe the approach to evaluate the dashboard for the case of vulnerability scan rating.

4.2 Evaluation Description

The evaluation was performed in a session with experts from the Siemens Cybersecurity Technology Security lifecycle team. After a presentation, the security experts were asked to answer a questionnaire about the dashboard.

The dashboard presentation contained information about the origin of the data and how the data was processed and imported into Kibana. Also, there was an overall explanation of the case of vulnerability scan rating, so the context and content presented was more precise and objective. It was then described each area of the dashboard, the main goal, and the data used.

The questionnaire was given in the beginning so participants could fulfill it as the presentation flowed. In the end, some questions were made and feedback collected regarding the dashboard. The main objective of the evaluation was qualitative rather than quantitative. Consequently, the feedback analyzes and extracts ideas from the written statements, considering the experts' point of view.

The questionnaire can be found in the Appendix A.

4.3 Dashboard Evaluation

Hevner et al. [5] proposed a research evaluation approach that describes a framework and a process with guidelines for conducting and evaluating good design-science research.

An artifact can be created from design-science studies and is usually a model, a method, or an implemented idea in which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished [5]. The dashboard used to assist in viewing data in the security context is considered an artifact. Drafts of the dashboard were used to explore and create ideas in search of a solution through design-science research.

Thus, this solution was developed to describe and organize the security data set in a dashboard, solving the problem of not having a clear overview of how to visualize security in an industrial system. Therefore, it is possible to provide visual solutions that help security teams to manage vulnerabilities and security problems.

The evaluation aims to evaluate the artifact by analyzing the answers to the questionnaire and the critical opinions given during the evaluation session. Thus extracting feedback to help in the process of improving the artifact. We used a questionnaire because it is possible to ask questions to a reasonable number of people, that can be clarified in a considerable short time. Each one can have a different perspective on what is under evaluation. Eight professionals, all employees at Siemens with specialization in cybersecurity, answered to the questionnaire.

The evaluation had only Siemens employees for reasons of data confidentiality. Although the sample is small to extract significant quantitative results, the experience brings significant qualitative opinions. These opinions were given anonymously, motivating the evaluators to give answers that are not influenced.

The artifact contributes to the visual and management of security areas as an artifact in the enterprise context that offers significant benefits for its research department. The solution developed uses data provided by Siemens Cybersecurity Technology Security lifecycle team through software. This data is used to create the dashboard according to the requirements to have an adequate industrial system view. The level of specification of the data model in the developed solution shows abstraction capacity during the development. The security attributes defined in the data model reflect the use cases' needs, excluding other attributes that would not add value to the limited scope.

With this method, we can see design-science research as a research process to find an effective solution to a problem. Design-science research often simplifies a problem by explicitly representing only a subset of the relevant topics, breaking down a problem into simpler sub-topics.

With the collaboration of Siemens Cybersecurity Technology Security lifecycle team involved in this study, steps have been defined to create a process for creating dashboards. Thus, several iterations were made to understand the best options from the choice of data and the visual elements in each phase. And with the input given in the questionnaire, it was possible to detect and correct the errors and improve, reaching the proposed objectives and requirements.

Hevner et al. [5] state the importance of describing the problem and the effectiveness of the solution. A guide on how to use the Kibana tool has been produced.

The result was displayed in a presentation given to Siemens Cybersecurity Technology Security lifecycle team for the audience. During the presentation, several topics were discussed, and an evaluation of the proposed solution was made. The construction model was shown, as well as the data flow. The dashboard organization was also shown as well as the description of each element present to explain so that there were no doubts.

With this, it is possible to affirm that the developed study successfully followed all the applicable guidelines described by the method proposed by Hevner et al. [5].

4.4 Results

The statistics tool used was Statistical Package for the Social Sciences (SPSS), but the questionnaire results are qualitative than quantitative. Although we did some statistics with the values collected in the closed question that used Likert scale.

In table, 4.1 are the results of the answers to the questions that use a Likert scale from 1-“Totally Disagree” up to 5-“Totally Agree”. From the eighteen items on the questionnaire, only one (S3Q3) got more negative than positive appreciation. The closest to zero the standard deviation, the less the measured data differ around the average.

Table 4.1: Results of Questionnaire from Section 2 to Section 5

	1	**2**	**3**	**4**	**5**	**M**	**SD**
S2Q1-Filters are easy to use and accessible	- -	1 12.5%	- -	5 62.5%	2 25%	4	0.926
S2Q2-The data in counters are relevant to see on the dashboard	1 12.5%	- -	- -	5 62.5%	2 25%	3.88	1.246
S2Q3-The counters are well represented with these visual elements	- -	2 25%	- -	4 50%	2 25%	3.75	1.165
S2Q4-The goal of this area is easily understood	- -	2 25%	3 37.5%	3 37.5%	- -	3.13	0.835
S3Q1-The graph is easily understood	- -	2 25%	2 25%	4 50%	- -	3.25	0.886
S3Q2-This data is important to see on the dashboard	- -	- -	- -	5 62.5%	3 37.5%	4.38	0.518
S3Q3-Data is well represented by this graph	- -	3 37.5%	3 37.5%	2 25%	- -	2.88	0.835
S3Q4-The goal of this area is easily understood	- -	2 25%	- -	4 50%	2 25%	3.75	1.165
S4Q1-These graphics are easily understood	- -	- -	2 25%	5 62.5%	1 12.5%	3.88	0.641
S4Q2-These data are important to see on the dashboard	- -	- -	2 25%	6 75%	- -	3.75	0.463
S4Q3-These graphs are insightful to analyze the risks	- -	1 12.5%	2 25%	4 50%	1 12.5%	3.63	0.916
S4Q4-Data is well represented by these graphs.	- -	1 12.5%	2 25%	4 50%	1 12.5%	3.63	0.916
S4Q5-The goal of this area is easily understood	- -	1 12.5%	3 37.5%	2 25%	2 25%	3.63	1.061
S5Q1-The table is easily understood	- -	1 12.5%	- -	3 37.5%	4 50%	4.25	1.035
S5Q2-These data are important to see on the dashboard	- -	1 12.5%	- -	4 50%	3 37.5%	4.13	0.991
S5Q3-Data is well represented by a table	- -	1 12.5%	- -	6 75%	1 12.5%	3.88	0.835
S5Q4-Having a link with details about the vulnerability is important	- -	- -	- -	3 37.5%	5 62.5%	4.63	0.518
S5Q5-The goal of this area is easily understood	- -	1 12.5%	- -	4 50%	3 37.5%	4.13	0.991

Notes: M-Mean and SD-Standard Deviation Likert scale: 1-Totally Disagree, 2-Disagree, 3-Neutral, 4-Agree, 5-Totally Agree.

In table 4.2 are the results of the answers to the questions with a different Likert scale from 1-“Very Difficult” up to 4-“Very Easy”. Except for the last line in the table with a note. Only two questions (S6Q2 and S6Q4) had a negative evaluation, “understanding the data on the visual elements was...” and “recognizing critical status from the dashboard and the data was...”.

Table 4.2: Results of Questionnaire from Section 6

	1	**2**	**3**	**4**	**M**	**SD**
S6Q1-Looking for specific indicators was	- -	- -	7 87.5%	1 12.5%	3.13	0.354
S6Q2-Understanding the data on the visual elements was	- -	4 50%	4 50%	- -	2.5	0.535
S6Q3-Understanding the scale of colors was	- -	3 37.5%	2 25%	3 37.5%	3	0.926
S6Q4-Recognizing critical status from the dashboard and the data was	- -	3 37.5%	3 37.5%	2 25%	2.88	0.835
S6Q5-Perceiving the overall idea of the dashboard was	- -	2 25%	4 50%	2 25%	3	0.756

Notes: M-Mean and SD-Standard Deviation
Likert scale: 1-Very Difficult, 2-Difficult, 3-Easy, 4-Very Easy.

From the question (S6Q6) in table 4.3, only one person classified the dashboard in an overall appreciation to be “Bad”. The rest of the participants considered it to be “Good” and “Very Good”. Some of the comments made by the professionals at the end of the questionnaire which are:

- “Easy to understand good overview.”;
- “Good visual differences, and mostly data can be seen with a quick view without have to look so long (of course when you know what everything means).”;
- “It is essential to understand that the most important view is to show that the risk reduces over time. With area 2 you go into that direction.”;
- “The selection of the data that is presented makes sense and the presentation of the data”.

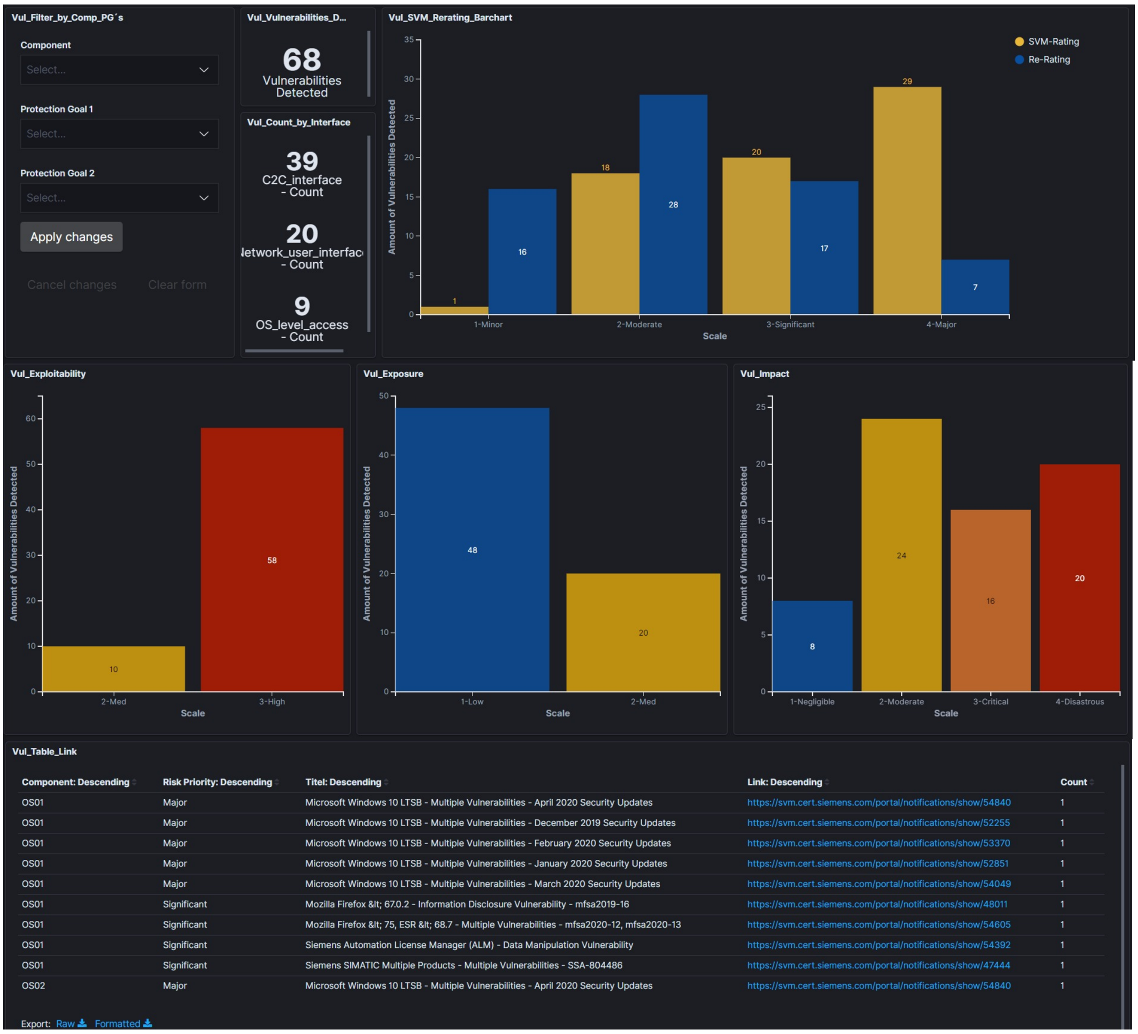
Table 4.3: Results of Questionnaire Overall Appreciation

	1	**2**	**3**	**4**	**M**	**SD**
S6Q6-Rate the dashboard considering all aspects	- -	1 12.5%	4 50%	3 37.5%	3.25	0.707

Notes: M-Mean and SD-Standard Deviation
Likert scale: 1-Very Bad, 2-Bad, 3-Good, 4-Very Good.

4.5 Improvements

The improvements that were made in the dashboard in figure 4.1 taking into account the ideas and point of views given in the presentation and the questionnaire were made for each area, and some had visual impacts in the visual elements that here made and other in the relations created so we can drill up and down the data to get more information. Using the same procedure to explain the dashboard, we will use it again to explain the improvements.



Vul_Table_Link

Component: Descending	Risk Priority: Descending	Titel: Descending	Link: Descending	Count
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - December 2019 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52255	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - February 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/53370	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - January 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/52851	1
OS01	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - March 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54049	1
OS01	Significant	Mozilla Firefox &lt; 67.0.2 - Information Disclosure Vulnerability - mfsa2019-16	https://svm.cert.siemens.com/portal/notifications/show/48011	1
OS01	Significant	Mozilla Firefox &lt; 75, ESR &lt; 68.7 - Multiple Vulnerabilities - mfsa2020-12, mfsa2020-13	https://svm.cert.siemens.com/portal/notifications/show/54605	1
OS01	Significant	Siemens Automation License Manager (ALM) - Data Manipulation Vulnerability	https://svm.cert.siemens.com/portal/notifications/show/54392	1
OS01	Significant	Siemens SIMATIC Multiple Products - Multiple Vulnerabilities - SSA-804486	https://svm.cert.siemens.com/portal/notifications/show/47444	1
OS02	Major	Microsoft Windows 10 LTSB - Multiple Vulnerabilities - April 2020 Security Updates	https://svm.cert.siemens.com/portal/notifications/show/54840	1

Export: Raw Formatted

Figure 4.1: Dashboard for Vulnerability Scan Rating after questionnaire

The areas in figure 3.24 we observe will be analyze.

In Area 1, some feedback regarding the filter lacked explanation and needed a better description of the fields of what protection goals 1 and 2 mean and if one component can aggregate with many protection goals. To fix this misunderstanding of the filter, more comprehensive and complete information is given to explain how the filter work and what possible combination we can make using the filters. Also the headlines and selection of plot were taking in consideration and changes were made to the headlines of visual elements present in the dashboard. Still, within Area 1 in the two counters that provide information about the number of vulnerabilities found, the feedback is that they take up a lot of space on the dashboard:

- “I think there is no need to consume so much space on the screen (or integrate them into graphs)”...“could also show an architecture picture and mark the components which are affected - maybe also how much/severe they have been affected represented by color.”;
- “including headlines and selection of plot types can be improved.”.

For this, the size was a little reduced because creating a graph in the same space was viable because all the other elements present in the dashboard would need to be reallocated in new positions, the minor changes that were made in the connection of the counters with the other visual elements in different areas so for that we can drill up and down the information with more detail for each vulnerability found in a specific interface. The second feedback about architecture is a good idea with a lot of potentials. Still, in Kibana, we ca not create that kind of architecture topology with the components.

In Area 2, the feedback given was more about the type of visual element used that was not representing well the information because:

- “Using a line graph here was not a that good choice. For a line graph, I expect that the values are continuously and interpolation between the points makes sense, which is not the case here since we have distinct steps here. Probably a bar graph is better (or another one without interpolation).”.

Considering the feedback, the graph was changed to a graph bar, and more details have added some information on the chart.

In Area 3, some of the feedback to this area is very interesting proposing need type of visual elements to represent the information and other ways to add the risk in these graphs and also exist some confusion with the colors that were changed. So the alterations made were adding the information to the y-axis and removing the scale color and add a better explanation of the scale of the graphs and a more complex drill up and down that can aggregate more information with the filter and by clicking on the graphs to see the information present. Regarding the feedback about the change the color to blue to green is not a good option. Blue is a color associate with information for the user’s and need to be take into account. Green color can mean that everything is in good standards. Also some summarized comments here made regarding some future improvements that can be done to the dashboard:

- Have better differentiate between impact and likelihood and not detail between exposure and exploitability. Focus more on which data is used, and here, my sensitive data is more affected. Try to show the likelihood of the relevant threat but not overall and how exposed the system is;
- “However, a better representation is still possible. All in all it is a good overview. Maybe you could change the blue to green.”;
- Have the risk broken down into impact and exploitability with other elements.

Considering this two feedback, they can be implemented successfully, although the first one can be more complex.

In Area 4, the feedback regarding the table was to add another column with the severity of the re-rating risk for each vulnerability found so that the major risk vulnerabilities can be fixed fast as possible.

- Add the severity of the vulnerability and sort it by severity (risk) and the titles describing which kind of vulnerability is detected. Get input from potential users. e.g. with this questionnaire to improve the representations;
- Divide into different vulnerability sources (vulnerabilities from TRAs vs. security vulnerabilities notifications) and show to the Management and Auditors that you have reduced your risk over time, creating another dashboard view.

It is possible to address Both feedbacks. The first one would need more time to interact with the user's to have the possibility to collect more information, and the second would need more data and functionalities in the Kibana dashboard to be successfully completed.

Overall feedback regarding the dashboard:

- "A lot of background information is needed to understand the displayed information and not all axes are labeled, it is not clear whether some information was after or before the re rating.";
- "However a description of every graph would be good (probably when you click on it or hovers the mouse).".

Both feedbacks can be solved with a detailed dashboard description. In the prototype dashboard, there were labels missing that were added in the final dashboard. For the second feedback, small text boxes were added in the dashboard with a small description for each element.

4.6 Threats to Validity

This section exposes potential threats to the validity of the study conducted.

- Representativeness - The Siemens supervisor recommended the participants who could attend the presentation, and the structure of the questionnaire was also revised. The participants were chosen because of their experience and knowledge in cybersecurity in the industrial control system, as they were part of the Siemens Cybersecurity Technology Security lifecycle team. This way, we can avoid bias. The sampling size in the questionnaire consisted of 8 members of the Siemens Cybersecurity Technology Security lifecycle team. This is in conformity with the current security research and alike studies that have a restricted environment [33].
- Confirmation bias - A review of this study was performed by an academic supervisor and a Siemens supervisor to avoid bias. Examples of biased analysis by the present study author, who was also the researcher could originate in false statements, twisted to validate hypotheses, and neglect of information.

4.7 Summary

The present work and the dashboard produced show that is possible to produce visualizations of security information respecting the security standards. The evaluation process with the presentation and the questionnaire was a way to confirm the proposed solution's adequacy. The majority of the questionnaire participants agreed that the solution proposed was a great way to show the security information, although some new improvements should be made.

[This page has been intentionally left blank]

Chapter Five

Conclusion and Future Work

Contents

5.1 Conclusion

The present study has proposed an approach and visualizations of security characteristics for the three cases in industrial control systems respecting IEC-62443 standards. The motivation for this research lies on creating a dashboard and methodologies to support the asset's overall security attributes.

The literature review was carried out in the areas of industrial control systems regarding security and security visualization. It was also researched visualization tools used to create dashboards and identified the requirements and attributes for visualization of security elements.

Through the work developed in this study, it was possible to observe the security representation using a visualization tool, taking into account the IEC-62443 security protocols, thus enabling a simplified security analysis of an industrial control system.

Summarizing the analysis and classification of all elements present in this study, we answer the following research questions mentioned in the section 1.5:

- **RQ1** - "How to visualize security in industrial control systems, incorporating requirements from IEC-62443 standards?"
  - This study shows that it is possible to describe security attributes through visualization for each developed case. The visualizations produced help to demonstrate compliance with security requirements and create detailed solutions to offer security analysis. Through the evaluation carried out, as previously mentioned, the dashboard represented security objectively. Although some improvements have been made and can still be made, seven participants out of eight found the security visualizations appropriate and useful.

    In conclusion, a proposed solution was developed and presents a successful solution throughout the developed case studies, but it is still an open and continuously changing solution. With the introduction of new technologies and security systems, needs are continually evolving.
- **RQ1.A** - "What would be an appropriate tool for security visualization?"
  - From the tools picked in the literature review, all of them could prove appropriate for this study but each one has their particularities. For this research question, we think that the answer is still open, and it depends on the study that will be developed and the needs and user experience perspective.
- **RQ1.B** - "What related components, systems, and network attributes should be present?"
  - The cases presented had specific characteristics and requirements for each of them, so it was necessary to analyze each case to understand which components, systems, and network attributes should be present in a dashboard for that case. It is also essential to consider that some requirements and characteristics are general to an industrial control system's security context. Thus, we believe that this question was successfully answered in this study.

In fact, for each case we described the requirement raised by previous research. We then used the mock-up to understand what kind of data was fundamental for that case to be well analysed and to transmit the information clearly.

5.2 Limitations

There was a limitation during this study's development since, the pandemic situation limited access to the laboratories for the use case digital twin motors present in section 3.2. It was necessary to create and use dummy data and not real data, although this use case had the objective of exploring the Kibana features and capabilities.

5.3 Future Work

All the proposed solutions for each use case are final dashboard prototypes, although the most relevant is the last use case covering the Vulnerability Scan Rating described in section 3.4 as some questionnaire's answers suggest. There is always room to improve the dashboard data, the visualization elements and add more functionalities to the dashboards that can be relevant for the users and the business. Other visualization tools to represent information can be used, and even Kibana can have more functionalities added. Also, the type of file that is imported to put the data on Kibana can be improved with the necessary attributes that may change from case to case. An automatic script can be created to upload the required data to increase the dashboard's real-time information.

References

[1] O. Kononenko, O. Baysal, R. Holmes, and M. W. Godfrey. "Mining modern repositories with Elasticsearch." In: *11th Working Conference on Mining Software Repositories, MSR 2014 - Proceedings* (2014), pp. 328–331. DOI: 10.1145/2597073.2597091.

[2] H. Shiravi, A. Shiravi, and A. A. Ghorbani. "A Survey of Visualization Systems for Network Security." In: *IEEE Transactions on Visualization and Computer Graphics* 18.8 (2012), pp. 1313–1329. DOI: 10.1109/TVCG.2011.144.

[3] Z. Drias, A. Serhrouchni, and O. Vogel. "Analysis of cyber security for industrial control systems." In: *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. 2015, pp. 1–8. DOI: 10.1109/SSIC.2015.7245330.

[4] M. Berndtsson. "Developing your Objectives." In: *Planning and Implementing your Computing Project - with Success!* (2008), pp. 54–70.

[5] A. Hevner, S. March, J. Park, and S. Ram. "Design Science in Information Systems Research." In: *MIS Quarterly* (2004), pp. 75–105. DOI: 10.2307/25148625.

[6] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn. "NIST Special Publication 800-82 Revision 2 Initial Public Draft Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations." In: (2014), p. 255.

[7] J. D. Gilsinn and E. C. Cosman. "NIST Cybersecurity Framework ISA99 Response to Request for Information." In: (2013). URL: https://www.nist.gov/system/files/documents/2017/06/08/20131213_eric_cosman_isa99_part1.pdf.

[8] A. Arampatzi. *What Is the ISA/IEC 62443 framework?* Tech. rep. 2019. URL: https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/.

[9] M. Maidl, D. Kroselberg, J. Christ, and K. Beckers. "A Comprehensive Framework for Security in Engineering Projects - Based on IEC 62443." In: *Proceedings - 29th IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2018* (2018), pp. 42–47. DOI: 10.1109/ISSREW.2018.00-33.

[10] W. Paper, O. Comprehensive, and S. Solution. “White Paper Meeting the Cybersecurity Standards of ANSI / ISA-62443-3-3.” In: (2014).

[11] N. Cai, J. Wang, and X. Yu. “SCADA system security: Complexity, history and new developments.” In: *IEEE International Conference on Industrial Informatics (INDIN)* (2008), pp. 569–574. ISSN: 19354576. DOI: 10.1109/INDIN.2008.4618165.

[12] R. Matulevičius. *Security Requirements Secure System Modelling.* Tech. rep. University of Tartu, Estonia, 2017.

[13] A. Sethi and G. Wills. “Expert-interviews led analysis of EEVi-A model for effective visualization in cyber-security.” In: *2017 IEEE Symposium on Visualization for Cyber Security, VizSec 2017.* Vol. 2017-Octob. 2017, pp. 1–8. ISBN: 9781538626931. DOI: 10.1109/VIZSEC.2017.8062195. URL: https://www.qsrinternational.com/product/nvivo-mac.

[14] M. Coudriau, A. Lahmadi, and J. Francois. “Topological analysis and visualisation of network monitoring data: Darknet case study.” In: *8th IEEE International Workshop on Information Forensics and Security, WIFS 2016* (2017), pp. 1–6. DOI: 10.1109/WIFS.2016.7823920.

[15] M. Angelini, N. Prigent, and G. Santucci. “PERCIVAL: Proactive and reactive attack and response assessment for cyber incidents using visual analytics.” In: *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015* (2015), pp. 1–8. DOI: 10.1109/VIZSEC.2015.7312764.

[16] V. S. Carvalho, M. J. Polidoro, and J. P. Magalhaes. “OwlSight: Platform for real-time detection and visualization of cyber threats.” In: *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and Security, IEEE IDS 2016* (2016), pp. 61–66. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.73.

[17] T. Wüchner, A. Pretschner, and M. Ochoa. “DAVAST: Data-centric system level activity visualization.” In: *ACM International Conference Proceeding Series* 10-November-2014 (2014), pp. 25–32. DOI: 10.1145/2671491.2671499.

[18] P. A. Legg. “Enhancing cyber situation awareness for Non-Expert Users using visual analytics.” In: *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016* Figure 1 (2016), pp. 1–8. DOI: 10.1109/CyberSA.2016.7503278.

[19] D. M. Best, A. Endert, and D. Kidwell. “7 Key challenges for visualization in cyber network defense.” In: *ACM International Conference Proceeding Series* 10-November-2014 (2014), pp. 33–40. DOI: 10.1145/2671491.2671497.

[20] L. Harrison, R. Spahn, M. Iannacone, E. Downing, and J. R. Goodall. "NV: Nessus vulnerability visualization for the web." In: *ACM International Conference Proceeding Series* (2012), pp. 25–32. DOI: 10.1145/2379690.2379694.

[21] M. Angelini, G. Blasilli, T. Catarci, S. Lenti, and G. Santucci. "Vulnus: Visual vulnerability analysis for network security." In: *IEEE Transactions on Visualization and Computer Graphics* 25.1 (2019), pp. 183–192. ISSN: 19410506. DOI: 10.1109/TVCG.2018.2865028.

[22] M. Bastian, S. Heymann, and M. Jacomy. "Gephi _ AAAI." In: *Icwsm* (2009), pp. 361–362. ISSN: 14753898. DOI: 10.1136/qshc.2004.010033.

[23] J. J. Miller. "Graph database applications and concepts with Neo4j." In: *Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA* 2324 (2013), p. 36.

[24] G. K. Yong. "A Data Analytic Module To Extend Grafana Functionality." In: January (2019), pp. 1–75.

[25] N. Chan. "A resource utilization analytics platform using grafana and telegraf for the Savio supercluster." In: *ACM International Conference Proceeding Series* (2019). DOI: 10.1145/3332186.3333053.

[26] J. Hamilton, M. Gonzalez Berges, J.-C. Tournier, and B. Schofield. "SCADA Statistics monitoring using the elastic stack (Elasticsearch, Logstash, Kibana)." In: *16th Int. Conf. on Accelerator and Large Experimental Control Systems* (2018), pp. 451–455. DOI: 10.18429/JACoW-ICALEPCS2017-TUPHA034.

[27] H. M. Kienle and H. A. Muiller. "Requirements of Software Visualization Tools : A Literature Survey." In: *2007 4th IEEE International Workshop on Visualizing Software for Understanding and Analysis* (2007), pp. 2–9. DOI: 10.1109/VISSOF.2007.4290693.

[28] S. Bougouffa, B. Vogel-Heuser, J. Fischer, I. Schaefer, and H. Li. "Visualization of Variability Analysis of Control Software from Industrial Automation Systems." In: *2019 Conf. Proc. IEEE Int. Conf. Syst. Man. Cybern.* (2019), pp. 3337–3344.

[29] M. David. *Visual Miscellaneum: The Bestselling Classic, Revised and Updated: A Colorful Guide to the World's Most Consequential Trivia.* 2012.

[30] D. R. V. Basili, G. Caldiera. *Goal question metric approach. Encyclopedia of Software Engineering.* 1994.

[31] V. Jagannathan. "Threat Modeling: Architecting & Designing With Security In Mind." In: *Threat Modeling Express* (2007), pp. 1–11. URL: https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf.

[32] K. A. Jensen, M. Levin, and O. Witschger. *Methods for Testing Dustiness.* 2016. DOI: 10.1002/9781118753460.ch10.

[33] L. Othmane, M. Jaatun, and E. Weippl. *Empirical research for software security: Foundations and experience*. 2017.

Appendix A

Questionnaire

Questionnaire for Vulnerability Rating Dashboard

This *Kibana* dashboard was designed based on our security asset database, intending to the key information got in the *SiESTA* scan. With the support of the security asset database and the vulnerability rating methodology, we can re-rate the vulnerability based on system-specific information and the result will be displayed in the dashboard.

The questionnaire is voluntary and anonymous.

The purpose of this questionnaire is to evaluate the dashboard model defined for this use case. By participating, you are helping to find and solve possible existing problems that we are not aware of, and potentially suggesting solutions to them. In each section, you will be asked to optionally write your opinion on an open-ended question. In other cases you will be asked whether you agree or disagree with the statement, making use of the scale used for the purpose.

Section 1 Role at Siemens The questionnaire is voluntary and anonymous, only your role at Siemens is being solicited as personal information, for analytical and results analysis purposes.

Q.1 - What is your role at Siemens? (Open question)

Section 2

Area 1 - Evaluation of Filter and Counters

This first area (please observe the image to help you remember) is related to the filters by components and protection goals and with the counter for the total vulnerabilities found and by interface. Please give your opinion about the following statements using the Likert Scale (1-Totally Disagree up to 5-Totally Agree).

-Questions with Likert Scale:

- Q.1 - Filters (marked in red) are easy to use and accessible.
- Q.2 - The data in counters are relevant to see on the dashboard (marked in blue).
- Q.3 - The counters are well represented with these visual elements (marked in blue).
- Q.4 - The goal of this area is easily understood (marked in blue).

Q.5 - Do you think this could be represented differently?

- Yes or No

Q.6 - If your answer was yes, which would be and why? (Open question)

Section 3

Area 2 - Evaluation of the SVM vs Re-Rating graph

This second area (please observe the image to help you remember) is related to the SVM rating system and with the Re-rating made by Siemens. Please give your opinion about the following statements using the Likert Scale (1-Totally Disagree up to 5-Totally Agree).

-Questions with Likert Scale:

- Q.1 - The graph is easily understood.
- Q.2 - This data is important to see on the dashboard.
- Q.3 - Data is well represented by this graph.
- Q.4 - The goal of this area is easily understood.

Q.5 - Do you think this could be represented differently?

- Yes or No

Q.6 - If your answer was yes, which would be and why? (Open question)

Section 4

Area 3 - Exploitability, Exposure and Impac This third area (please observe the image above to help you remember) is related to the number of vulnerabilities found on the scans divided by Exposure, Exploitability, and Impact organized by a scale. Please give your opinion about the following statements using the Likert Scale (1-Totally Disagree up to 5-Totally Agree).

-Questions with Likert Scale:

- Q.1 - These graphics are easily understood.
- Q.2 - These data are important to see on the dashboard.
- Q.3 - These graphs are insightful to analyze the risks.
- Q.4 - Data is well represented by these graphs.
- Q.5 -The goal of this area is easily understood.

Q.6 - Do you think this could be represented differently?

- Yes or No

Q.7 - If your answer was yes, which would be and why? (Open question)

Section 5

Area 4 - Table with Components and Links This last area (please observe the image above to help you remember) is related to the vulnerability found on each component with a link that contains vital information about the vulnerability and solutions already been found to solve the vulnerability. Please give your opinion about the following statements using the Likert Scale (1-Totally Disagree up to 5-Totally Agree).

-Questions with Likert Scale:

- Q.1 - The table is easily understood.
- Q.2 - These data are important to see on the dashboard.
- Q.3 - Data is well represented by a table.
- Q.4 - Having a link with details about the vulnerability is important.
- Q.5 - The goal of this area is easily understood.

Q.6 - Do you think this could be represented differently?

- Yes or No

Q.7 - If your answer was yes, which would be and why? (Open question)

Section 6

Overall Appreciation of the Dashboard Finally, now the questions will be about the dashboard in general. Please give your opinion about the following statements using the Likert Scale (1-Very Difficult up to 4-Very Easy).

-Questions with Likert Scale:

- Q.1 - Looking for specific indicators was...
- Q.2 - Understanding the data on the visual elements was...
- Q.3 - Understanding the scale of colors was...
- Q.4 - Recognizing critical status from the dashboard and the data was...
- Q.5 - Perceiving the overall idea of the dashboard was...

Q.6 - Rate the dashboard considering all aspects (organization, type of visual elements, colors and size of visual elements, the relevance of data, type of data displayed). Scale: Very Bad | Bad | Good | Very Good

Q.7 - What are the two main reasons for assigning this score?(Open question)