INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Title
Knowledge Management System for Cybersecurity Incident Response

Candidate Name
Miriam Isabel Farinha Rodrigues

Master in,
Computer Science and Business Management

Supervisor:
PhD Carlos José Corredoura Serrão, Associate Professor,
Iscte - IUL

Supervisor:
PhD Ana Maria Carvalho de Almeida, Associate Professor,
Iscte - IUL

September 2024

TECNOLOGIAS
E ARQUITETURA

Department of Science and Information Technology

Title
Knowledge Management System for Cybersecurity Incident Response

Candidate Name
Miriam Isabel Farinha Rodrigues

Master in,
Computer Science and Business Management

Supervisor:
PhD Carlos José Corredoura Serrão, Associate Professor,
Iscte - IUL

Supervisor:
PhD Ana Maria Carvalho de Almeida, Associate Professor,
Iscte - IUL

September 2024

Acknowledgments

An expression of gratitude is extended to Prof. Carlos Serrão and Prof. Ana Maria de Almeida, my thesis supervisors, for their valuable insights and dissemination of knowledge, which made this research possible. I also wish to express my gratitude to my parents, Pedro and Cristina, my partner Afonso, and my colleague Alex, for their unwavering support throughout this challenging period. It was crucial to have their assistance and understanding, to complete this work. Last but not least, I would like to acknowledge all the participants in the interviews and colleagues who have helped my personal development and have consistently offered support and valuable lessons. To each and every one of you – Thank you.

Resumo

Esta investigação centra-se no desenvolvimento de um Sistema de Gestão do Conhecimento (KMS) concebido para melhorar a colaboração e a eficiência nos procedimentos de resposta a incidentes de cibersegurança. A Resposta a Incidentes (IR) de cibersegurança é crucial para detetar, mitigar e recuperar de ameaças cibernéticas, sendo que Planos de Resposta a Incidentes (IRPs) bem estruturados são necessários para minimizar interrupções e proteger informações sensíveis. No entanto, muitas organizações enfrentam desafios, como limitações de recursos, partilha de conhecimento fragmentada e estratégias de resposta inconsistentes. Este estudo visa colmatar estas lacunas propondo um design de KMS que facilite a colaboração, melhore a troca de conhecimento e agilize a gestão de incidentes através de *playbooks* de resposta partilhados. Utilizando a metodologia de Investigação Científica em Design (DSR), o KMS foi desenvolvido através de um envolvimento iterativo com especialistas, análise de casos de uso e validação de *mock-ups*. O sistema apresenta uma arquitetura modular e oferece ferramentas para a criação de *playbooks*, mecanismos de feedback e colaboração em tempo real, respeitando sempre as normas de segurança dos dados. Após validação por especialistas na área, os resultados demonstraram a eficácia do KMS na melhoria do acesso ao conhecimento, na promoção da colaboração entre as equipas de resposta e na normalização dos processos de gestão de incidentes. Esta investigação tem amplas implicações para as práticas de cibersegurança, promovendo estratégias de resposta proativas e adaptativas e reforçando a resiliência organizacional face a ameaças cibernéticas em evolução.

Palavras-Chave: Colaboração, Sistema de Gestão de Conhecimento, Resposta a Incidentes, Cibersegurança, *Playbooks*

Abstract

This research focuses on developing a Knowledge Management System (KMS) designed to enhance collaboration and efficiency in cybersecurity Incident Response (IR) procedures. Cybersecurity IR is critical for detecting, mitigating, and recovering from cyber threats, with well-structured Incident Response Plans (IRPs) necessary for minimizing disruptions and protecting sensitive information. However, many organizations face challenges, such as resource constraints, fragmented knowledge sharing, and inconsistent response strategies. This study aims to address these gaps by proposing a KMS design that facilitates collaboration, improves knowledge exchange, and streamlines incident management through shared response playbooks. Using a Design Science Research (DSR) methodology, the KMS was designed through iterative expert engagement, use case analysis, and mockup validation. The system features a modular architecture and provides tools for playbook creation, feedback mechanisms, and real-time collaboration, all while adhering to security of the data. Upon obtaining validation from domain experts, the results demonstrated the KMS's effectiveness in improving access to knowledge, fostering collaboration among response teams, and standardizing incident handling processes. This research has broad implications for cybersecurity practices, promoting proactive and adaptive response strategies and enhancing organizational resilience against evolving cyber threats.

Keywords: Collaboration, Knowledge Management System, Incident Response, Cybersecurity, Playbooks

Index

Table of Contents

Table of Figures

Glossary

AI	Artificial Intelligence
AIR	Automatic Incident Responder
APIs	Application Programming Interfaces
CAESAIR	Collaborative Analysis Engine for Situational Awareness and Incident Response
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSIRTs	Computer Security Incident Response Teams
CTI	Cyber Threat Intelligence
DSR	Design Science Research
GUI	Graphical User Interface
IoCs	Indicators of Compromise
IR	Incident Response
IRP	Incident Response Plan
IS	Information Systems
ISMS	Information Security Management System
IT	Information Technology
KM	Knowledge Management
KMS	Knowledge Management System
MISP	Malware Information Sharing Platform
NIST	National Institute of Standards and Technology
OnSOAP	Ontology-driven approach for Security OrchestrAtion Platform
OWL	Web Ontology Language
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RDF	Resource Description Framework
RDFS	Resource Description Framework Schema
SANS	Sysadmin, Audit, Network, and Security
SASP	Semantic web-based Approach for management of Sharable cybersecurity Playbooks
SLR	Systematic Literature Review
SOC	Security Operations Center
TTP	Tactics, Techniques and Procedures
SIEM	Security Information and Event Management

GDPR	General Data Protection Regulation
CACAO	Collaborative Automated Course of Action Operations
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
EoI	Events of Interest
ENISA	European Union Agency for Cybersecurity
CNCS	Centro Nacional de Cibersegurança

CHAPTER 1

Introduction

This chapter aims to contextualize the research, present the motivation for performing it, as well as identifying the problem and objective of this study. This chapter also includes the outline of the remaining thesis in Section 1.4.

1.1. Motivation

In the realm of cybersecurity Incident Response (IR), effective Knowledge Management (KM) stands as a key factor for proactive handling of cyber threats. Authors from [1], [2], and [3] underscore the significance of leveraging knowledge to proactively address potential security breaches, thereby reducing risks like financial loss, damage to reputation, and threats to personnel safety. According to IBM's *Cost of a Data Breach 2023 Report* [4], organizations equipped with IR teams and regularly tested Incident Response Plans (IRPs) experienced an average data breach cost that was USD 1.49 million lower compared to organizations lacking such teams and IRPs.

Incident Response Plans demand well-structured strategies encompassing pre-incident preparation, real-time detection, response actions, and post-incident recovery measures. Swift adaptation to the evolving attack vectors and immediate counteraction remains imperative [5]. Authors from [6] emphasize the need for a comprehensive understanding of security incident management concepts to reinforce response effectiveness.

Leveraging knowledge for proactive IR lies in the practical application of a Knowledge Management System (KMS) within existing frameworks and workflows. Organizations can focus on how to integrate KMS [7] into their current IR processes while addressing issues related to data interoperability, knowledge sharing, and continuous improvement [8]. This involves not only the technical integration of systems but also fostering a culture that values and promotes the use of shared knowledge in everyday IR practices. While the significance of a KMS in IR is recognized, the disparity in the application of these systems to pragmatic cybersecurity challenges is in need of further investigation.

1.2. Problem

Organizations face challenges such as limited resources and expertise contributing to a shortage of skilled cybersecurity professionals [9][10]. This shortage disproportionately impacts smaller entities lacking specialized Security Operations Centers (SOCs), making them more vulnerable [11]. Larger companies have SOCs, and personnel dedicated to this activity. However, smaller companies lack the capabilities and specific knowledge repositories for SOCs, unlike larger companies [12].

With this context, KM emerges as a vital organizational asset [10], by enabling the sharing and application of insights to address incidents promptly. It aids in fortifying cyber resilience, reducing costs, and augmenting operational efficiency [7] [12]. Despite significant investments in KM capabilities, the escalating nature of cyber threats demands continual reassessment of tools and strategies [5]. Also, transitioning from reactive to proactive cybersecurity requires updated IT resources and a concerted effort in advanced threat detection and countermeasures [13]. Additionally, the scarcity of cybersecurity professionals globally underscores the urgency to comprehend and address the skills gap through robust education and training programs [14]. According to the (ISC^2) Cybersecurity Workforce Study [14], the gap grew by 13% from 2022, which means that in 2023 there are roughly 4 million cybersecurity professionals needed worldwide.

Given these challenges, cybersecurity IR demands a robust KMS to counter evolving threats effectively, and they play the critical role of knowledge dissemination and continuous skill development, which needs to be implemented and improved in Computer Security Incident Response Teams (CSIRTs) and SOCs.

1.3. Objetive

This research conducts a Systematic Literature Review (SLR) to gain a comprehensive understanding of the current use of KMS in cybersecurity IR, analyze the concepts of knowledge utilization and management, and subsequently address the identified gaps. The following Questions (Qs) are answered to help identify what the current employment of KMSs is:

Q1: What are the types of knowledge used for cybersecurity IR?

Q2: How is knowledge managed for cybersecurity IR?

Q3: Are KMS used for cybersecurity IR?

Additionally, this research aims to propose a conceptualized model of a KMS specifically tailored for cybersecurity IR. The goal is to promote collaboration, enhance knowledge exchange and improve incident management across organizations, addressing the gaps identified in Section 1.2.

A Design Science Research (DSR) methodology is used to achieve this. The research focuses on creating a proof of concept for a collaborative KMS that facilitates the capture and dissemination of cybersecurity response playbooks. This model aims to answer the following research question:

"Is it possible to specify and design a KMS to help low resource organizations respond to cyber incidents in a collaborative manner?"

1.4. Contributions

This research makes a significant contribution to the domain of cybersecurity by introducing a validated, collaborative KMS model specifically crafted for IR. By identifying the possibility to help low resource organizations respond to cyber incidents, facilitating effective knowledge sharing, improving proactive IR procedures and encouraging continuous learning, this model establishes the foundation for future progress in enhancing cybersecurity resilience.

1.5. Communication

Out of the research presented, an article is being prepared for submission and publication in the Journal of Knowledge Management.

1.6. Dissertation Structure

In Chapter 1 the motivation, research problem, the objectives and main contributions of this research are exposed.

The remainder of the research is structured as follows. Chapter 2 describes the State of the Art conducted through a SLR to identify the current use of KMS in the cybersecurity IR and analyze what knowledge is used and how it is managed for the respective effect. Chapter 3 outlines the methodology implemented and its application in the research process, as well as a detailed description of the artifact' design. Chapter 4 provides the artifact' evaluation, conducted through semi-structured interviews. The findings are deliberated in Chapter 5 presented with the concluding remarks.

CHAPTER 2

State of the Art

The focus of this research is to propose a KMS for cybersecurity IR. Prior to developing the system's design, an initial search for related work was performed, based on the SLR methodology [15], in order to identify any existing studies related to these topics. Section 2.1 offers a conceptual foundation on these subjects. While section 2.2 covers what types of knowledge are used, how knowledge is used and what KMS exist for IR in the cybersecurity domain.

2.1. Theoretical Background

This section provides a theoretical background for the topics discussed in this research, namely IR and KM.

2.1.1. Incident Response

In cybersecurity practices, IR involves the set of processes and technologies employed by an organization to detect and address cyber threats, security breaches, or cyberattacks. The National Institute of Standards and Technology (NIST)[1] defines IR as "the mitigation of violations of security policies and recommended practices", referring incidents might arise from internal incidents, cyberattacks and policy violations. This article [16] states that the primary objective of IR is to proactively prevent cyberattacks and mitigate the impact and disruption to business operations resulting from such incidents.

Organizations develop formalized IRPs to outline the specific processes and technologies for identifying, containing, and resolving different types of cyberattacks. This plan serves as a comprehensive guide for IR activities [17]. A well-executed IRP is crucial for cybersecurity teams as it enables prompt detection and containment of cyberthreats, expedites the restoration of affected systems, and minimizes financial losses, regulatory penalties, and associated costs resulting from these threats.

[1] https://www.nist.gov

Effective IR allows organizations to mitigate the impact of cyberattacks, protect sensitive information, and maintain business continuity. By following established IR frameworks such as the NIST [18] and Sysadmin, Audit, Network, and Security (SANS)[2] [19], organizations can ensure a systematic and efficient approach to incident handling [20]. The execution of IR activities is contingent upon an organization's IRP. Typically, these plans are created and executed by a CSIRT, composed of stakeholders from various organization sectors. This includes the chief information security officer (CISO), SOC, the information technology (IT) personnel, as well as representatives from executive leadership, legal, human resources, regulatory compliance, and risk management.

It is not uncommon for the CSIRT to develop distinct IRPs tailored to different types of incidents, given that each type necessitates a unique response. The IBM 2021 Cyber Resilient Organization Study [21] reveals that most organizations possess specific IRPs addressing DDoS attacks, malware and ransomware incidents, and phishing, with nearly half of them also formulating plans to combat insider threats.

Certain organizations increase their in-house CSIRTs by engaging external partners to provide IR services. These partners are often retained on a contractual basis and help in various aspects of the incident management process, including the preparation and execution of IRPs.

According to [22], a cybersecurity playbook is composed of several building blocks that collectively develop an action plan to be used before, during, and after a cyberattack. It includes crucial and common steps for preparing, assessing, and dealing with incidents, as well as best practices to handle similar incidents and security threats. Providing a detailed workflow to mitigate or respond to specific incidents is not always intuitive and requires a significant effort from cybersecurity analysts and experts. A playbook contains the rules associated with the execution of an IRP [1].

2.1.2. Knowledge Management

In organizational contexts, KM refers to the processes and strategies implemented by organizations to effectively capture, store, transform, and transfer knowledge among individuals and units within the organization. It involves the use of information and communication technologies, as well as the creation of a corporate culture that promotes sharing and collaboration [23] [24]. The goal of KM is to enhance the organization's ability to learn from its environment, incorporate knowledge into business processes, and make informed decisions [25] . It encompasses various practices such as retaining, analyzing, organizing, enhancing, and sharing insights and experiences [26] .

[2] https://www.sans.org/emea/

To support the mechanisms and processes involved in knowledge management, KMS are used to support the mechanisms and processes involved in knowledge management. By effectively managing knowledge, organizations can improve their ability to adapt, innovate, and achieve sustainable advantages. However, there are challenges in bridging the gap between the department responsible for IR and the department responsible for applying knowledge throughout the company. One common type of KMS in organizations is the Information Security Management System (ISMS) [25].

2.2. Systematic Literature Review

A SLR is a comprehensive and methodical approach to evaluate, summarize and interpret all research relevant to a particular investigation, subject, or field. Following the principles of repeatability described in [27], this approach adopts the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)[3] framework (Figure 1) to explain our rationale for the decisions taken on the search strategy, sources, eligibility criteria, selection process, and how the studies were analyzed [15]. PRISMA is now a common technique used in cyber security research [28].

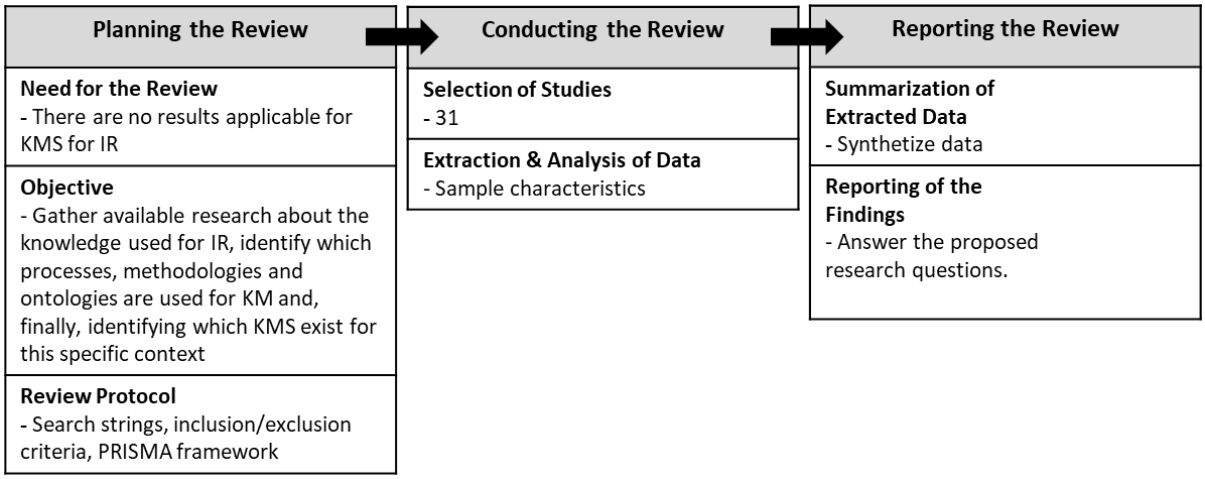


Figure 1. Phases of the SLR.

2.2.1. Literature Review Methodology

The review protocol consists of redefining the keywords appropriately derived from the research questions and their combination in several ways to search for the more adequate studies. The research is conducted interactively refining the search words. After the refinement process, the returned papers are reviewed using the screening criteria (Table 1).

[3] http://www.prisma-statement.org

Table 1. Description of inclusive and exclusive criteria.

Inclusion	Exclusion
(1) – Full Text	(1) – not Full Text
(2) - Abstract	(2) - Not in Abstract (3) – Duplicates and repeated studies
(4) - Relevance to the use of KMS for Cybersecurity IR, within the Abstract that could include: - KMS and IR - Automation of IR - Detection of incidents for IR	(4) - Non relevance to the use of KMS for Cybersecurity IR, within the Abstract: - Training & Awareness

The scientific databases considered for the search are Scopus[4] Web of Science[5], IEEE Xplore Digital Library[6], and ACM Digital Library[7].

The initial identification is done by applying the search string in each database applied to the study full text. After that, the screening considers the initial inclusion and exclusion criteria Table 1. Finally, the included articles are manually selected as the relevant studies based on their abstract and corresponding criteria.

The entire review protocol is represented in Figure 2.

2.2.2. Data Collection

This sub-section is part of the second phase of the SLR methodology (Conducting the Review) and describes the application of the review protocol and analysis of the extracted data.

[4] https://www.scopus.com/
[5] https://www.webofknowledge.com
[6] https://ieeexplore.ieee.org/
[7] https://dl.acm.org/

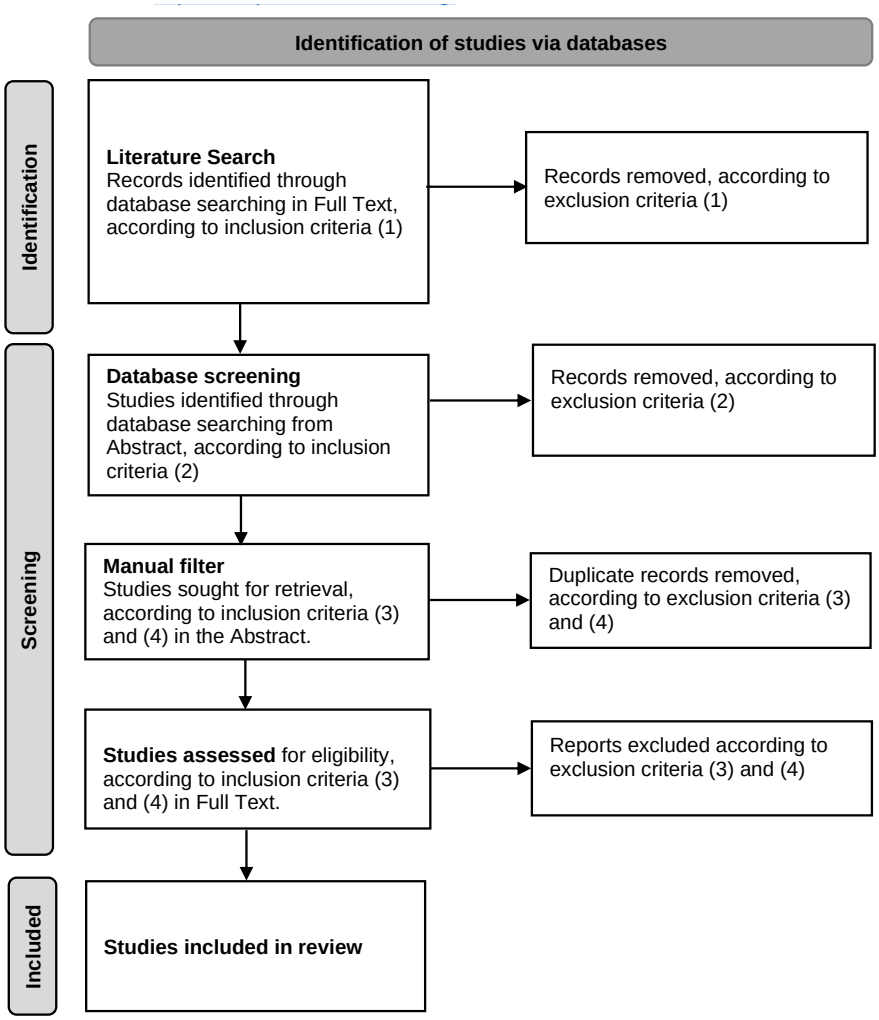


Figure 2. Review Protocol.

The search terms used were refined iteratively. The terms which naturally link to the topic ('knowledge management system' and 'incident response') were tailored according to the results. An example of a search refinement was as follows: the term 'knowledge management system' returns no results related to cyber security; therefore, terms such as 'knowledge management system', 'knowledge management', 'knowledge system', 'knowledge graph', 'knowledge sharing', 'knowledge representation' and 'expert system' were used. After this refinement process, the final search string was defined, which combined several critical search terms: ((“knowledge*” OR “expert system”) AND “incident response” AND (cyber OR security)), as represented in Table 2.

Table 2. Description of keywords and search string.

Keywords:	'knowledge management system', 'knowledge management', 'knowledge system', 'knowledge graph', 'knowledge sharing', 'knowledge representation' and 'expert system'
Search String:	((“knowledge*” OR “expert system”) AND “incident response” AND (cyber OR security))

The results of the database searches identified 5,209 full text studies, which were then screened according to exclusion criteria 2–4, in Table 1. Firstly, only 156 were identified through searching from the Abstract. These remaining studies were sought for retrieval from which 54 were duplicate studies. Titles, abstracts and keywords were reviewed for the remaining 102 articles to assess their relevance in answering the research questions, where 62 articles were not relevant for the research and 8 were Training & Awareness related. This resulted in 70 studies being excluded and another 16 excluded after a full-text review, leaving 15 papers selected through the initial search.

Figure 3 synthesis the selection of studies process through the databases search, based on the PRISMA framework.

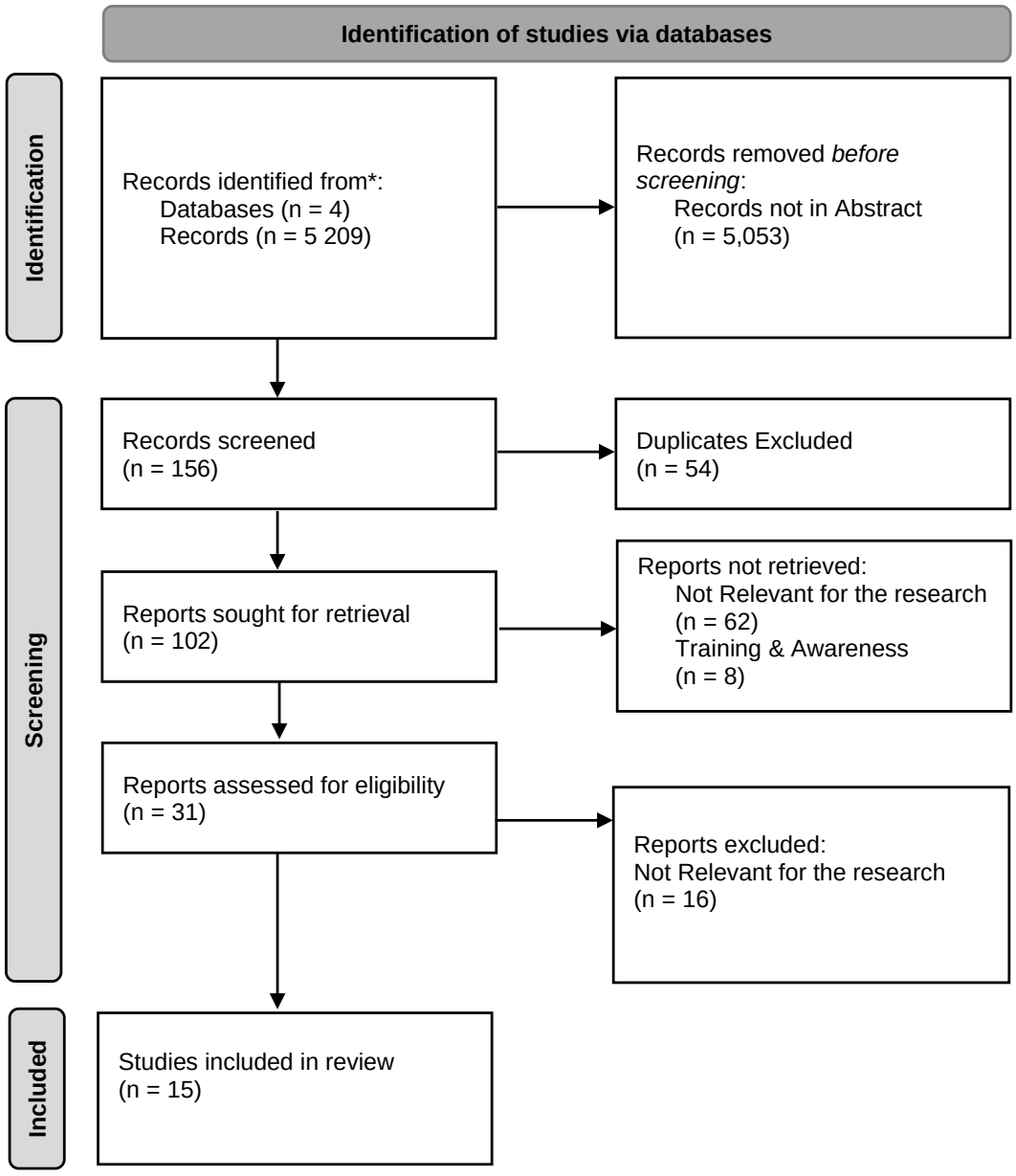


Figure 3. Stages of the studies selection process.

After the screening process, which resulted in 31 articles, all relevant data were extracted and analyzed to summarize information, including title and authors; year of publication; type of article (journal or conference); the name and quality rank of conference or journal; and answers to the research questions.

Among the 31 articles, the distribution of conference papers is predominant, representing about 60% of selected studies, as shown in Figure 4. Although no date criteria were considered in the filtering process all articles were published after 2015, which indicates the early stage of this research topic (Figure 5). Moreover, the evolution of the number of articles published per year shows an increase of publications in recent years (note that 2023 only reflects articles published until October, when this research was conducted), which indicates a growth in interest in using KM techniques in cybersecurity IR.

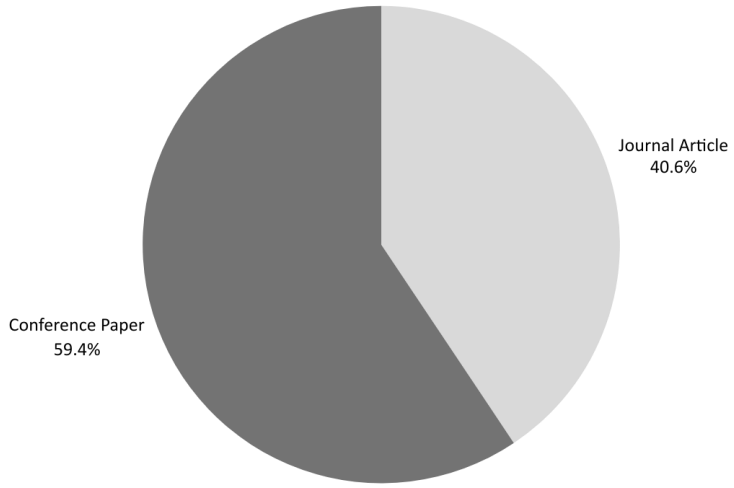


Figure 4. Distribution of selected journal and conference articles.

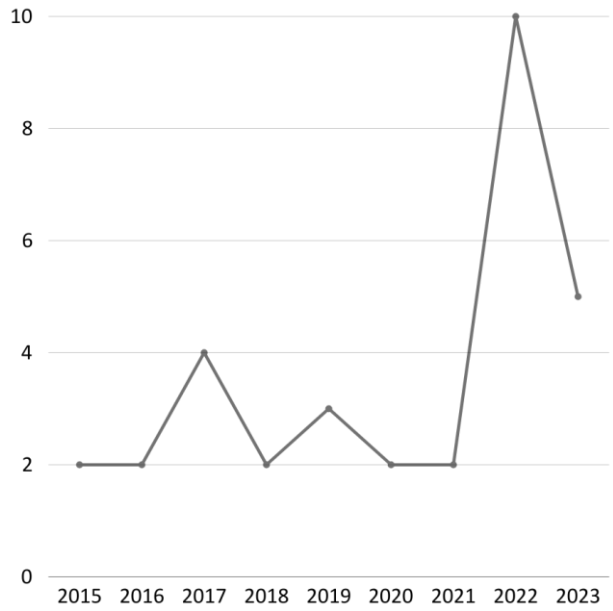


Figure 5. Distribution of selected articles by year.

It is important to note that all the articles removed for the eligibility phase were excluded because they did not answer the research questions. However, their relevance to the topic is highlighted in this sub-section.

2.2.3. Literature Review

In this sub-section the Research Questions (Q1 to Q3) were answered, together with the overall conclusions and identified gaps.

2.2.3.1. Q1: What are the types of knowledge used for cybersecurity IR?

The analysis of the selected articles showed what types of knowledge are in fact used for IR. The diverse topics identified were aggregated from the knowledge originated from IR Frameworks and Playbooks, Knowledge Bases, Knowledge Representation, Cyber Threat Intelligence (CTI) and Artificial Intelligence (AI)-based detection systems and machine learning techniques.

Table 3 shows the distribution of articles by each mentioned category and identifies that there are few articles that focus on each type of knowledge employed. Since IR knowledge is an aggregation of proactive measures, structured frameworks, collaborative sharing initiatives, semantic web utilization, CTI, and technological advancements, the integrated approaches reinforce IR capabilities as a whole and make use of multifaced portfolio of knowledge for fortifying cybersecurity against evolving threats.

Table 3. References of approaches for each identified type of knowledge used

Types of Knowledge	**Articles**
Procedural	[16], [29]
Explicit	[22] , [25]
Semantic	[1] , [20], [30]
Technical	[29], [31], [32]
Analytical	[33], [34]

Based on Table 3, the types of knowledge used for IR, can be categorized as Procedural Knowledge, Explicit Knowledge, Semantic Knowledge, Technical and Analytical Knowledge.

Procedural knowledge contained in the use of IR Frameworks and Playbooks is motivated by a holistic approach in the E-commerce sector, outlined in [15], aiming not only to rectify current issues but also to prevent future attacks by eliminating vulnerabilities, and deploying automated response plans for incident handling. This aligns closely with the automatic digital forensic model proposed by [29], which integrates evidence collection, analysis, anomaly detection, and incident reporting based on the NIST IR lifecycle framework, such as signatures of malware, indicators of compromise (IoCs), malicious payload patterns, or malicious domains. Additionally, using a knowledge base housing traces of such attacks for efficient incident reporting and proactive protection against similar attacks, using a feedback mechanism.

Knowledge Bases, considered explicit knowledge, can contain incident records, such as proposed by [25] the incident's date and time, description, cause, route of occurrence, severity, incurred damages, detection and analysis reports, containment, eradication, and recovery measures. Additionally, it includes specifics on divisional countermeasures introduced, costs associated with preventing future incidents, requests for external countermeasures, and remarks highlighting crucial points for consideration.

Moreover, the significance of shareable playbooks in IR, as advocated by [22], demonstrates the importance of structured frameworks like MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) [8] for incident mitigation. This emphasizes the collaborative effort, highlighted in [19], stressing the importance of structured IR frameworks such as NIST and SANS, fostering information sharing and enhancing defensive strategies within the cybersecurity community such as:

- analyzing and correlating security logs for data-driven incident analysis;
- implementing containment, remediation, and recovery strategies post-incident detection;

[8] https://attack.mitre.org

- utilizing monitoring and detection capabilities to identify early warning signs of compromise;
- Conducting regular training and tabletop exercises to improve team readiness;
- Maintaining an up-to-date enterprise IR policy and well-documented procedures.

Knowledge Representation trough semantic knowledge and web technologies, showcased in [22] and [30].

Additionally, the significance of the technical knowledge discovered in CTI, emphasized by [31]

The utilization of analytical knowledge provided by AI-based detection systems and machine learning techniques, as advocated by [33] and [34], emphasizes the importance of real-time anomaly detection and efficient malware analysis, complementing the proactive and preventive strategies in IR elucidated in various references.

2.2.3.2. Q2: How is knowledge managed for cybersecurity IR?

Incident Response knowledge management integrates structured frameworks, ontology-driven systems, graph-based analytics, AI techniques, updated repositories, continuous learning frameworks, and team coordination models. These collective approaches are presented in Table 4 to summarize the existing literature.

Table 4.References of approaches for each identified use of knowledge.

Use of Knowledge	Articles
IR Framework and Playbooks	[1], [16], [22], [35]
Knowledge Bases	[8]
Knowledge Representation	[31], [36]
CTI	[37]
AI-based detection systems and machine learning techniques	[34]

In the domain of IR, managing knowledge is a comprehensive process that covers multiple methodologies and systems aimed at handling security incidents. It was not found a common approach to responding to incidents effectively.

Article [16] highlights the significance of structured IR frameworks, emphasizing the creation of playbooks and incident handling plans. This aspect underlines the pivotal role of information sharing and proactive measures in fraud prevention, particularly in the E-commerce context.

The Semantic web-based Approach for management of Sharable cybersecurity Playbooks (SASP) framework proposed by [22] introduces a playbook manager Graphical User Interface (GUI), streamlining the management of playbooks and their components. This tool emphasizes the need for user-friendly interfaces in efficiently managing IR knowledge.

Ontology-driven systems leveraged by IR, as illustrated by [1], such as OnSOAP, which integrates semantic interpretation of security system capabilities and IR processes. This sophisticated approach enables automated IR processes.

Graph-based analysis, as highlighted by [35], formalizes the Threat Hunting process, aiding in refining IoC and Events of Interest (EoI), consequently enhancing the efficiency of IR.

The Automatic Incident Responder (AIR) methodology introduced by [31] combines attack hypothesis generation with IR, providing automated defense suggestions based on graph-based analytics. This emphasizes the role of automated response strategies in promoting IR capabilities.

Knowledge bases like Collaborative Analysis Engine for Situational Awareness and Incident Response (CAESAIR), as detailed in [32], store up-to-date information, facilitating quick assessment of cybersecurity situations and suggesting resource clusters. This signifies the pivotal role of updated repositories in bridging knowledge gaps within IR teams.

Article [25] proposes a structured incident learning approach through the Delta ISMS, fostering a repository for 'learning from incidents' and promoting company-wide knowledge transfer.

The utilization of AI techniques, network traffic analysis, and specialized IR frameworks, outlined by [34], accentuates the importance of proactive and reactive analysis in IR, promoting continuous monitoring and knowledge-driven responses.

The Tactics, Techniques and Procedures (TTP)-based framework introduced by [8] aids in cybercrime investigation by mapping incidents and guiding investigative actions. This systematic approach enables the collection, analysis, and annotation of cybercrime cases with new evidence.

Moreover, [36] showcases how the Malware Information Sharing Platform (MISP) platform serves as a repository for IoCs and threat data, supporting incident analysis and mitigation by providing strategic countermeasures and enhancing incident understanding through threat data correlation.

Lastly, [37] demonstrates how CSIRTs manage knowledge through shared mental models, adaptive thinking training, and after-action reviews, enhancing team understanding, coordination, and adaptability during crises.

2.2.3.3. Q3: Are KMS used for cybersecurity IR?

Lastly, Table 5 presents the by each identified aspect of KM that can be integrated in a robust KMS.

Table 5. References of approaches for each identified aspect of KM.

Aspects of Knowledge Management	Articles
Use of playbooks	[1], [16],[22]
Semantic knowledge	[1], [22], [36]

Aspects of Knowledge Management	Articles
AI and machine learning	[30], [31]
Knowledge sharing and collaboration	[20], [25]
IR Systems	[16], [17]
Threat Intelligence Frameworks	[31], [37]

As retracted in the last research questions the IR landscape is diverse, with various methodologies and frameworks focusing on different aspects of incident handling and knowledge management. Even though, there are no results closely related to KMS, one recurrent theme is the utilization of playbooks or incident handling plans [1], [16] and [22]. These playbooks encapsulate a sequence of actions, best practices, and procedures for responding to specific incidents, contributing significantly to KM in IR.
Moreover, semantic knowledge plays a pivotal role in many systems [1], [22] and [36]. Leveraging semantic web technologies like Resource Description Framework (RDF), Resource Description Framework Schema (RDFS), and Web Ontology Language (OWL) helps in formalizing incident-related knowledge, establishing relationships, and enabling standardized queries and reasoning, thereby facilitating more efficient incident handling.

Several frameworks and models integrate AI and machine learning [30], [31], [33] and [34] for incident detection, classification, and response. These systems contribute significantly to automating certain aspects of IR, enabling quicker and more accurate identification of threats.

Knowledge sharing and collaboration among various stakeholders and within SOCs are crucial aspects highlighted by [20], [25] and [32]. This emphasizes the importance of information dissemination, communication, and continuous learning from incidents for better preparedness and response.

Additionally, IR systems often incorporate specialized tools for incident detection, tracing, and analysis [16], [17]. These tools range from tracing software to security patches and resource kits, empowering incident responders with the necessary resources to handle incidents effectively.
The utilization of threat intelligence frameworks such as MITRE ATT&CK [8], [31] and [37] and the incorporation of CTI contribute significantly to understanding adversarial tactics, enhancing IR capabilities, and informing defensive strategies.

Overall, the reviewed literature emphasizes the multifaceted nature of IR and KM in cybersecurity. The integration of playbooks, semantic knowledge representation, AI and machine learning, collaborative frameworks, specialized tools, and threat intelligence collectively form a robust ecosystem for incident handling and response, which result on multiple relevant aspects of KMS.

These systems help organizations effectively mitigate ongoing or future cyberattacks, improve communication and information sharing, and reduce the time taken to restore normal operations [38], [16].

2.2.3.4. Conclusions and identified gaps

The findings highlight the multidimensional nature of knowledge used for IR. Based on the diverse types of knowledge employed for cybersecurity IR, the integrated approaches reinforce IR capabilities and make use of a multifaced portfolio of knowledge for fortifying cybersecurity against evolving threats.

In the domain of IR, managing knowledge is a comprehensive process that encompasses multiple methodologies and systems to streamline the handling of security incidents. It was not found a common approach to responding to incidents. In the cybersecurity domain, IR knowledge management can go from integrating structured frameworks, updated repositories, continuous learning frameworks, and team coordination models to ontology-driven systems, graph-based analytics and AI techniques.

The formal term KMS was never mentioned in any of the articles reviewed. Meaning, the existing literature identifies the gap of a KMS in IR; Therefore, it is evident that further exploration and implementation of such systems are necessary. Specially, an integrated solution that prioritizes enhancing the interoperability of KMS across diverse organizational structures and scaling their implementation to address the ever-evolving threat landscape.

CHAPTER 3

Methodology

In the initial steps of this research, a Literature Review has been conducted to identify the problem of this research, reflected in Chapter 2. This chapter used the activities of DSR proposed in [39] and [40], as the main research methodology.

Following the methodology described in Figure 7. This chapter aims to expose the proposed system design. Semi-structured interviews were conducted with a research specialist in order to define the initial artifact use cases, types of users and requirements, after which the system design was constructed, defined and demonstrated. The final goal of this method was to be able to answer the research question: *Is it possible to create a KMS to help organizations respond to cyber incidents?*

3.1. Design Science Research

The DSR methodology, proposed by Peffers K et. Al [39], is going to be followed. DSR is used in Information Systems (IS) research to improve knowledge bases by developing new solutions that solve problems while also improving the environment in which they are implemented [40]. Based on [39], the process model for presenting and evaluating the DSR in IS that was used, is shown in Figure 6.

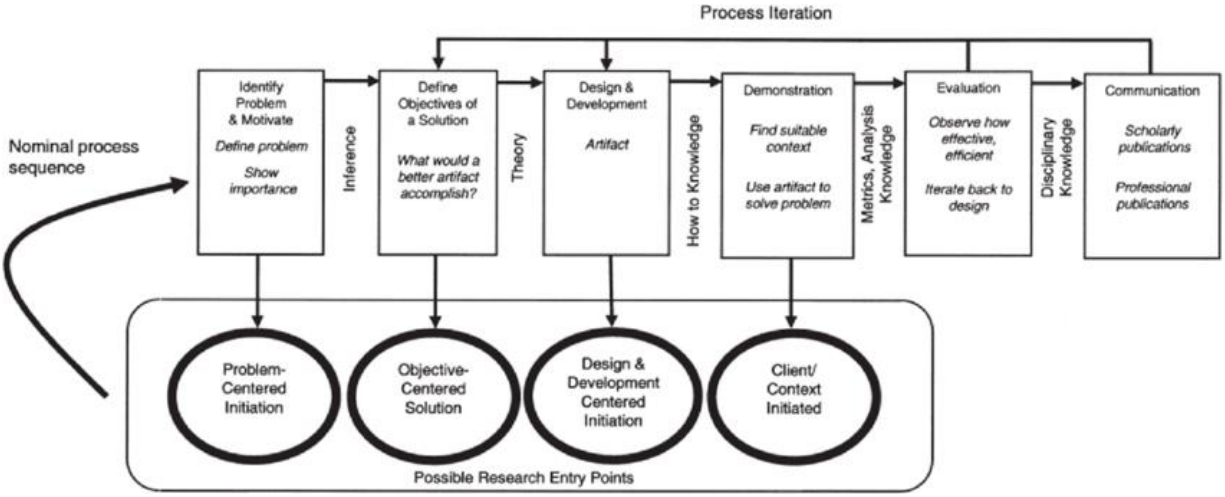


Figure 6. DSR Methodology Process Model.

The DSR process model is composed of the following steps:

1. Identification of the problem and motivation.
2. Definition of objectives for a solution.
3. Design and development.
4. Demonstration.
5. Evaluation.
6. Communication.

Initially, the procedure begins with the identification and delineation of the research issue, underscoring the significance of the resolution. Subsequently, the second step involves defining the objective for the proposed solution. The third step entails designing and developing the artifact, specifying its desired functionality and architecture. Following this, the fourth step demonstrates how the artifact solves instances of the research problem.

The fifth step involves evaluating the solution by comparing the achieved results against predefined goals. Lastly, communication of all aspects concerning the problem, and the designed artifact occurs with relevant stakeholders, which could be fellow researchers or professionals in the field.

Additionally, the DSR process presents four distinct entry points for different research approaches. These include the problem-centered approach, objective-centered solution, design and development-centered approach, and the client/context-initiated solution. Each entry point serves specific research needs, depending on the situation and existing conditions.

In the specific work described, the problem-centered approach was employed, given the pre-existing knowledge of the addressed problem (sub-section 2.2.3). This approach is detailed in Figure 7 of the study.

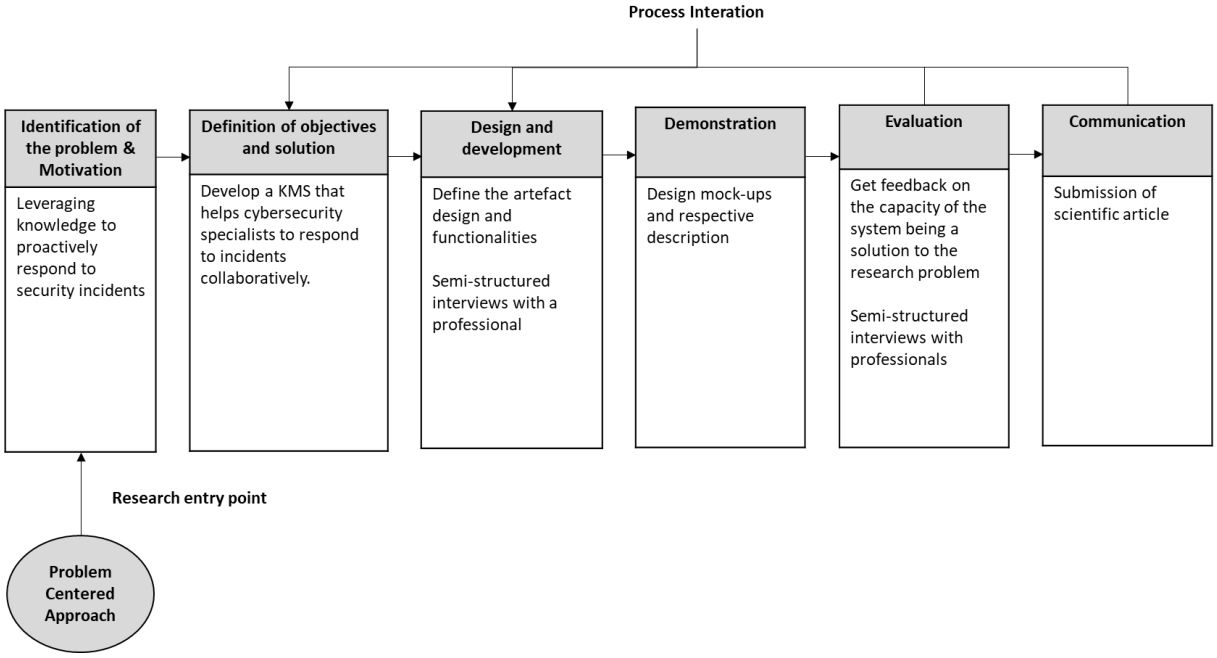


Figure 7. DSR Methodology adapted to the specific work.

3.2. Definition of objectives and solution

This research focuses on the development of a KMS for cybersecurity IR, developing a design artifact and its respective functionalities. As referred in [40], scientific research needs to be characterized by abstraction, originality, justification, and publication. This is necessary to be distinguished of the way that solutions are developed by organizations or practitioners' communities. In Table 6 we describe the principles of the research.

Table 6. DSR Principles applied to the specific work.

DSR Principle	Explanation
Abstraction	The research consists of proposing a design artifact and functionalities for enhancing collaborative IR.
Originality	The design of a KMS for playbook edition and collaboration is not in the known body of knowledge (sub-section 2.2.3).
Justification	The multidimensional aspect of knowledge used in IR has its complexity and the necessity for varied strategies. Ontology-driven systems already help organize and categorize knowledge, making it more accessible and easier to retrieve when needed. For now, the interoperability of a system used to manage this information across different organizational structures is in lack. Expert(s) were interviewed and addressed concerning the proposed system alongside its possible implementation.
Benefit	Proactive approach to IR, ensuring preparedness and quicker response and recovery from cyber incidents.

In this study we follow the DSR guidelines proposed by [40] as described in Table 7. These practice rules, when followed, assure that the DSR achieves its purpose: the creation of an artifact that expand the limits of human capabilities and organizations.

Table 7. DSR Guidelines applied in the specific work.

Guideline	Description applied to the KMS
Guideline 1: Design as an artifact	The artifact is a KMS design of playbook creation, edition and collaboration for cybersecurity IR procedures.

Guideline	Description applied to the KMS
Guideline 2: Problem relevance	Help cybersecurity specialists to manage incident knowledge and respond to incidents collaboratively.
Guideline 3: Design evaluation	Utility, quality and efficacy on responding to incidents. Evaluated by semi-formal interviews to specialists on the demonstration of functional use cases (mock-ups).
Guideline 4: Research contributions	KMS design and documentation verified by experts. Gap filling on the research topics.
Guideline 5: Research rigor	DSR relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a search process	Iterations with 1 research specialist feedback
Guideline 7: Communication as research	Publication of the research

3.3. Design and development

The development of playbooks is typically carried out independently by organizations, often utilizing frameworks such as those provided by NIST and SANS as foundational guidelines. According to [41], these frameworks can be applied in two separate manners:

- Static processes - which consists of documented procedures detailing the tools to be used, the steps to be executed, and the individuals responsible for carrying out each task.
- Dynamic processes - which involve scripts that interact with relevant systems and tools to execute predefined actions in response to alerts. These automated processes are commonly referred to as runbooks.

A playbook must include an initial trigger condition, such as an alert or the detection of an incident, followed by a sequential series of steps. These steps typically involve triage, analysis, containment, and remediation actions. The playbook's goal is to achieve a predefined outcome, which signifies its completion.

In addition to playbooks, IR platforms can be employed. These platforms are software tools designed to guide, support, and automate IR efforts. They often offer comprehensive integration with existing systems and provide various functionalities. The common features of IR platforms include:

Table 8. Common features of IR platforms.

Analytical Support	Intelligence and analytics	Security automation
-Knowledge Base of regulations, response plans, and contacts -Automatic escalation and assignment of alerts - SLA tracking -Compliance and breach reporting	-Integration with Security Information and Event Management (SIEM) and other monitoring tools -Analysis and correlation of event timelines -Real-time attack behavior analysis -Forensic data retention and querying	-Pre-configured IR playbooks -Support for customizable playbooks -Automatic isolation of compromised systems or user accounts -Automatic remediation

As illustrated in sub-section 2.2.3, various methodologies and systems exist to enhance the efficiency of managing security incidents. Playbooks represent a series of prescribed actions, optimal approaches, and protocols designed to address incidents, thereby playing a crucial role in KM within IR.

A system for IR has been developed to facilitate the sharing, storage, and correlation of playbook information. This sub-section presents the overview of the system's use cases, requirements, types of users expected, design and demonstration steps aligned with the DSR methodology.

The use cases and requirements were defined together with a research specialist to obtain initial information about current approaches, advantages, disadvantages and expectations regarding playbook management. The primary interviews also covered the functionalities definition for the design of the KMS. Overall constraints and challenges of the suggested system were identified with the goal of adding value to the solution, compared to the current approaches, advantages and disadvantages.

3.3.1. Use Cases

To meet the goal of developing a system capable of interacting with the user to provide the knowledge that he needs, the following use cases were defined, aligned with Figure 8 and posteriorly transformed into functional and non-functional requirements described in sub-section 3.3.3:

- User registers and authenticates by email address and password
- User manages its profile

- Tool generates notifications about playbook updates (added comments, feedback and views) and new versions generated to the Playbook owner
- User can search for a playbook for a type of incident
- User wants to search for the top 3 response processes to a type of incident
- User chooses the most suitable playbooks based on other users' feedback and last reviewed playbooks.
- User visualizes and explores visually the playbooks
- Users ask for help from expert users.
- User gives feedback on the playbook.
- User suggests a change to the playbook owner by commenting on the playbook.
- User creates a playbook with assisted recommendations based on the playbooks database.
- User uploads a playbook
- User edits a new playbook version that he takes as playbook owner.
- Playbook owner accesses the user's proposals, validates and performs changes in the playbook

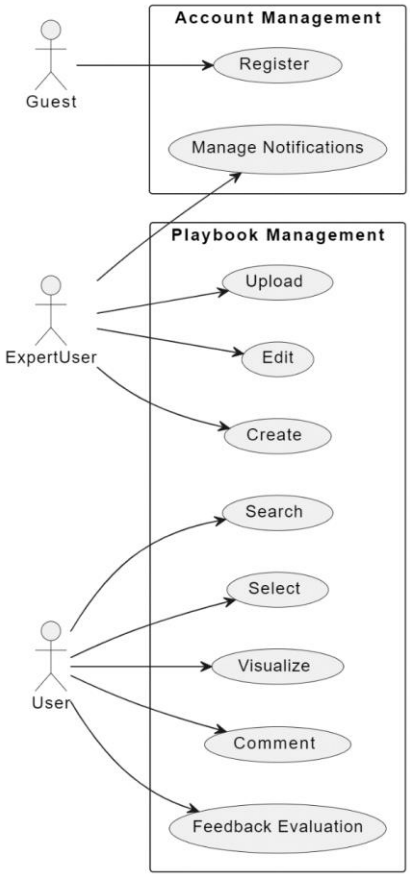


Figure 8. UML Use-case Diagram.

The capability to enable users to input information into the suggested playbooks is essential. This enables users to share insights on handling specific incidents and facilitates collaboration among the users' different profiles. The tool is designed to collect and provide access to playbook knowledge.

3.3.2. Types of Users

There are six types of users foreseen, who have different perspectives of using the system. Represented in Table 9 are the types of users, their proposed use of the system and the Actor represented in Figure 8.

Table 9. Type of users.

Type of user	Description	Actor
Guest	Unregistered user who accesses the platform and intends to explore it. The actor has the lowest level of privileges.	Guest
Learner	Registered user that aims to obtain knowledge from the playbooks and learn from the tool.	User
Collaborator	Registered user that participates in the collaboration of playbooks commenting, viewing and giving feedback.	User
Playbook Owner	Experienced user who creates the playbook (from scratch or new version) and adds knowledge to the system. Additionally, it can propose changes or improvements.	User, Expert User
Playbook Owner Deputy	Assigned by the playbook owner is an experienced user that can perform additional validations, suggestions and updates to the content of the playbook assigned.	User, Expert User
Administrator	Responsible for user's management, platform design, evolution and maintenance	User, Expert User

3.3.3. Requirements

Functional requirements cover the definition of the system's intended actions, particular behaviors, tasks, and functions necessary for fulfilling the defined user requirements. These specifications outline the dynamics between the system and its context, considering users and external systems. Non-functional requirements, conversely, relate to the mechanisms by which the system carries out its functions, encompassing the establishment of the system's quality attributes, performance benchmarks, and operational constraints.

In Table 10 and Table 11, functional requirements were defined, englobing requirements created from the use cases defined in sub-section 3.3.1. Additionally, non-functional requirements were added as a complement to the defined systems requirements to aid the future development of system.

Table 10. Use Cases and Feature Requirements.

Requirement	**Functional**	**Non- Functional**
User Authentication	- Provide a registration form that collects the user's email address and password. - Validate the email address format and password strength. - Send a confirmation email with a link to verify the email address. - Allow users to log in using their registered email address and password. - Provide a password recovery mechanism.	- The registration and authentication processes must complete within 2 seconds on average. - Passwords must be encrypted using a secure hashing algorithm (e.g., bcrypt[9]). - The system must comply with relevant data privacy regulations (e.g., General Data Protection Regulation - GDPR).
User Profile Management	- Allow users to view and edit their profile information, including name, email address, and password. - Allow users to upload a profile picture. - Allow users to join add their organization trough a magic link given to the enterprise. - Save changes and notify the user of successful updates.	- Profile updates must be processed within 2 seconds on average. - Profile information must be stored securely and only accessible to authorized users.
Notification Management	- Send notifications to playbook owners when comments, feedback, or views are added to their playbooks.	- Notifications must be delivered within 1 minute of the triggering event. - The system must ensure notifications are not sent for spam or malicious activities.

[9] https://www.npmjs.com/package/bcrypt

Requirement	Functional	Non- Functional
	- Notify playbook owners and deputy when new versions of their playbooks are generated. - Notify playbook owners and deputy when help requests are generated in the comments. - Allow users to configure their notification preferences.	
User Search	- Provide a search interface based on a recommendation system that allows users to enter keywords. - Allow users to search for the top playbooks by search criteria. - Rank and display the top 3 playbooks based on predefined criteria. - Display feedback ratings for each playbook. - Highlight playbooks that have been recently viewed. - The ranking algorithm must be transparent and explainable.	- Search results must be displayed within 2 seconds. - The search engine must handle large volumes of data efficiently.
User Select	- Allow user to select any playbook displayed - Display user comments for the playbook selected	- Playbook results must be displayed within 2 seconds.
Playbook Visualize	- Provide a graphical interface for users to visualize playbook steps, actions and properties - Allow users to explore playbook details interactively.	- The graphical interface must load within 2 seconds. - The visualization tools must be intuitive and user-friendly.

Requirement	Functional	Non- Functional
Playbook Comment	- Allow users to send help requests to designated expert users (playbook owner and deputy). - Allow users to comment on playbooks to suggest changes. - Allow playbook owner to validate and incorporate changes (edit) the playbook	- The system must track help request responses for accountability. - The system must support threaded comments for better discussion tracking. - Validation and incorporation of changes must be processed within 2 seconds.
Playbook Feedback	- Allow users to submit feedback on playbooks. - Store feedback and associate it with the relevant playbook.	- Feedback submissions must be processed within 2 seconds. - Feedback data must be stored securely and be easily retrievable.
Playbook Creation	- Provide a playbook creation interface with step-by-step guidance. - Offer recommendations based on existing playbooks in the database.	- The creation interface must be intuitive and user-friendly. - Recommendations must be generated within 2 seconds.
Playbook Upload	- Allow users to upload playbooks in various formats (e.g., json, yml, bpmn, .pdf, .docx, .txt). - Validates and store the uploaded playbooks.	- Uploads must be processed within 5 seconds. - The system must support large file uploads without performance degradation.
Playbook Edit	- Allow playbook owners to edit and save new versions of playbooks. - Maintain a version history for each playbook.	- Edits must be saved within 2 seconds. - The history version must be easily navigable.

Table 11. System Requirements.

Requirement	Functional	Non- Functional
Database and Data Management	- Store and manage technical and non-technical playbook information.	- Ensure data consistency and integrity. - Support high-volume data operations with minimal latency.

Requirement	Functional	Non- Functional
	- Support automatic correlation of playbook attributes and sub-playbooks.	
Sharing and Collaboration	- Built-in sharing functionality for various distribution models. - Advanced filtering to meet organizational sharing policies.	- Secure data sharing mechanisms. - Ensure compatibility with different distribution models.
User Interface	-Intuitive interface for creating, updating, and collaborating on playbooks. - Graphical interface for seamless navigation between incidents and playbooks.	- Interface must be responsive and load within 2 seconds. - Ensure accessibility compliance.
Recommendations and Analytics	- Recommendation system for standardized response plans. - Generate statistics on content and user profiles.	- Recommendations and reports must be generated within 5 seconds. - Ensure accuracy and relevance of recommendations.
Import and Export	- Support importing playbooks in multiple formats. - Export playbooks in *bpmn* and *yml* format.	- Import and export processes must be completed within 5 seconds. - Support for large files and complex data structures.
API and Integration	- Flexible API for integration with organizational solutions. - Support feed import and export for various data sources.	- API must handle high volumes of requests efficiently. - Ensure secure data transmission and integration.
Taxonomy and Classification	- Adjustable taxonomy to classify and tag events. - Support sharing of taxonomies among system instances.	- Taxonomy management must be intuitive and flexible. - Ensure compatibility with standard classification schemes (e.g., European Union Agency for Cybersecurity - ENISA[10] and *Centro Nacional de Cibersegurança*

[10] https://www.enisa.europa.eu

Requirement	Functional	Non- Functional
		- CNCS[11])

Additionally, Table 12 describes the requirements for the definition of the roles within the system comparing privileges and restrictions of such.

Table 12. Roles and Permissions.

Role	Privileges	Restrictions
Guest	- Can browse public playbooks. - Can view feedback and comments.	- Cannot create, edit, or comment on playbooks. - Cannot access advanced features.
Learner	- Can search and view playbooks. - Can request help from expert users.	- Cannot edit or upload playbooks. - Limited commenting capabilities.
Collaborator	- Can comment on and give feedback on playbooks. - Can view detailed playbook histories and user feedback.	- Cannot create or edit playbooks directly.
Playbook Owner	- Can create, edit, and delete playbooks. - Can validate and incorporate user proposals. - Can access detailed statistics and reports.	- Subject to validation from PO Deputy.
Administrator	- Full access to all system functionalities. - Can manage users, roles, and platform settings. - Can perform system maintenance and upgrades.	- Must ensure system security and integrity.

3.3.4. Design

This sub-section explains how the Use Cases and Features (Table 10) were transformed into the system's design.

Firstly, modules were defined based on each requirement and aggregated according to Table 13.

[11] https://www.cncs.gov.pt

Table 13. Design Modules based on Use Case Requirements.

Module	Requirements
Login and Sign-up	User Authentication
Playbook Selection	User Search, User Select
Playbook Creation	Playbook Creation, Playbook Upload, Playbook Edit
Playbook Collaboration	Playbook Visualize, Playbook Comment, Playbook Feedback

Afterwards, each module was described according to the system's functionalities, actions, and proposed repositories (Figure 9), and the proposed system is represented using the following figures.

Figure 9. System Design Caption.

In Figure 10, the relationship between the modules is displayed [42].

In the following figures, Functionality refers to the core features or capabilities that the system should provide, including the essential operations that a system must perform to achieve its intended purpose. Actions are specific tasks or steps taken within the functionality to achieve a particular outcome. They represent the user interactions or system responses based on the user's inputs. A Repository represents a centralized location where data or information is stored, managed, and retrieved. In the system design, it typically refers to a database or data storage system that holds persistent information. The repository ensures that the system has access to the necessary data to perform its functionalities.

The Login and Sign-up module, represented in Figure 11, encompasses the user authentication process, which is fundamental to maintaining the system's security and user access control. This module enables users to register and authenticate themselves using their email addresses and passwords. The system verifies the user's credentials and ensures that appropriate data privacy regulations, such as GDPR, are followed. It also incorporates functionalities for password recovery and account validation through email confirmation. This module plays a key role in ensuring that only authorized individuals can access the system and perform tasks such as playbook creation, selection, and collaboration. Therefore, it establishes the essential security and privacy protocols necessary for maintaining the integrity of IR data.

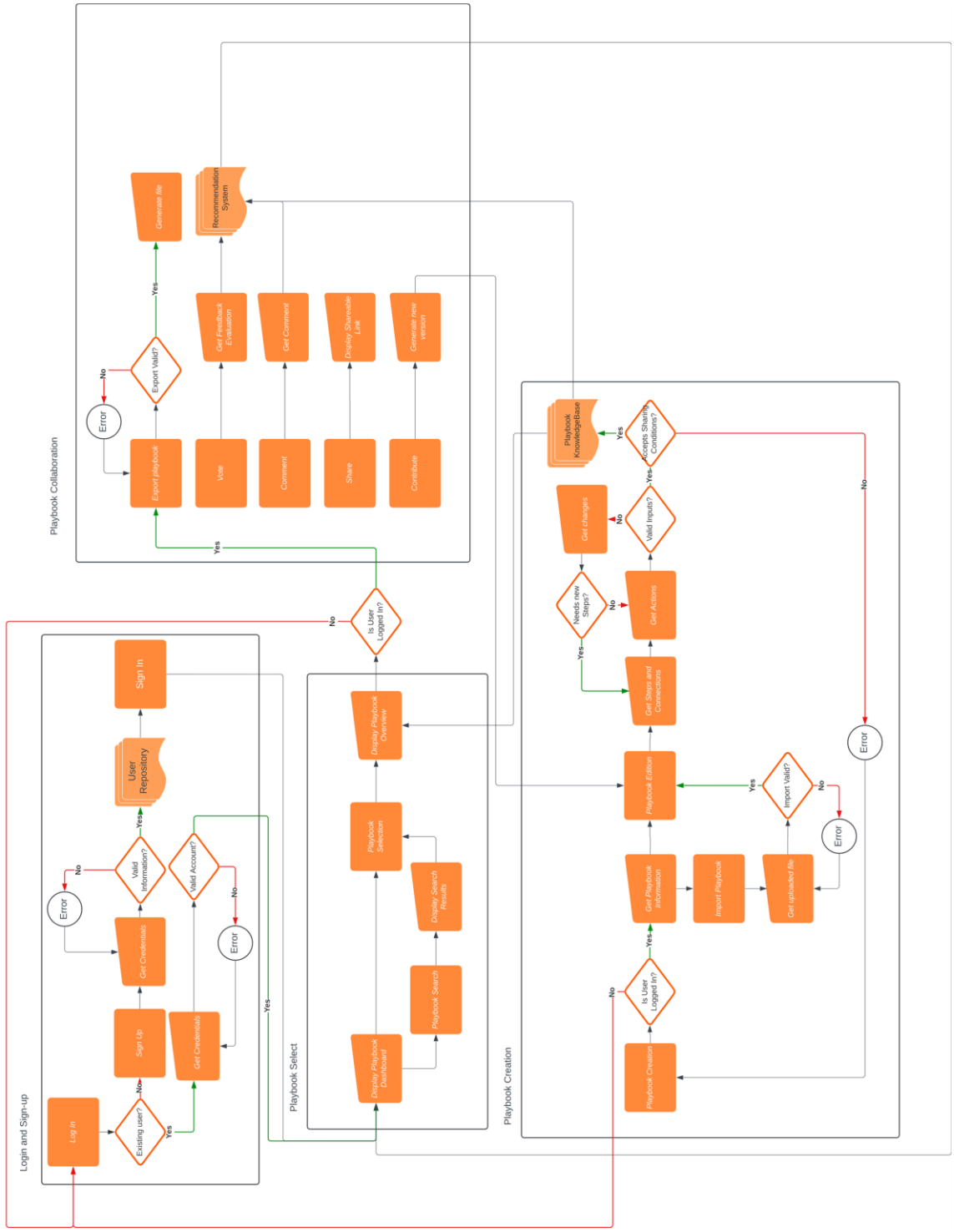


Figure 10. System Design Diagram.

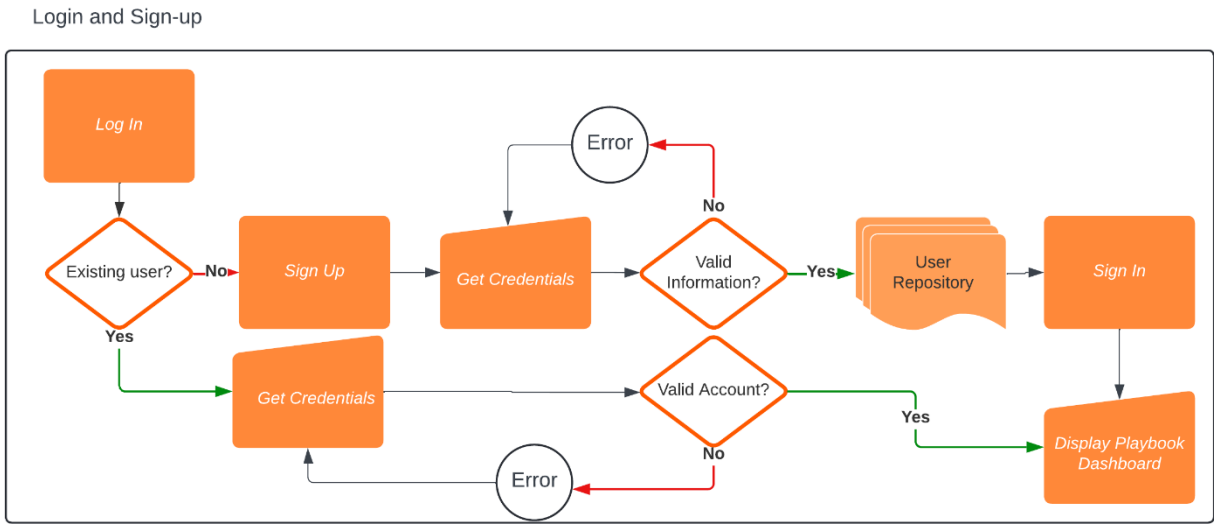


Figure 11. Login and Sign-up module.

The Playbook Selection module, represented in Figure 12, is designed to facilitate user interaction with the playbooks stored within the system. This module incorporates search functionalities, allowing users to search for relevant playbooks based on specific criteria. Once the search results are displayed, users are able to view and select any playbook of interest. The selection process is enhanced by the system's recommendation algorithm, which ranks and highlights the most relevant or frequently viewed playbooks. The integration of user comments within the playbook overview ensures that users are guided in selecting the most appropriate playbooks for their needs. This module supports the system's goal of streamlining access to important IR resources.

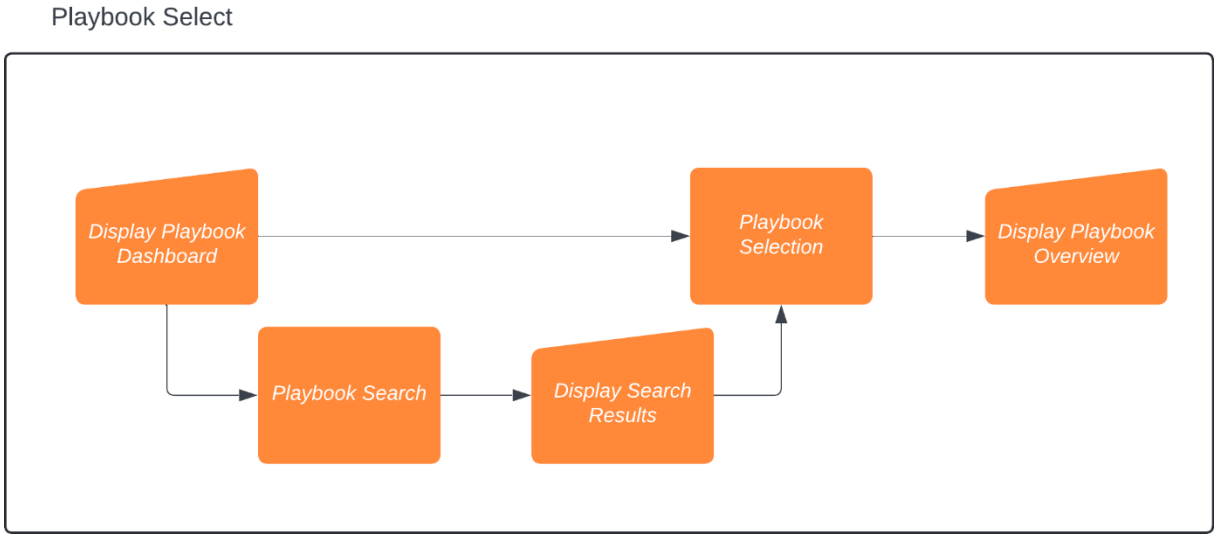


Figure 12. Playbook Selection module.

The Playbook Creation module, represented in Figure 13, supports users in generating new playbooks, as well as modifying existing ones. Users can either create playbooks from scratch or upload playbooks in various supported formats. Once uploaded, the system validates the playbook and stores it within the repository, ensuring the consistency and accuracy of the data. The module also incorporates an editing interface that allows users to update existing playbooks and save new versions. Version control is an integral part of this module, enabling users to maintain a history of edits and revisions, which is particularly important in a collaborative environment where multiple users may contribute to the development of a playbook. This module plays a pivotal role in the dynamic creation and refinement of knowledge artifacts essential for cybersecurity incident response.

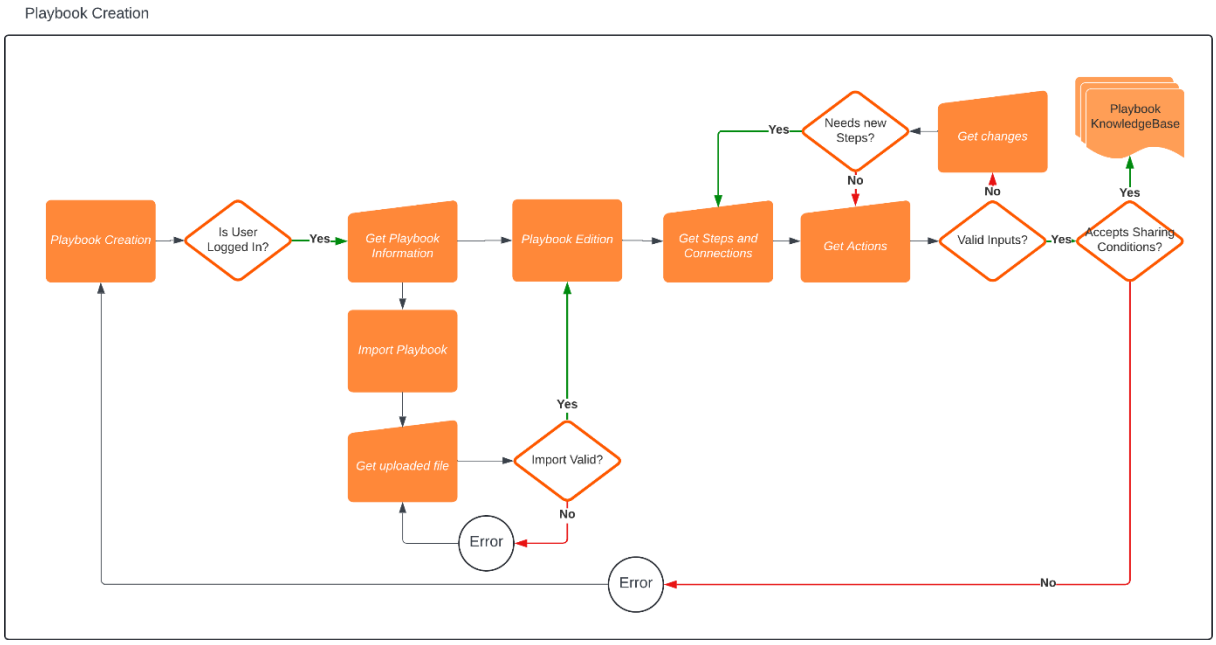


Figure 13. Playbook Creation module.

The Playbook Collaboration module, represented in Figure 14, enhances the collaborative nature of the system by enabling users to interact with playbooks through visualization, comments, and feedback. This module provides a graphical interface that allows users to visualize the various steps, actions, and properties associated with each playbook. In addition to exploring playbook details interactively, users can provide feedback, submit comments, and suggest modifications. Threaded comments ensure that discussions are structured, improving the clarity and traceability of suggestions. Furthermore, playbook owners or designated deputies can validate and incorporate feedback, leading to the generation of new playbook versions. By facilitating real-time collaboration and discussion, this module contributes to the continuous improvement of IR procedures and enhances knowledge sharing among users.

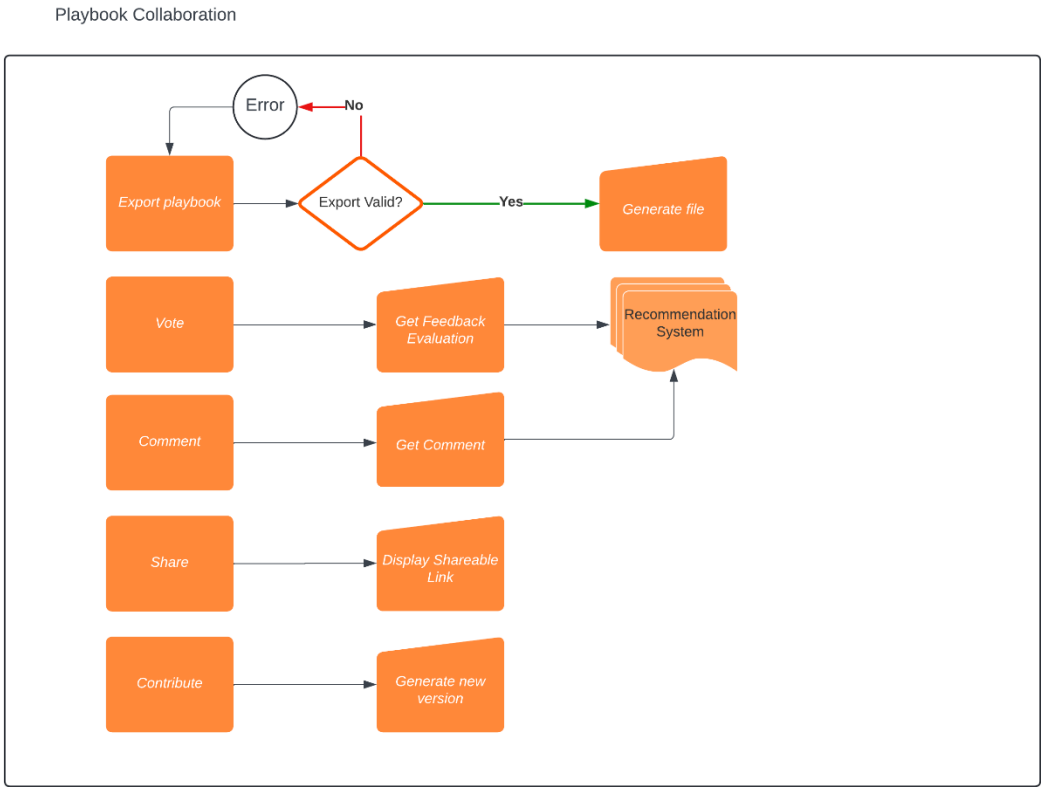


Figure 14. Playbook Collaboration module.

3.3.5. Demonstration

This sub-section describes the expected usability from the users' point of view. To enable the validation of a system design by experts, mockups were developed based on the specifications described on sub-section 3.3.3.

The following mock-ups are a representation of the flows created in Figma [43], based on the *StackOverflow* website and the Collaborative Automated Course of Action Operations (CACAO) roaster project [44], following CACAO Security Playbooks Version 2.0 (https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html). These mock-ups include:

- In Figure *15*, a login page where the user can insert e-mail and password.

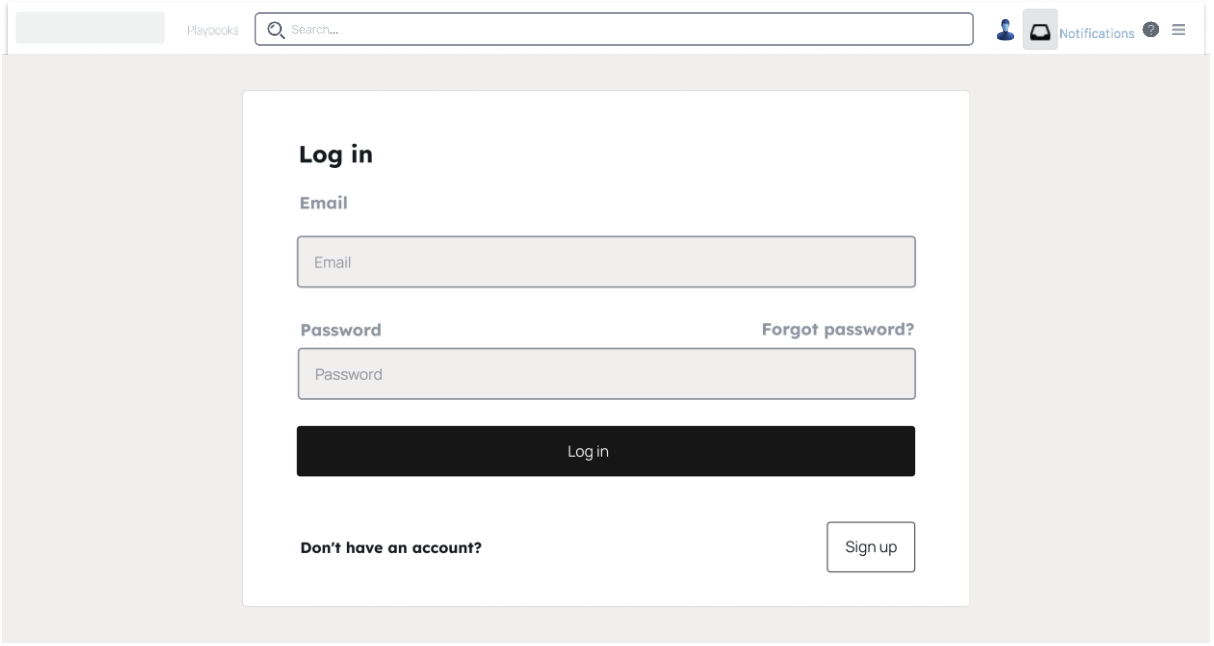


Figure 15. Log in Page.

- In Figure *16* and Figure *17*, a sign-up page where the user can insert First and Last name plus e-mail and password. Followed by a Verification Page where the user can input the code received in the e-mail inputted beforehand.

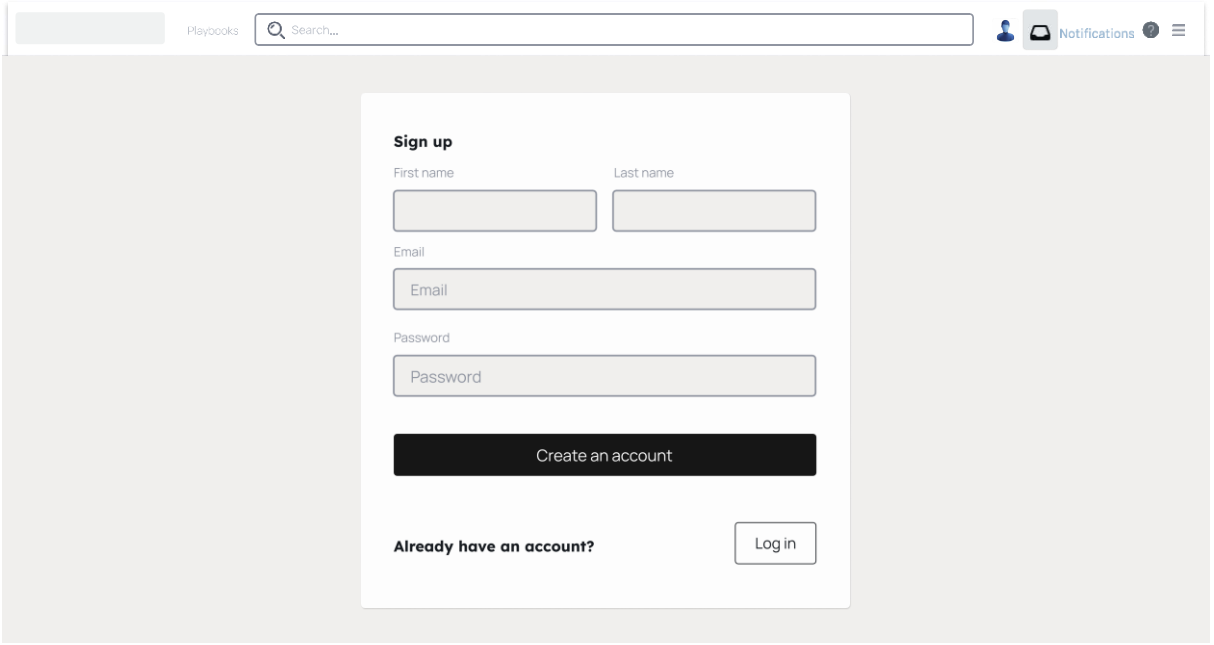


Figure 16. Sign up Page.

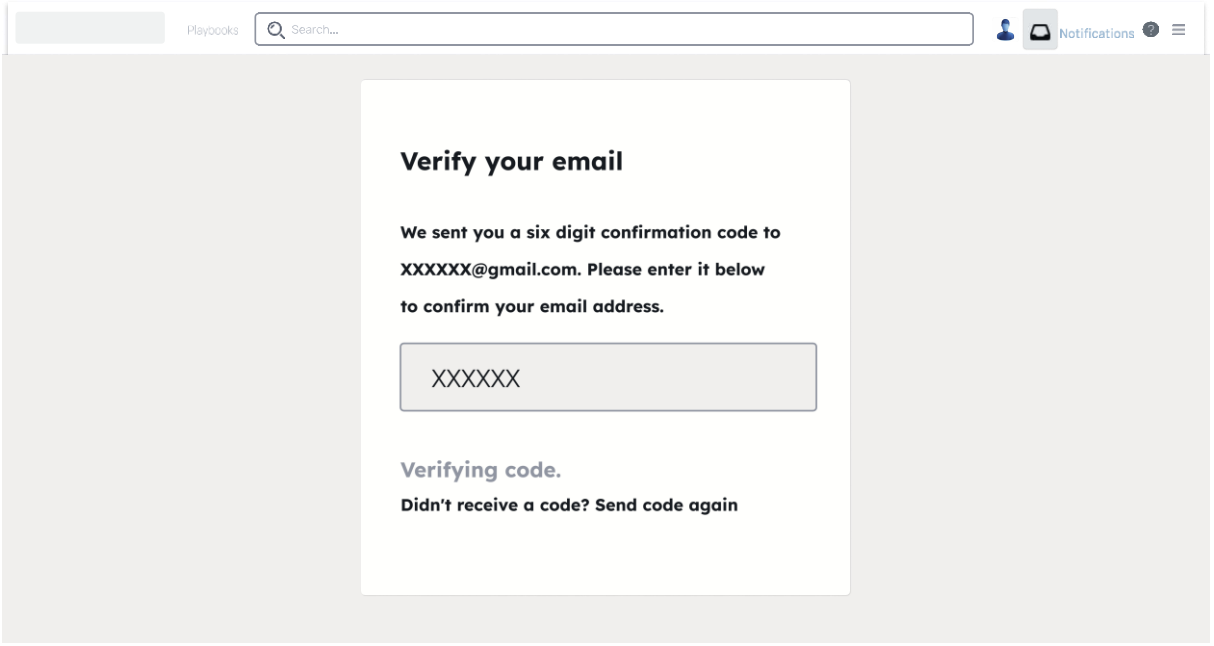


Figure 17. E-mail verification.

- In Figure *18*, a homepage where recommended top playbooks are presented based on the number of upper votes (feedback), comments and views. Together with the Playbook Owner's profile and defined tags.

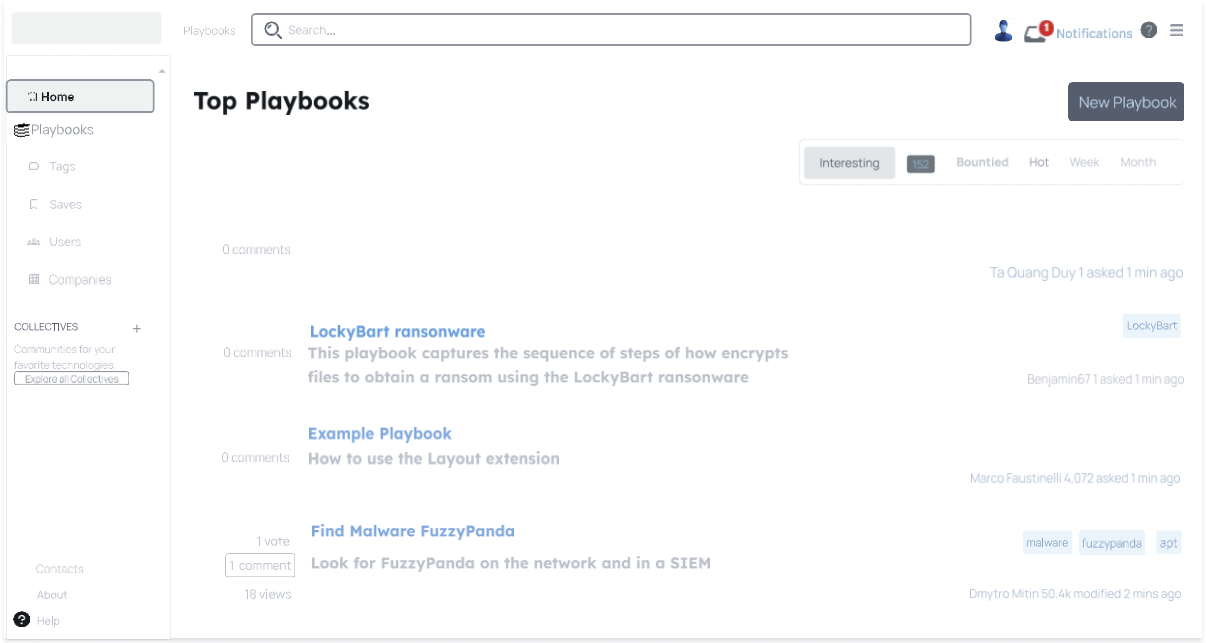


Figure 18. Home Page.

- In Figure *19* and Figure *20*, a Notification Center section where the user can read the content and mark the notifications as read.

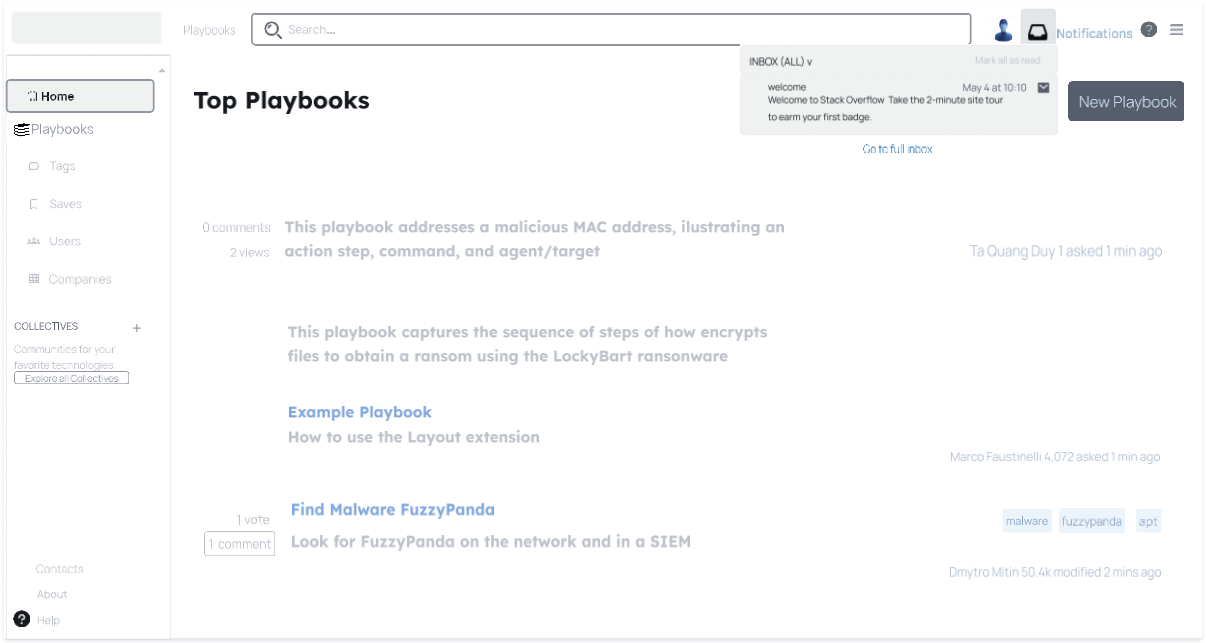


Figure 19. Unread Notification.

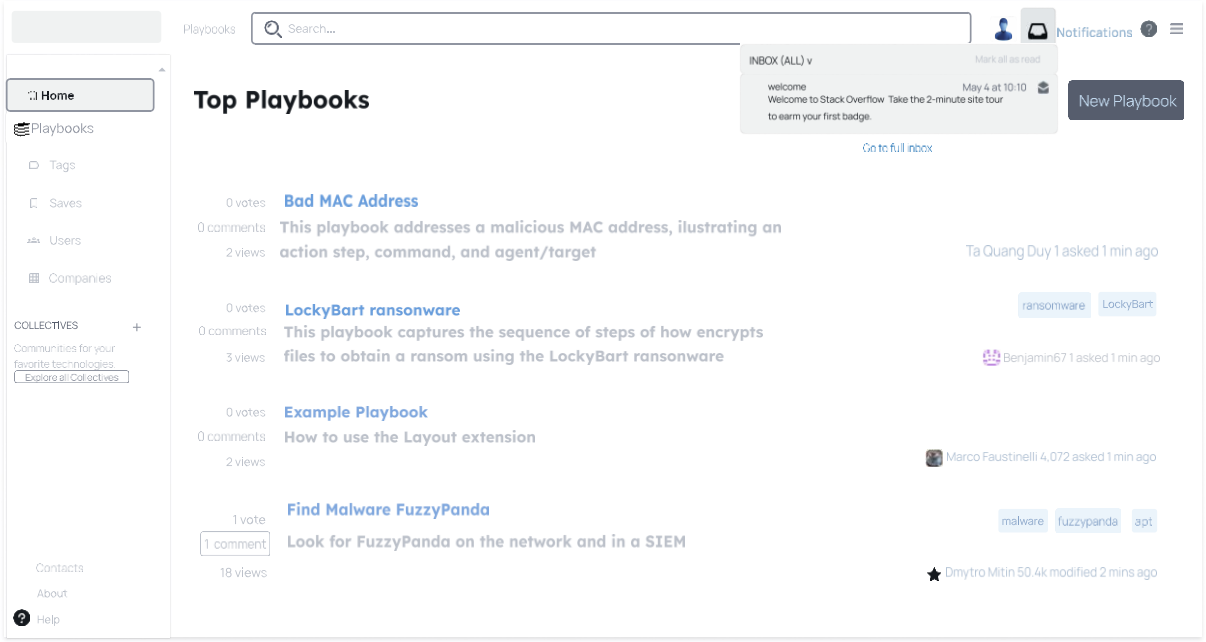


Figure 20. Read Notification.

- In Figure *21* and Figure *22*, a Playbooks Dashboard page with All playbooks and filtering and sorting functionalities according to feedback evaluation, version tracking, newly created playbooks, recent activity, highest feedback score and most frequent playbooks. Additionally, a tag filter based on the classification of the playbooks (e.g. ransomware or malware).

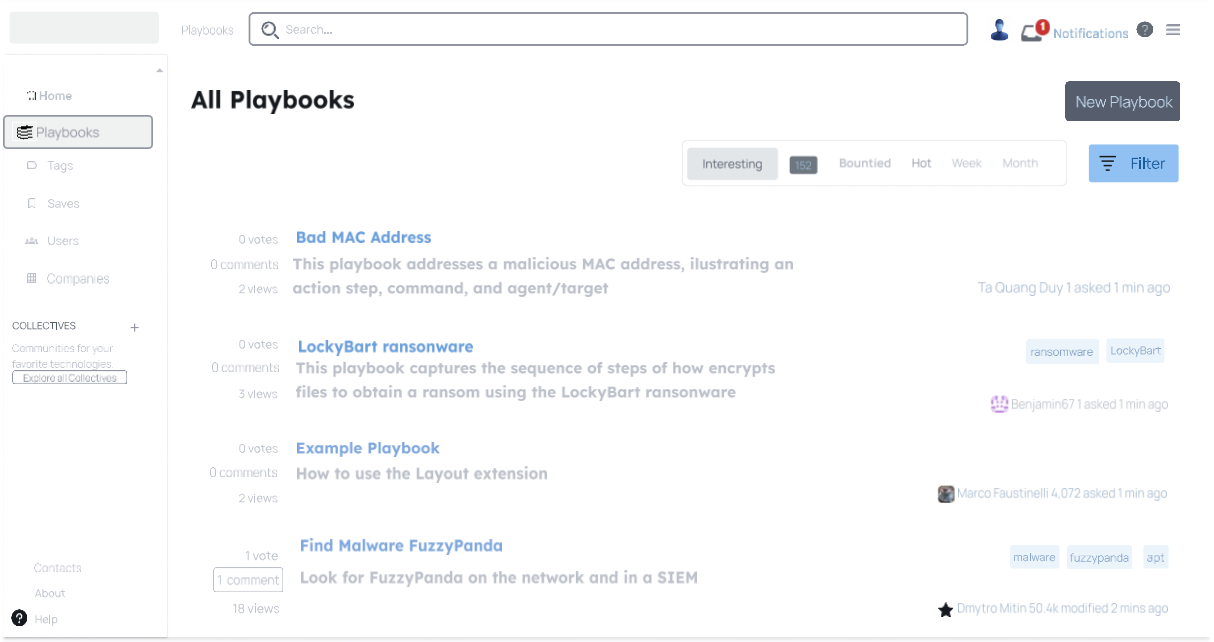


Figure 21. Playbook Dashboard.

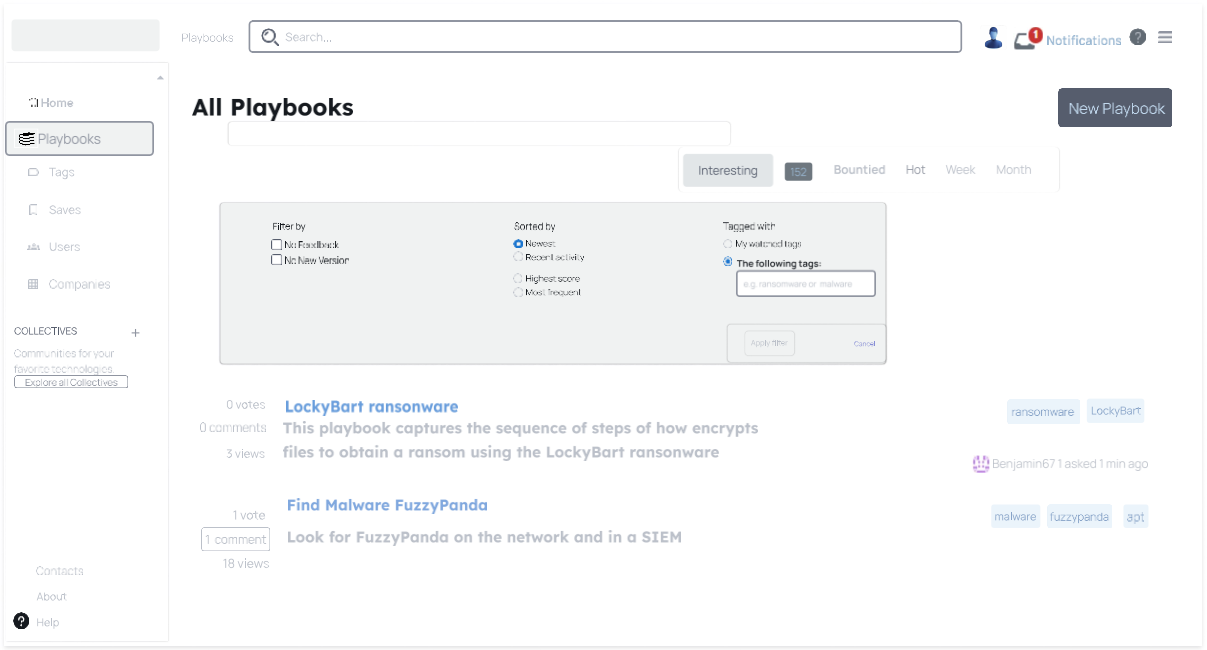


Figure 22. Playbook Dashboard Filtering options.

- In Figure *23*, Figure *24*, Figure *25* and Figure *26*, a playbook Overview page with playbook description, steps, actions and properties with added comments from other users. Additionally, and with insurance of proper user registration, options section to collaborate on the playbook by:
    - commenting on the description, steps, actions and properties.
    - exporting the playbook (*bpmn* and *yml*)
    - sharing the playbook via a web link

- voting as part of feedback evaluation (Like or Dislike)
- creating a new version of the playbook in which the user will become the playbook owner of such playbook.

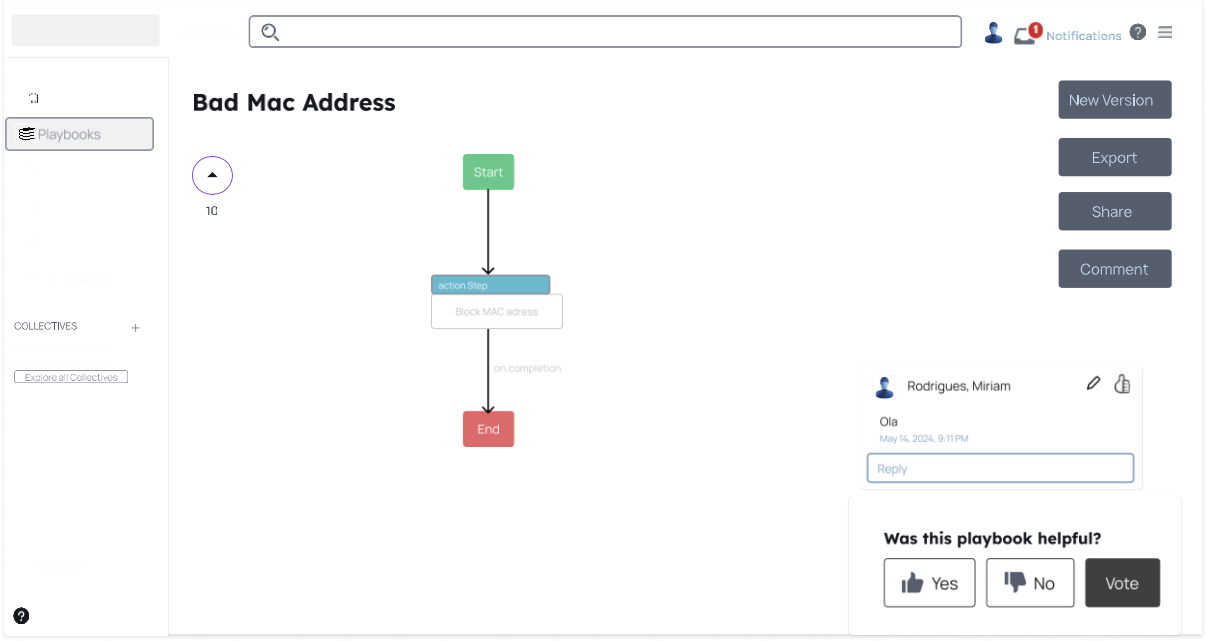


Figure 23. Playbook Overview.

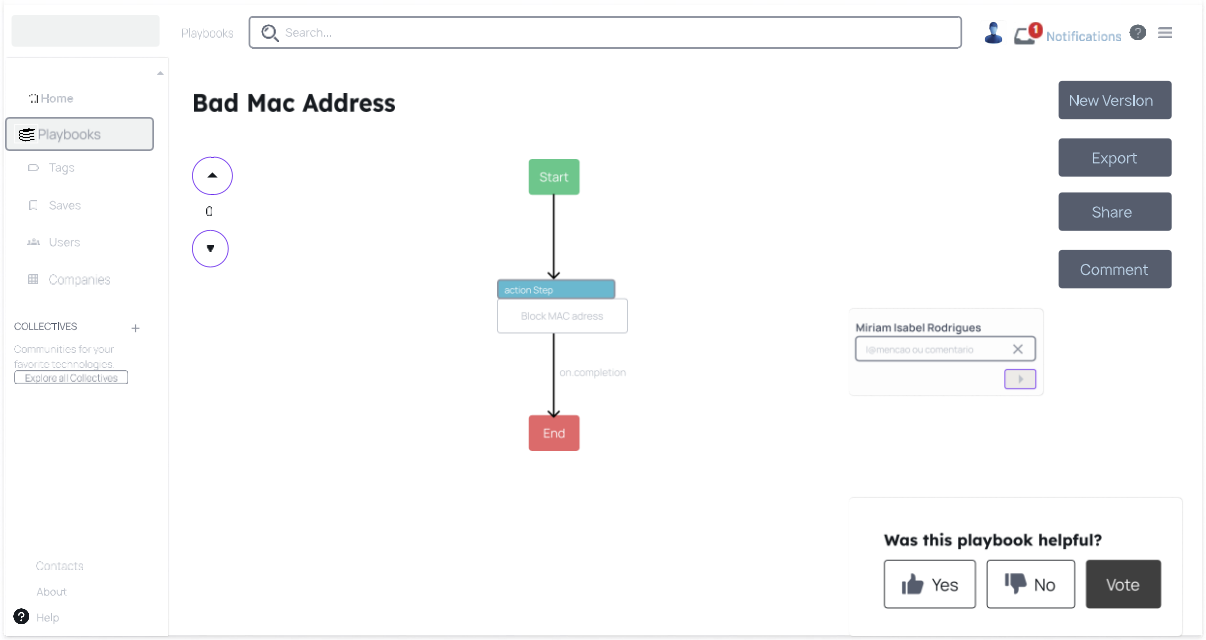


Figure 24. Playbook Overview Options.

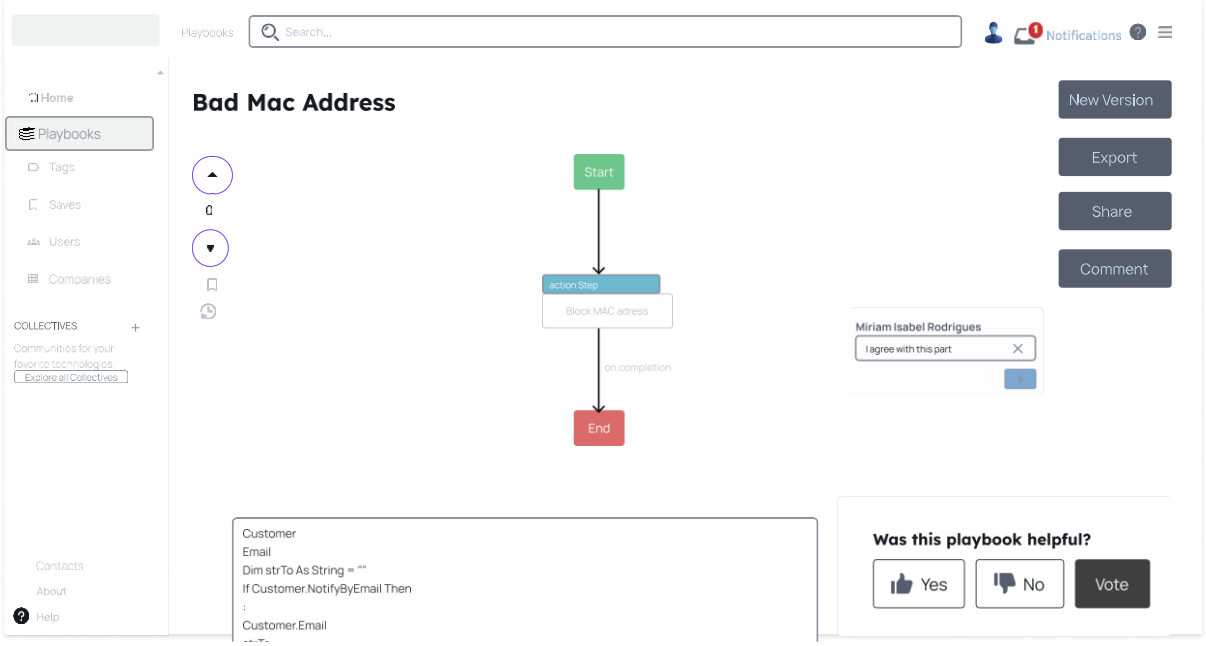


Figure 25. Playbook Overview Comment Post.

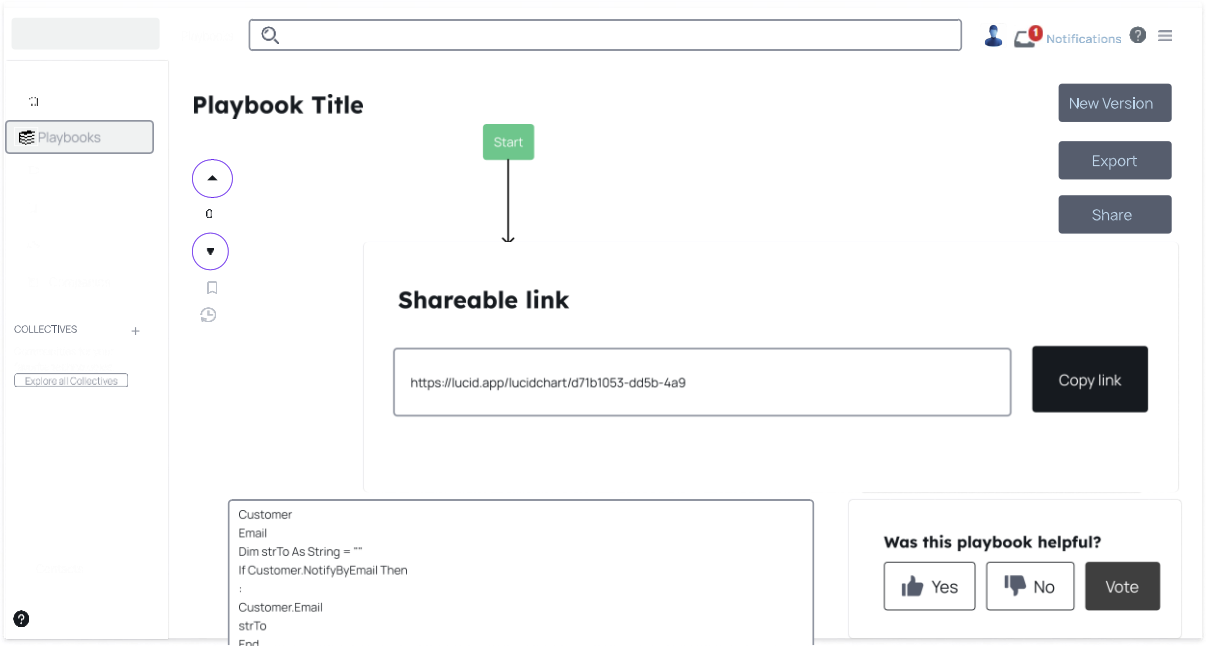


Figure 26. Playbook Overview Shareable link.

- In Figure *27* and Figure *28*, a playbook Creation page where playbook name, description and tags are defined by the playbook owner. Additionally, an import option is present to the user where he can upload an import file (*json*, *yml*, *bpmn*, *pdf*, *docx*, *txt*).

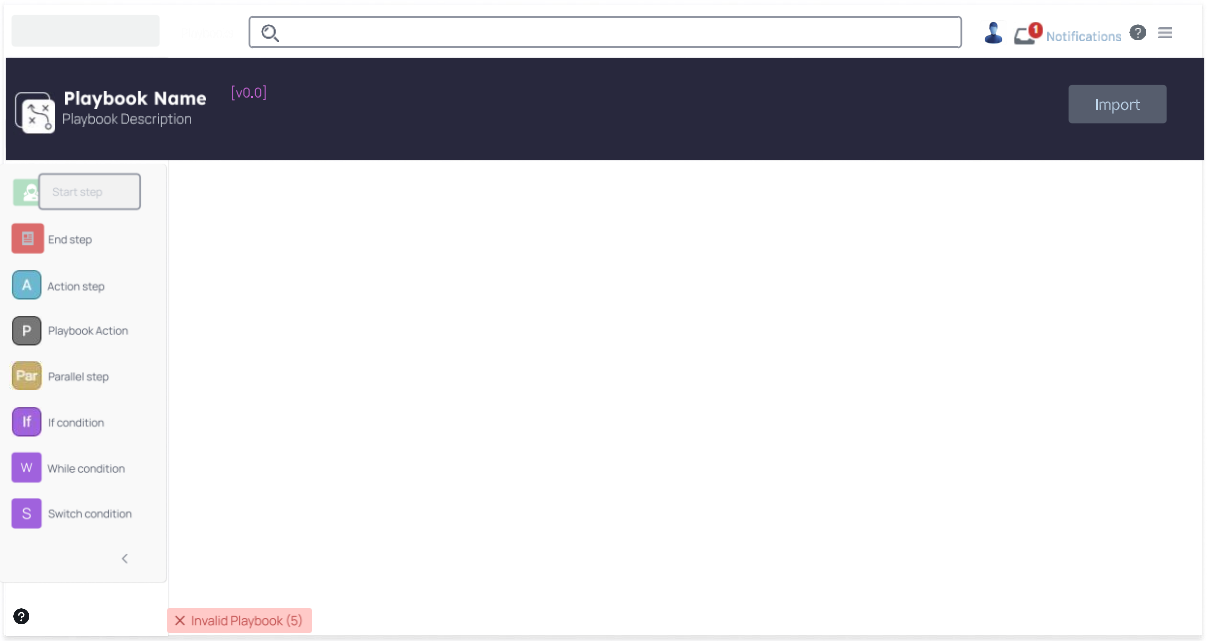


Figure 27. Playbook Creation.

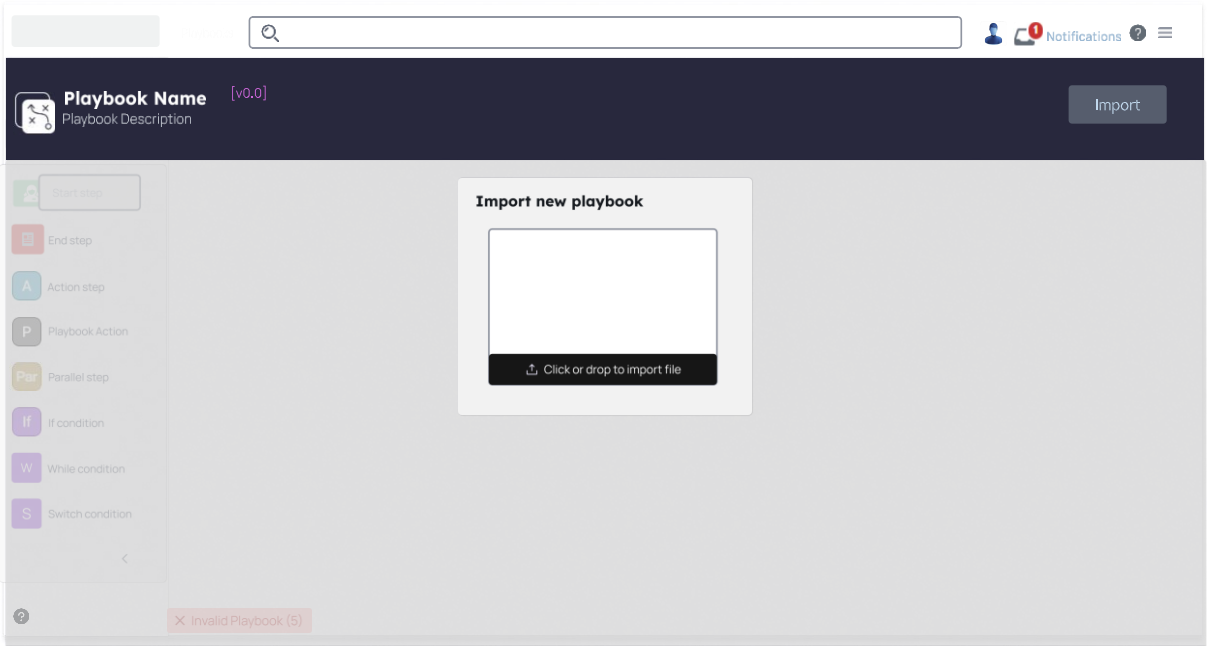


Figure 28. Playbook Creation Import.

- In Figure *29*, Figure *28*, Figure *30* and Figure *31*, a playbook Edition page that can be accessed by the playbook owner of the corresponded version and changes according to Action steps, Playbook Actions, If conditions, While conditions and Switch conditions. All fields can be added, created and deleted from the playbook interactive interface. Validation is displayed according to systems errors that might be generated.

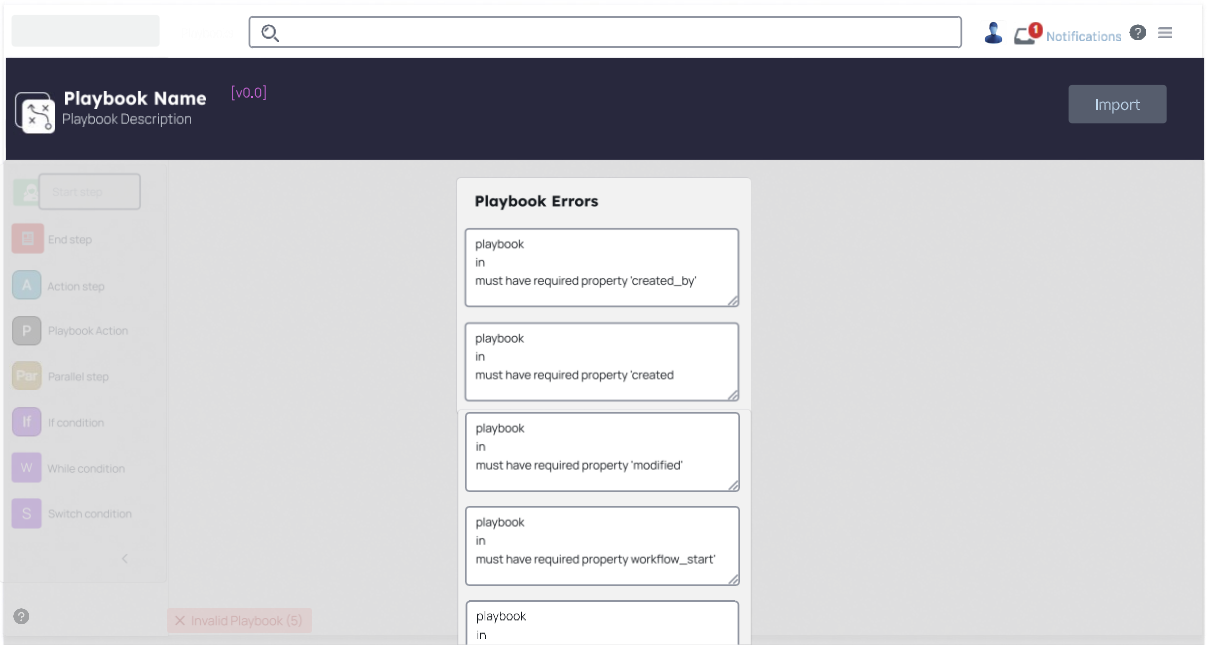


Figure 29. Playbook Creation and Edition Error message.

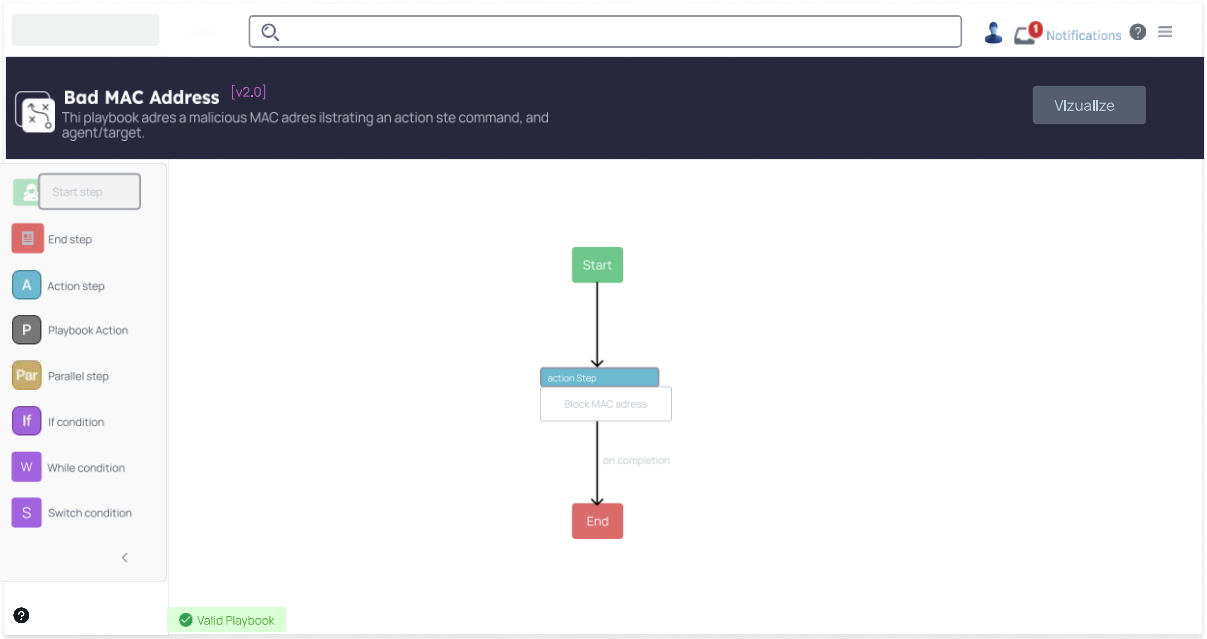


Figure 30. Playbook Edition Page.

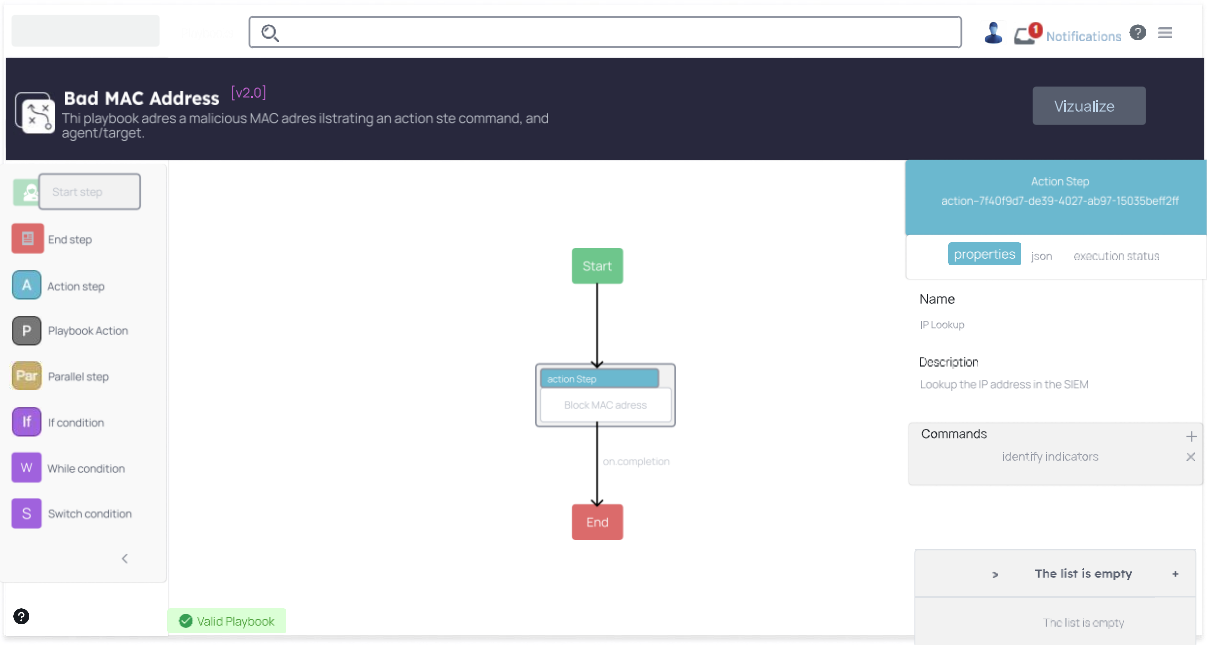


Figure 31. Playbook Edition Details.

Additionally, the expected user flow for demonstration purposes is the following:

1. The user logins to the system in a secure way (Figure *15*).
2. The user is presented with a dashboard of available playbooks (Figure *21*), displayed including recently accessed playbooks, recommended playbooks based on user's role and previous activity, options to search, create, or collaborate on them.
3. Recommended playbooks are displayed based on the collaborative knowledge base. (Figure 14)
4. For the Playbook Search functionality, the playbooks can be filtered based on the Incident type, keywords and playbook owner (Figure *22*). Search results are displayed with relevant metadata (e.g., title, description, scope of playbook, sub-playbooks) - Figure *21*.
5. For the Playbook Selection functionality, the user selects a playbook from the search results, detailed playbook information is displayed, including steps and procedures, incident type it addresses, version history and Collaborative feedback - Figure *24*.
6. For Playbook Collaboration, the user can provide feedback on the playbook by: suggesting improvements in a comment section (Figure *25*); rating/review of the information; update of the selected playbook with a new version - Figure *24*.
7. A new version is requested to the playbook owner and shall be traced back through the lessons-learned-sharing of a playbook. With this, multiple users can work on playbook refinement simultaneously, and it is the playbook owner's responsibility to review and approve a new playbook version.

8. For Playbook Creation, there will be an import functionality available to the user where it is possible to import structured playbook in a *yml*, *md*, *xml*, *json* or *bpmn* formats (Figure 28). Additionally, there should be a create from scratch functionality where the playbook owner or any user that is assigned to collaborate on the playbook creation can insert free text to ease the integration of unstructured playbooks - playbook collaboration functionality allows multiple users to work on playbook refinement simultaneously. Playbook edition consists of defining incident type and objectives, adding step-by-step procedures, anonymizing organization-specific information for sharing and assigning access permissions to authorized users. (SASP Perspective -Figure 30 and Figure 31)
9. After creating a playbook, the playbook owner is presented with a version control functionality where it is possible to trace all changes of that playbook and accept/approve a new change. Following this, the user who requested a new version will be notified of the update's acceptance or denial. The new version will be presented on the dashboard with a link back to the previous versions. This information will be updated on the collaborative knowledge base and presented in the dashboard to users (The goal here is to not only recommend updated versions, but also based the recommendations on user's feedback. Users can compare different versions to identify changes and improvements.).

The 3 use cases were used as the base of the demonstration are presented in Appendix A.

CHAPTER 4

Evaluation

The evaluation of the artefact follows the evaluation process in the design cycle mentioned in Section 3.3. According to Hevner et al. in [40], the evaluation of an IS artifact is only finished when it covers all the requirements and constraints defined to solve the problem at hand.

4.1. Evaluation Process

An *ex-ante* (prior to artifact construction) naturalistic evaluation strategy was applied, considering that it is suitable for deciding on technology investments. According to the DSR Evaluation Framework described in [45], an *ex-ante* strategy focuses on formative and a cost-benefit analysis, basing the evaluation design on a partial prototype and discussing it in a focus group. In these cases, the artifact is evaluated based on its design specifications alone. And consequently, the moment when the evaluation is made shows how design research is a part of the design science.

One-on-one interviews are often considered highly beneficial for assessment purposes, typically lasting anywhere from thirty minutes to several hours as required [40]. These engagements with relevant parties play a crucial role in enhancing the artefact. Furthermore, employing analytical evaluation approaches may include static analysis, architecture analysis, optimization and dynamic analysis, according to [45].

4.2. Semi-structured interviews

For the purpose of design development, the models to be evaluated were the mockups defined in sub-section 3.3.5, together with their usability. This usability was pointed out by the selected interviewers during the use of the mock-ups created in Figma. Additionally, a comparison between the developed artifact against similar tools known to the interviewers was discussed and relevant limitations/weaknesses of the system were highlighted by the interviewers. A panel of experts was assembled to identify the necessary criteria and offer input on the design selection and capabilities of the solution. The evaluation process included the utilization of semi-structured interviews, which presents a cost-effective method for evaluating the solution with actual users in relevant settings while upholding a robust evaluation approach to study the artifacts' dynamic qualities, ensuring sustained utility and benefits in practical and applicable use cases. This phase specifically targeted individuals with diverse expertise to capture varied perspectives and guarantee a more comprehensive validation of the approved artifact.

A total of ten semi-structured interviews were conducted with professionals as detailed and classified in Table 14.

Table 14. Semi-structured interviews for evaluation details.

ID	Interview Date	Current Position	Experience in Cybersecurity (years)	Experience in IR (years)	Company
IT01	2024-06-18	Cybersecurity Team Leader	>= 5	1-3	ISCTE
IT02	2024-07-10	Information Security Professional	>= 25	< 1	Siemens
IT03	2024-07-11	Information Security Manager	>= 25	1-3	Grupo Nabeiro
IT04	2024-07-15	Cybersecurity Team Leader	10-20	10-20	Siemens
IT05	2024-07-15	Cybersecurity Team Leader	10-20	10-20	Siemens
IT06	2024-07-15	Cybersecurity Team Leader	10-20	10-20	Siemens
IT07	2024-07-16	IT Security Director	10-20	>= 5	Santa Casa da Misericórdia
IT08	2024-07-19	CSIRT Global Lead	10-20	>= 5	Siemens
IT09	2024-07-23	CSIRT Member	< 10	< 1	Siemens
IT10	2024-07-31	Information Security Consultant	< 10	< 1	Axians

The first interviewee (IT01) was interviewed, after participating in the design process as the nominated research specialist.

A total of 10 interviews were conducted both academia and industry. 4 out of 10 participants are Cybersecurity Team Leaders, 3 out of 10 are Information Security professionals, 2 out of 10 are CSIRT team members and 1 out of 10 holds the position of IT Director. All participants have at least 5 years of experience working in Cybersecurity, with 67% possessing 10 or more years of experience. Participants knowledge in IR goes from less than a year to 20, with 50% being less than 5 years and the remaining half going from 5 to 20 years of expertise.

4.2.1. Evaluation Interactions

In this sub-section, each expert was requested to review the proposed research artifact, following the mock-ups provided in sub-section 3.3.5. The interviewees were encouraged to comment on the proposed system, identify weakness or limitations and suggest recommendations for modifying or adding features and functionalities they deemed necessary, to validate the system' use from the expected user's perspective and to compare it to existing tools. The feedback gathered from the interviews (presented in Appendix B) provides valuable insights and recommendations that can guide the enhancement of the proposed system. The interviews reveal several key themes that are essential for refining the system.

A recurrent positive aspect identified by the experts was the tool abstraction approach, highlighted in IT03 and IT06. This approach was mentioned for its ability to provide flexibility and adaptability, allowing organizations to centralize knowledge regardless of the specific tools they use, which could evolve over time. Similarly, the visual representation of playbooks emerged as a notable strength, acknowledged by IT04, IT07 and IT09 on how these visual outputs significantly aid in understanding complex workflows, making it easier to identify redundancies and streamline the playbook creation process.

Moreover, the idea of collaborative playbook creation with a centralized database was recognized as a critical strength in IT02, IT07, IT08, and IT10. This feature was seen as essential for fostering teamwork and enabling shared learning within organizations, although it was noted that it could introduce risks if not managed properly. Additionally, the transition from static to dynamic playbooks was highlighted as a significant advantage, by IT02, IT08, and IT09 recognizing the system's potential to evolve alongside emerging threats and adapt to changes more effectively than static counterparts.

Another feature mentioned by IT06 was the system's capacity for feedback collection, which was seen as an important mechanism for continuous improvement. Additionally, the potential for the system to be used for learning and training purposes was emphasized, with IT09 and IT10 pointing out that the platform could serve as a valuable resource for educating and upskilling cybersecurity professionals.

On the other hand, access control and sharing policies were consistently identified as significant weaknesses in IT01, IT02, IT04, IT05, IT08, and IT10. Experts expressed concerns regarding the need to protect sensitive information and manage who can access and contribute to the playbooks, ensuring that only authorized personnel can modify or view certain playbooks. This concern was closely linked to issues of playbook trustworthiness and quality, IT01, IT05, IT07, and IT08 stressed that without stringent criteria and validation processes, the system could suffer from a lack of reliability, which would undermine its effectiveness.

Another significant limitation identified was the lack of interconnections between playbooks, mentioned in IT07 and IT09. This was seen as a potential inefficiency of the IR process, as playbooks that are not linked might fail to share crucial steps or procedures that are relevant across different scenarios. The absence of such linkages could lead to redundancies or gaps in the IR strategies.

In terms of suggestions for improvement, interoperability with other tools for implementation purposes was a frequently recommended enhancement. IT01, IT03, IT04, IT05, IT06, IT07 and IT09 suggested that enabling the KMS to integrate seamlessly with existing tools would allow it to be more widely applicable and better integrated into the workflows of different organizations. This recommendation was accompanied by a call for the system to support internal organizational use by IT02, IT03, IT06, IT07, IT08 and IT09, emphasizing the need for the KMS to enhance, rather than merely supplement, existing processes within organizations.

Advanced feedback capabilities were also recommended in IT06 as a way to ensure the system's continuous improvement based on user input. Additionally, IT01, IT02 and IT08 identified the incorporation of advanced creation and search capabilities, such as those powered by AI, LLMs, and autocomplete features, was suggested as a way to significantly enhance the usability and intelligence of the system. These capabilities would make it easier for users to create, find, and use playbooks effectively.

Finally, the development of a classification and taxonomy system was highlighted as a critical enhancement by IT01 and IT10. Such system would facilitate the organization of playbooks in a systematic manner, making it easier to manage large volumes of information and ensuring that users can quickly find the playbooks most relevant to their needs. This would not only improve the user experience but also enhance the overall functionality and effectiveness of the KMS.

4.2.2. Evaluation Results

In this sub-section, the key results of the evaluation done with the ten interviews iterations are summarized in Table 15.

Table 15. Evaluation Results Matrix.

	Topic	IT01	IT02	IT03	IT04	IT05	IT06	IT07	IT08	IT09	IT10
Positive feedback	Tool abstraction approach			✓			✓				
	Visual Representation				✓			✓		✓	
	Collaborative Playbook creation with Centralized database		✓					✓	✓		✓
	Static to Dynamic Playbooks		✓						✓	✓	
	Feedback Collection						✓				
	Learning & Training purposes									✓	✓

	Topic	IT01	IT02	IT03	IT04	IT05	IT06	IT07	IT08	IT09	IT10
Weaknesses and limitations	Access Control & Sharing Policies	✓	✓		✓	✓			✓		✓
	Playbook Trustworthiness & quality	✓				✓		✓	✓		
	Interconnections between playbooks							✓		✓	
	Interoperability with other tools for implementation purposes (import and export)	✓		✓	✓	✓	✓	✓		✓	
Additional Suggestions	Internal Organizational use		✓	✓			✓	✓	✓	✓	
	Advanced Feedback Capabilities						✓				
	Advanced Creation and search Capabilities (AI, LLMs, autocomplete)	✓	✓						✓		
	Classification and Taxonomy System	✓									✓

In an overall analysis, the interviewees commonly agreed that the proposed artifact possesses several strengths, particularly in its flexibility, visual representation, and collaborative features, there are also critical areas that require attention. The consistent emphasis on the need for strong access control, playbook quality, and interoperability with other tools underscores the importance of making the system secure, reliable, and widely usable. Addressing these limitations by implementing robust security measures, enhancing interoperability, and supporting internal organizational use will be crucial in ensuring the KMS's practical applicability.

Regarding positive feedback, of all interviewees, 80% gave positive feedback on the system. However, no trend was specifically identified. Collaborative Playbook creation with Centralized database was mentioned by 40% of the interviewees and Static to Dynamic playbooks was a topic pointed out only from employees that used static playbooks over dynamic ones. The other 20% of interviewees focused on both weaknesses and additional suggestions to the system.

Regarding weaknesses and limitations, 20% of the interviewees did not identify any to the system, meaning 80% identified 1 to 2 topics in this regard. The trend identified by 60% of the interviewees was the Access Control & Sharing Policies, followed by 40% agreeing on the Playbook Trustworthiness & Quality.

The common trend of all interviews was shifted to the implementation of the proposed system and further introduction of advanced features. Namely, the trend identified for Additional suggestions was the Interoperability with other tools for implementation purposes (import and export) by 70% of the interviewers, related to Internal Organizational use of the system mentioned by 60%. These additional suggestions were primarily residual, focusing on adjustments between systems requirements rather than the use case requirements formally presented as the scope of the research. The minimal changes required to the scope of the artifacts design indicate that data saturation was achieved, confirming the robustness and completeness of the initial design. The evaluation process effectively validated the artifact, ensuring that it meets the practical needs and expectations of users in real-world cybersecurity IR scenarios.

4.3. Validated Artifact

Using the validated artifact here presented, future researchers will be able to continuously improve the systems functionalities and capabilities identifying which use case requirements are the most significant as seen in Table 16 and highlighting the system requirements that should become the primary focus of future iterations as seen in Table 17.

Table 16. Validated Use Case Requirements.

Module	Requirements	IT01	IT02	IT03	IT04	IT05	IT06	IT07	IT08	IT09	IT10
Login and Sign-up	User Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	User Profile Management	✓	✓		✓	✓			✓		
Playbook Selection	User Search	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	User Select	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Playbook Creation	Playbook Creation		✓						✓	✓	
	Playbook Upload	✓		✓	✓	✓	✓	✓		✓	
	Playbook Edit	✓			✓						
Playbook Collaboration	Playbook Visualize			✓	✓			✓		✓	✓
	Playbook Comment		✓	✓				✓			✓
	Playbook Feedback						✓				✓

Table 17. Validated System requirements.

Requirements	IT01	IT02	IT03	IT04	IT05	IT06	IT07	IT08	IT09	IT10
Database and Data Management		✓								✓
Sharing and Collaboration	✓	✓		✓	✓			✓		✓
User Interface			✓	✓		✓	✓		✓	
Recommendations and Analytics	✓	✓						✓		✓
Import and Export	✓		✓	✓	✓	✓	✓		✓	
API and Integration	✓		✓	✓	✓	✓	✓		✓	
Taxonomy and Classification	✓									✓

4.4. Comparison with other solutions

In this sub-section a comparation between the proposed system and similar tools commonly used for KM within organizations is presented in Table 18. The selected tools were referenced by the interviewers, during the Evaluation Process (section 4.1) and the ones referenced in the in sub-section 2.2.3. The proposed system identified in this comparison already integrates the additional details provided by the interviewers into definition of the system.

The comparative analysis of the proposed system against existing cybersecurity IR tools reveals several key strengths that position it as a highly effective solution for enhancing KM and collaboration in IR. The proposed system distinguishes itself through its robust playbook management capabilities, which include a visual playbook editor, auto-complete features, and duplication checks. These functionalities surpass the capabilities of tools like *MISP* and *Confluence*, which either lack comprehensive playbook management features or offer only limited support for such processes. By enabling seamless collaboration and ensuring the accuracy and relevance of IR playbooks, the proposed system fosters a more dynamic and interactive approach to knowledge sharing, opposite from a static one.

Furthermore, the proposed system's access control mechanisms offer significant advantages over many existing tools. With its ability to define granular roles and permissions, the system provides flexibility in managing user access, balancing security requirements with the need for collaboration. This is particularly crucial in environments where sensitive information must be shared securely across teams. While tools like *TheHive* and *Demisto* offer similar role-based access controls, the proposed system enhances this with the ability to define both public and private user permissions, offering more nuanced control over how playbooks and knowledge are disseminated.

Table 18. Comparison between the proposed system and other tools

Topic	Proposed System	Demisto (Cortex XSOAR)	SASP	TheHive	MISP	Confluence
Interoperability with other tools	✓ import and export of playbooks	✓ orchestration and automation	✗ semantic web-based approach	✗ case management and collaboration	✗ limited playbook integration	✗ document import
Playbook Management	✓ playbook creator ✓ visual playbook editor ✓ avoid playbook duplication ✓ autocomplete ✓ recommendation system ✓ collaboration features	✓ playbook creator ✓ visual playbook editor ✓ avoid playbook duplication ✓ pre-built playbooks	✓ playbook creator ✓ visual playbook editor ✓ playbooks sharing	✗ define workflows	✗ threat intelligence focus	✗ manual process, only upload and create
Access Control	✓ public managed accessibility ✓ private user permissions	✓ administrators define user roles and permissions	✓ enforce security policies and access restrictions	✓ role-based access control ✓ supports granular permissions	✓ role-based access control ✗ supports granular permissions to threat data	✓ administrators define permissions
Classification System	✓ robust classification and taxonomy	✗ user managed classification	✓ robust classification and taxonomy	✓ tags and custom fields	✗ comprehensive tags for threat data	✗ user managed labelling
User Familiarity and Integration	✓ similiarity with StackOverflow ✓ playbook integration	✓ user-friendly interface with wide range of security tools	✗ not widely known to the community	✓ MISP integration	✗ widely used for threat intelligence	✗ common choice for documentation
Dynamic Capabilities	✓ transition from static to dynamic playbooks ✓ continous updates	✓ dynamic playbooks ✓ real-time updates ✓ automation	✓ dynamic playbooks ✓ continuous updates	✗ not very dynamic playbooks	✗ threat intelligence focus	✗ static playbooks

Another distinctive feature of the proposed system is its integration of a robust classification and taxonomy system. This feature enhances the organization and retrieval of information, making it easier for users to access the knowledge needed to respond effectively to incidents. Unlike systems such as *MISP* and *TheHive,* which offer less comprehensive classification mechanisms, the proposed system ensures that knowledge is systematically categorized, promoting more efficient knowledge management.

The proposed system's dynamic capabilities further set it apart from other tools. It transitions from static playbook management to dynamic, continuously updated playbooks, a feature essential in the fast-evolving landscape of cybersecurity. This is an area where many traditional systems, such as *Confluence* and *SASP*, fall short, offering more static and less adaptive playbook functionalities. By supporting real-time updates and automation, the proposed system enables IR teams to remain agile and responsive to emerging threats.

In terms of user familiarity, the proposed system benefits from its interface design, which mirrors platforms like *StackOverflow*, making it more intuitive for users who are already accustomed to similar environments. This ease of use enhances the system's accessibility and reduces the learning curve, a feature that is less emphasized in some of the other tools analyzed. Although *Demisto* also offers a user-friendly interface, the proposed system's combination of familiarity and advanced functionality gives it a distinctive edge.

In conclusion, the proposed system offers a comprehensive, collaborative, and user-friendly approach to KM in cybersecurity IR. Its advanced playbook management, flexible access controls, robust classification system, and dynamic capabilities make it a superior alternative to many existing tools. By fostering collaboration, enabling continuous updates, and ensuring ease of use, the system addresses critical gaps in current IR tools and provides a framework that can significantly enhance the effectiveness and efficiency of knowledge sharing in cybersecurity.

CHAPTER 5

Conclusion

In this chapter, we summarize the findings of the study, addressing the research conclusions, limitations, potential future work, and the communication followed.

5.1. Research Conclusions

The SLR conducted through this research highlights the multidimensional nature of knowledge utilized in IR, encompassing IR Frameworks, Playbooks, Knowledge Bases, AI-based detection systems, and CTI[16], [25] and [31]. Collectively, these components contribute to the proactive management and mitigation of cyber threats within organizations [1] and [36]. Moreover, the methodologies employed in IR scenarios for knowledge management, such as structured IR frameworks, ontology-driven systems, graph-based analysis, and collaborative approaches within SOCs, have emerged as essential strategies [1], [22], [31] and [37]. The existing literature emphasizes the crucial role of KM in IR; however, further exploration and implementation of these systems are still necessary.

To address this gap, this research proposes a conceptual KMS model specifically designed for IR. The DSR methodology employed ensured a systematic development process for the KMS design artifact described in Chapter 3. The artifact is designed with a collaborative knowledge base that stores and shares structured IR playbooks, enabling professionals to access and contribute to the shared knowledge.

The system includes functionalities for creating, visualizing, and managing playbooks with version control and collaborative feedback features. Secure user authentication and profile management ensures that access to sensitive information is restricted to authorized personnel, while real-time notifications and alerts facilitate swift collaboration in the playbook's actions. Additionally, the system supports dynamic playbooks, enabling real-time adaptation to evolving threats and scenarios, ensuring flexibility and responsiveness in IR procedures.

Users would be able to register, authenticate, and manage their profiles, ensuring secure access to the system based on role-specific permissions. They could create, search for, and visualize IR playbooks, allowing for the efficient management of response protocols. The system supports collaborative feedback and version control, enabling users to provide input, update, and refine playbooks collectively. Additionally, users can receive real-time notifications and alerts related to their managed playbooks, ensuring timely involvement in update actions. The system also allows users to interact with knowledge retrieval, improving decision-making and proactive playbooks management. In the model, the requirements focused on usability of the users in Table 10 were meet.

The evaluation process conducted through semi-structured interviews with cybersecurity experts substantiated the artifact's relevance, usability, and potential to improve cybersecurity IR workflows. Feedback from experts highlighted the system's advantages for structured knowledge sharing and the necessity for dynamic playbooks as opposed to static ones.

5.2. Limitations

The limitations identified in this study are shaped by both self-imposed limitations and resource constraints, which influenced the overall research. The exclusion of specific use cases, such as the ability for the tool to generate statistics, trace modifications in playbooks, and offer input suggestions, restricts the scope of the study and the temporal limitations involved. These functionalities were not prioritized due to a strategic emphasis on fundamental capabilities that corresponded with the research objectives. Incorporating these advanced use cases would have required additional resources, time, and expertise, which were not feasible within the scope of this research.

Another significant limitation is the dependence on the viewpoint of an individual interviewer throughout the design phase. This restriction emerged due to constraints in engaging a broader spectrum of stakeholders during the research period. Although the inclusion of a wider array of perspectives could have enhanced the artifact design, logistical impediments, such as availability and scheduling conflicts, rendered it challenging to assemble a more extensive pool of expert feedback. Consequently, the system’s design embodies the insights of one principal expert, which limited the diversity of perspectives but ensured coherence and concentration in the artifact's conceptualization.

Moreover, the inability to incorporate suggested modifications from the interviews into the final artifact reflects a resource-related constraint. A self-imposed limitation was defined for the design phase, without extending into developmental or implementation stages. The absence of development implied that iterative enhancements based on expert feedback could not be fully realized. Resource constraints, encompassing time, funding, and developmental capacity, restricted the advancement of the artifact from theoretical design to practical application.

In conclusion, the limitations are predominantly a consequence of pragmatic decisions associated with scope, resource distribution, and the availability of expert feedback. Future investigations could mitigate these limitations by broadening the spectrum of use cases, engaging a more extensive array of experts, and progressing to a Minimal Viable Product (MVP) or fully operational system to evaluate the practicality of the designed system.

5.3. Future Work

The future work outlined in this section demonstrates a clear direction for advancing the research on the KMS for cybersecurity IR. Firstly, focusing on the implementation of the proposed artifact, ensuring that all the functional and non-functional requirements defined in this research are integrated and tested in real-world scenarios. Structured interviews with cybersecurity professionals using an implemented system will provide valuable feedback and validate its practical effectiveness.

Additionally, future research should evaluate the incorporation of advanced technologies such as artificial intelligence and machine learning, as suggested by interviewers. These technologies have the potential to enhance the system's proactive capabilities, particularly in the areas of anomaly detection, incident classification, and predictive analytics, enabling more efficient and responsive playbook management.

It is also important to explore the integration of mechanisms that ensure the trustworthiness and quality of playbooks, with robust access control and sharing policies. These measures are crucial for safeguarding sensitive knowledge and ensuring that only authorized users can modify or access the system's content.

Furthermore, there is a need to investigate the correlation between incidents and playbooks used within the KMS. This could lead to the development of advanced features that highlight interconnections between playbooks and build a comprehensive taxonomy and classification system for them. Understanding these relationships will enable more targeted and effective responses to incidents.

Lastly, further studies should focus on the expansion of use cases that were excluded due to resource limitations, such as generating statistics based on content and user profiles, tracking playbook changes across versions, and suggesting improvements to playbooks based on historical data. These features would enhance the usability and adaptability of the KMS, contributing to a more dynamic and efficient IR process.

References

[1] C. Islam and M. A. Babar, “An Ontology-Driven Approach to Automating the Process of Integrating Security Software Systems,” 2019.

[2] S. Facchinetti, S. A. Osmetti, and C. Tarantola, “A statistical approach for assessing cyber risk via ordered response models,” *Risk Analysis*, 2023, doi: 10.1111/risa.14186.

[3] P. O. Obitade, “Big data analytics: a link between knowledge management capabilities and superior cyber protection,” *J Big Data*, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0229-9.

[4] “Cost of a Data Breach Report 2023,” 2023. Accessed: Dec. 16, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[5] S. R. B. Mohd Kassim, S. Li, and B. Arief, “Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions,” *Digital Threats: Research and Practice*, vol. 4, no. 3, pp. 1–24, Sep. 2023, doi: 10.1145/3609230.

[6] C. M. Patterson, J. R. C. Nurse, and V. N. L. Franqueira, “Learning from cyber security incidents: A systematic review and future research agenda,” *Comput Secur*, vol. 132, Sep. 2023, doi: 10.1016/j.cose.2023.103309.

[7] M. S. Kamarulzaman, N. Hussin, M. S. M. Shoid, A. Ab Rahman, M. N. Ahmad, and R. Abdul Aziz, “Information and Knowledge Management in the Scope of the Information Security Practices: The Human Factor within Organizations,” *International Journal of Academic Research in Business and Social Sciences*, vol. 10, no. 11, Nov. 2020, doi: 10.6007/ijarbss/v10-i11/8185.

[8] G. Sarkar, H. Singh, S. Kumar, and S. K. Shukla, “Tactics, Techniques and Procedures of Cybercrime: A Methodology and Tool for Cybercrime Investigation Process,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2023. doi: 10.1145/3600160.3605013.

[9] “FORESIGHT 2030 THREATS.” [Online]. Available: www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[10] M. Ammi, O. Adedugbe, F. M. Alharby, and E. Benkhelifa, “Taxonomical Challenges for Cyber Incident Response Threat Intelligence: A Review,” 2022, *IGI Global*. doi: 10.4018/IJCAC.300770.

[11] V. Sreejith, P. U. Reddy, B. H. Rao, and S. A. Balakrishnan, “Hybrid Network Security Model for Small and Mid Sized Enterprises,” in *Proceedings of the 2022 3rd International Conference on Intelligent Computing, Instrumentation and Control Technologies: Computational Intelligence for Smart Systems, ICICICT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 622–626. doi: 10.1109/ICICICT54557.2022.9917896.

[12] A. ZAMFIROIU and R. C. SHARMA, “Cybersecurity Management for Incident Response,” *Romanian Cyber Security Journal*, vol. 4, no. 1, pp. 69–75, May 2022, doi: 10.54851/v4i1y202208.

[13] K. Daimi and C. Peoples, *Advances in cybersecurity management*. Springer International Publishing, 2021. doi: 10.1007/978-3-030-71381-2.

[14] “ISC2_Cybersecurity_Workforce_Study_2023,” 2023, Accessed: Dec. 16, 2023. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

[15] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA Statement,” 2009.

[16] J. Dwight, “ECOMMERCE FRAUD INCIDENT RESPONSE: A GROUNDED THEORY STUDY,” *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 18, pp. 173–202, 2023, doi: 10.28945/5110.

[17] R. Smith, H. Janicke, Y. He, F. Ferra, and A. Albakri, “The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework,” *Comput Secur*, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102398.

[18] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology,” Gaithersburg, MD, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[19] R. Dickerson, “Incident Management 101 Preparation and Initial Response (aka Identification),” 2021.

[20] O. I. Falowo, S. Popoola, J. Riep, V. A. Adewopo, and J. Koch, “Threat Actors’ Tenacity to Disrupt: Examination of Major Cybersecurity Incidents,” *IEEE Access*, vol. 10, pp. 134038–134051, 2022, doi: 10.1109/ACCESS.2022.3231847.

[21] “IBM 2021 Cyber Resilient Organization Study.” Accessed: Nov. 18, 2023. [Online]. Available: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

[22] M. Akbari Gurabi, A. Mandal, J. Popanda, R. Rapp, and S. Decker, “SASP: A Semantic web-based Approach for management of Sharable cybersecurity Playbooks,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2022. doi: 10.1145/3538969.3544478.

[23] F. Fauziyah, Z. Wang, and G. Joy, “Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT),” *Journal of Information Security*, vol. 13, no. 04, pp. 294–311, 2022, doi: 10.4236/jis.2022.134016.

[24] K. Jang and N. G. Landuyt, “Limited Benefits of Technological Advances in Human Service Organizations: Going beyond the Hype Using Sociotechnical Knowledge Management

System," *J Soc Serv Res*, vol. 49, no. 4, pp. 426–446, 2023, doi: 10.1080/01488376.2023.2236131.

[25] H. Horikawa *et al.*, "Enhancement of a Company-Wide Information Security Management System Through Incident Learning," *SN Comput Sci*, vol. 4, no. 3, May 2023, doi: 10.1007/s42979-023-01691-7.

[26] P. O. Obitade, "Big data analytics: a link between knowledge management capabilities and superior cyber protection," *J Big Data*, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0229-9.

[27] B. Kitchenham, P. Brereton, Z. Li, D. Budgen, and A. Burn, "Repeatability of systematic literature reviews," in *IET Seminar Digest*, 2011, pp. 46–55. doi: 10.1049/ic.2011.0006.

[28] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Comput Secur*, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102387.

[29] C.-M. Chen, Z.-X. Cai, and Dan-Wei (Marian) Wen, "Designing and Evaluating an Automatic Forensic Model for Fast Response of Cross-Border E-Commerce Security Incidents," *Journal of Global Information Management*, vol. 30, no. 2, pp. 1–19, Sep. 2021, doi: 10.4018/jgim.20220301.oa5.

[30] Z. T. Sworna, M. Ali Babar, and A. Sreekumar, "IRP2API: Automated Mapping of Cyber Security Incident Response Plan to Security Tools' APIs," in *Proceedings - 2023 IEEE International Conference on Software Analysis, Evolution and Reengineering, SANER 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 546–557. doi: 10.1109/SANER56733.2023.00057.

[31] F. K. Kaiser, L. J. Andris, T. F. Tennig, J. M. Iser, M. Wiens, and F. Schultmann, "Cyber threat intelligence enabled automated attack incident response," in *Proceedings - 3rd International Conference on Next Generation Computing Applications, NextComp 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/NextComp55567.2022.9932254.

[32] G. Settanni, F. Skopik, Y. Shovgenya, and R. Fiedler, "A collaborative analysis system for crob-organization cyber incident handling," in *ICISSP 2016 - Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, SciTePress, 2016, pp. 105–116. doi: 10.5220/0005688301050116.

[33] C. Molloy, S. H. H. Ding, P. Charland, and B. C. M. Fung, "JARV1S: Phenotype Clone Search for Rapid Zero-Day Malware Triage and Functional Decomposition for Cyber Threat Intelligence," 2022. [Online]. Available: https://www.av-test.org/en/statistics/malware/

[34] S. Rizvi, M. Scanlon, S. Member, J. Mcgibney, and J. Sheppard, "Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions," 2022, doi: 10.1109/ACCESS.2022.DOI.

[35] A. Berady, M. Jaume, V. V. T. Tong, and G. Guette, “From TTP to IoC: Advanced Persistent Graphs for Threat Hunting,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1321–1333, Jun. 2021, doi: 10.1109/TNSM.2021.3056999.

[36] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, “MISP - The design and implementation of a collaborative threat intelligence sharing platform,” in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, Association for Computing Machinery, Inc, Oct. 2016, pp. 49–56. doi: 10.1145/2994539.2994542.

[37] J. Steinke *et al.*, “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” 2015. [Online]. Available: www.computer.org/security

[38] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. M. Siddiqui, “Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities,” *Comput Secur*, vol. 135, Dec. 2023, doi: 10.1016/j.cose.2023.103525.

[39] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[40] A. R. Hevner, S. T. March, J. Park, and S. Ram, “DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1,” 2004.

[41] “Incident Response Procedures.” Accessed: Mar. 15, 2024. [Online]. Available: https://www.cynet.com/incident-response/

[42] M. Rodrigues, “System Diagram.” Accessed: Sep. 30, 2024. [Online]. Available: https://lucid.app/lucidchart/8219969b-6d28-4f98-8ba9-05a2c8570ea0/edit?viewport_loc=-3120%2C-822%2C5627%2C2938%2C0_0&invitationId=inv_11184fc7-e3f0-40e5-9ac5-fdb10e3ab7bf

[43] M. Rodrigues, “Figma mock-ups.” Accessed: Sep. 30, 2024. [Online]. Available: Figma mock-ups

[44] M. Zych, “CACAO Roaster Project .” Accessed: Sep. 30, 2024. [Online]. Available: https://github.com/opencybersecurityalliance/cacao-roaster

[45] J. Venable, J. Pries-Heje, and R. Baskerville, “A comprehensive framework for evaluation in design science research,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, pp. 423–438. doi: 10.1007/978-3-642-29863-9_31.

[46] M. Zych, “CACAO Playbook Examples.” Accessed: Sep. 30, 2024. [Online]. Available: https://github.com/oasis-tcs/cacao/tree/master/Examples/CACAO-2.0

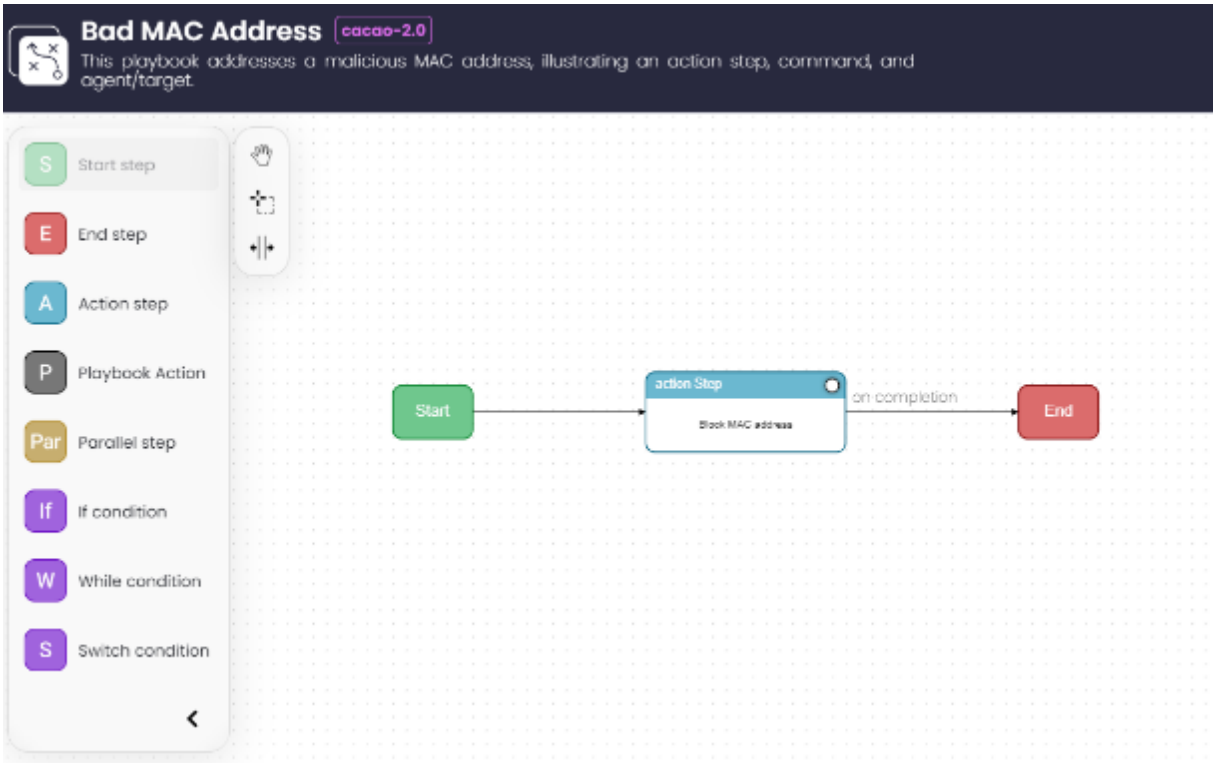
[47] B. Jordan and A. Thomson, “CACAO Security Playbooks V2.0.” Accessed: Sep. 30, 2024. [Online]. Available: http://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html

APPENDIX A

Use Cases

The following Use Cases are CACAO Playbook Examples from [46]. The mock-ups were created according to the CACAO roaster project [44], following CACAO Security Playbooks Version 2.0 [47].

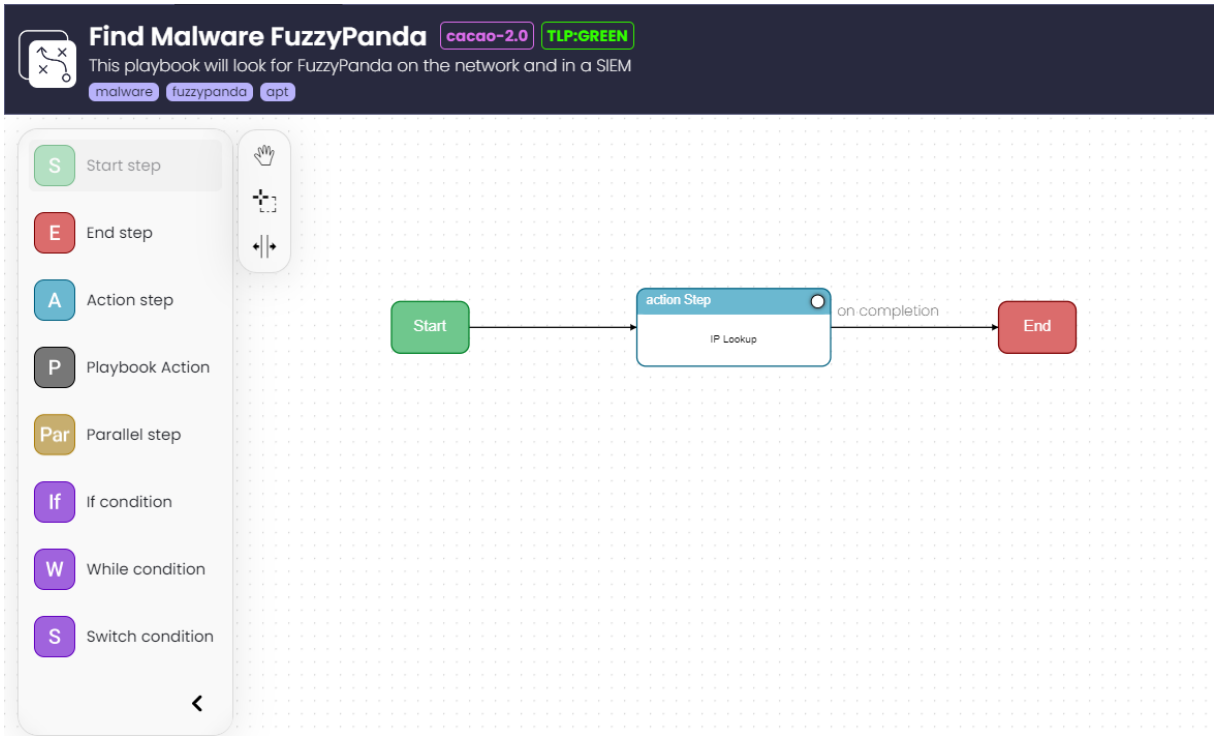
Use Case 1




```
{
  "type": "playbook",
  "spec_version": "cacao-2.0",
  "id": "playbook--fe85f68d-1960-4596-96a2-228113e143cf",
  "name": "Bad MAC Address",
  "description": "This playbook addresses a malicious MAC address,
illustrating an action step, command, and agent/target.",
  "playbook_processing_summary": {},
  "created_by": "identity--351b1469-64b4-4778-8d93-f7949a88990d",
  "created": "2023-02-19T01:09:00.000Z",
  "modified": "2023-02-19T01:09:00.000Z",
  "workflow_start": "start--fa16a4e9-e6b9-4658-b464-ca1632ff57f4",
  "workflow": {
    "start--fa16a4e9-e6b9-4658-b464-ca1632ff57f4": {
      "type": "start",
      "description": "Start example playbook.",
      "on_completion": "action--6398eb05-3eb8-43f5-87d3-f24e07492a41"
    },
    "action--6398eb05-3eb8-43f5-87d3-f24e07492a41": {
```

```
      "type": "action",
      "name": "Block MAC address",
      "description": "This command blocks a MAC address on a switch.",
      "commands": [{
        "type": "ssh",
        "command": "Switch(conf)#mac address-table static 3467.0933.341c
vlan X drop"
      }],
      "agent": "individual--75baba7d-a198-4c5c-805c-af616b4f7a31",
      "targets": ["security-category--3c1daf98-7e22-4e0c-bb8c-
6bd78159ca5d"],
      "on_completion": "end--116cdac5-63f1-4d8f-b3a8-e5667936e9b6"
    },
    "end--116cdac5-63f1-4d8f-b3a8-e5667936e9b6": {
      "type": "end",
      "description": "End of example playbook."
    }
  },
  "agent_definitions": {
    "individual--75baba7d-a198-4c5c-805c-af616b4f7a31": {
      "type": "individual",
      "name": "Network Admin",
      "description": "The admin who responds to an alert by configuring a
switch."
    }
  },
  "target_definitions": {
    "security-category--3c1daf98-7e22-4e0c-bb8c-6bd78159ca5d": {
      "type": "security-category",
      "name": "Switch",
      "category": ["switch"]
    }
  }
}
```

Use Case 2




```
{
  "type": "playbook",
  "spec_version": "cacao-2.0",
  "id": "playbook--61a6c41e-6efc-4516-a242-dfbc5c89d562",
  "name": "Find Malware FuzzyPanda",
  "description": "This playbook will look for FuzzyPanda on the network and
in a SIEM",
  "playbook_types": ["investigation"],
  "playbook_activities": ["analyze-collected-data", "identify-indicators"],
  "playbook_processing_summary": {
    "data_markings": true
  },
  "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
  "created": "2023-02-19T08:00:24.918Z",
  "modified": "2023-02-19T08:00:24.918Z",
  "valid_from": "2023-02-19T08:00:24.918Z",
  "valid_until": "2023-12-31T23:59:59.999Z",
  "derived_from": ["playbook--00ee41a2-c2ca-41da-8ea9-681344eb3926"],
  "priority": 3,
  "severity": 70,
  "impact": 5,
  "industry_sectors": ["aerospace", "defense"],
  "labels": ["malware", "fuzzypanda", "apt"],
  "external_references": [
    {
      "name": "ACME Security FuzzyPanda Report",
      "description": "ACME security review of FuzzyPanda 2021",
```

```
      "source": "ACME Security Company, Solutions for FuzzyPanda 2021,
January 2021. Available online:
hxxp://www[.]example[.]com/info/fuzzypanda2021.html",
      "url": "hxxp://www[.]example[.]com/info/fuzzypanda2021.html",
      "external_id": "fuzzypanda 2023.01",
      "reference_id": "malware--2008c526-508f-4ad4-a565-b84a4949b2af"
    }
  ],
  "markings": [
    "marking-statement--6424867b-0440-4885-bd0b-604d51786d06",
    "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb"
  ],
  "playbook_variables": {
    "__data_exfil_site__": {
      "type": "ipv4-addr",
      "description": "The IP address for the data exfiltration site",
      "value": "1.2.3.4"
    }
  },
  "workflow_start": "start--07bea005-4a36-4a77-bd1f-79a6e4682a13",
  "workflow": {
    "start--07bea005-4a36-4a77-bd1f-79a6e4682a13": {
      "type": "start",
      "name": "Start Playbook Example 1",
      "on_completion": "action--7f40f9d7-de39-4027-ab97-15035beff2ff"
    },
    "action--7f40f9d7-de39-4027-ab97-15035beff2ff": {
      "type": "action",
      "name": "IP Lookup",
      "description": "Lookup the IP address in the SIEM",
      "on_completion": "end--6b23c237-ade8-4d00-9aa1-75999738d557",
      "commands": [
        {
          "type": "manual",
          "command": "Look up IP __data_exfil_site__:value in SIEM",
          "playbook_activity": "identify-indicators"
        }
      ],
      "agent": "group--18d3a2e0-f534-4374-a117-abdddd3e809b"
    },
    "end--6b23c237-ade8-4d00-9aa1-75999738d557": {
      "type": "end",
      "name": "End Playbook Example 1"
    }
  },
  "agent_definitions": {
    "group--18d3a2e0-f534-4374-a117-abdddd3e809b": {
      "type": "group",
      "name": "IR team"
```

```
    }
  },
  "data_marking_definitions": {
    "marking-statement--6424867b-0440-4885-bd0b-604d51786d06": {
      "type": "marking-statement",
      "id": "marking-statement--6424867b-0440-4885-bd0b-604d51786d06",
      "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
      "created": "2023-02-19T08:00:24.918Z",
      "statement": "Copyright 2023 ACME Security Company"
    },
    "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb": {
      "type": "marking-tlp",
      "id": "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb",
      "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
      "created": "2022-10-01T00:00:00.000Z",
      "tlpv2_level": "TLP:GREEN"
    }
  }
}
```


Use Case 3


```
{
  "type": "playbook",
  "spec_version": "cacao-2.0",
  "id": "playbook--fefb9f12-d308-461c-8aa7-a5d6279ab468",
  "name": "LockyBart ransomware",
  "description": "This playbook captures the sequence of steps of how
encrypts files to obtain a ransom using the LockyBart ransomware.",
  "playbook_types": ["attack"],
  "playbook_activities": ["step-sequence"],
  "created_by": "identity--c59f3ff7-2f24-5bd4-a0ed-2fd36ec04b06",
  "created": "2023-05-01T12:08:00.000Z",
  "modified": "2023-05-01T12:08:00.000Z",
  "labels": [
      "ransonware",
      "LockyBart"
  ],
  "external_references": [{
      "name": "Locky Bart ransomware and backend server analysis",
      "url": "https://www.malwarebytes.com/blog/news/2017/01/locky-bart-
ransomware-and-backend-server-analysis"
  }],
  "workflow_start": "start--507aadb2-9f8f-4937-8643-5f50cd358906",
  "workflow": {
      "start--507aadb2-9f8f-4937-8643-5f50cd358906": {
          "type": "start",
          "name": "Start LockyBart ransomware attack",
          "on_completion": "action--cdc2f237-8823-413b-8beb-84a612be0ae8"
```

```
      },
      "action--cdc2f237-8823-413b-8beb-84a612be0ae8": {
          "type": "action",
          "name": "Use a software protection technique",
          "description": "Code virtualization is added to the Locky Bart
binary using WPProtect.",
          "external_references": [{
              "name": "Anti-Static Analysis::Executable Code
Virtualization",
              "source": "mbc",
              "external_id": "B0008",
              "reference_id": "malware-behavior--2cfd6d52-467d-4d05-9091-
b31916218bc2"
          }],
          "commands": [{
              "type": "bash",
              "command": "WPProtect",
              "playbook_activity": "step-sequence"
          }],
          "agent": "group--a757ce82-b838-4c68-9e41-74b0e94211a5",
          "targets": ["software--5e1cadae-7532-45d8-89f8-fe051a1e7df8"],
          "on_completion": "action--3fdb51db-2548-4beb-ab7d-f52b3ab1e5ed"
      },
      "action--3fdb51db-2548-4beb-ab7d-f52b3ab1e5ed": {
          "type": "action",
          "name": " Install LockyBart on victim's endpoint",
          "description": "ftp LockyBart to victim",
          "external_references": [{
              "name": "Command and Control::Ingress Tool Transfer",
              "source": "mitre-attack",
              "external_id": "T1105",
              "reference_id": "attack-pattern--e6919abc-99f9-4c6c-95a5-
14761e7b2add"
          }],
          "commands": [{
              "type": "ftp",
              "command": "ftp malware.victim.com lockybart.exe",
              "playbook_activity": "step-sequence"
          }],
          "agent": "group--a757ce82-b838-4c68-9e41-74b0e94211a5",
          "targets": ["security-category--324ccb41-3306-4876-b017-
1e07a81e16de"],
          "on_completion": "action--7953f6e2-5f09-4fe3-8ffd-476ec5dabe3c"
      },
      "action--7953f6e2-5f09-4fe3-8ffd-476ec5dabe3c": {
          "type": "action",
          "name": "Wipe System Restore Points with VSSadmin",
          "description": "The ransomware deletes any backed-up files",
          "external_references": [{
```

```
                "name": "Impact:: Inhibit System Recovery",
                "source": "mitre-attack",
                "external_id": "T1490",
                "reference_id": "attack-pattern--f5d8eed6-48a9-4cdf-a3d7-
d1ffa99c3d2a"
            }],
            "commands": [{
                "type": "bash",
                "command": "vssadmin.exe delete shadows /all /quiet",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "on_completion": "action--d31e28d1-3584-4f59-a139-6764c6509c6e"
        },
        "action--d31e28d1-3584-4f59-a139-6764c6509c6e": {
            "type": "action",
            "name": "Generate a seed to create a key to encrypt user's
files.",
            "description": "Execute the function used to generate a seed,
which is used to create a key to encrypt the files with. It uses variables
like system time, process ID, thread ID, Process Alive Time, and CPU ticks
to generate a random number",
            "external_references": [{
                "name": "Cryptography::Generate Pseudo-random Sequence::Use",
                "source": "mbc",
                "external_id": "C0021.003",
                "reference_id": "malware-method--82332a69-b4e9-4ce1-a3df-
8d846a5b568e"
            }],
            "commands": [{
                "type": "subroutine",
                "command": "GenerateSeed()",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "on_completion": "action--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d"
        },
        "action--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d": {
            "type": "action",
            "name": "Enumerate the files it wants to encrypt, skipping certain
folders to speed it up",
            "description": "Scan filesystem for user files",
            "external_references": [{
                "name": "Discovery::File and Directory Discovery",
                "source": "mbc",
                "external_id": "E1083",
                "reference_id": "malware-behavior--bd42af9f-9cb2-43c2-948d-
da271591f890"
            }],
```

```
            "commands": [{
                "type": "subroutine",
                "command": "Enumerate()",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "targets": ["security-category--acc1cff5-af87-4caa-8529-
84b08c187653"],
            "on_completion": "action--edd41723-869d-5a07-9971-55876c706533"
        },
        "action--edd41723-869d-5a07-9971-55876c706533": {
            "type": "action",
            "name": "Generate Key using data on victim's endpoint",
            "description": "Locky Bart gathers information on the victim’s
machine to create an encryption key.",
            "external_references": [
                {
                    "name": "Discovery::Process Discovery",
                    "source": "mitre-attack",
                    "url": "https://attack.mitre.org/techniques/T1057/",
                    "external_id": "T1057",
                    "reference_id": "attack-pattern--8f4a33ec-8b1f-4b80-a2f6-
642b2e479580"
                },
                {
                    "name": "Cryptography::Encryption Key",
                    "source": "mbc",
                    "external_id": "C0028",
                    "reference_id": "malware-behavior--99267783-7a99-4ab7-
881f-0dbf52c5bfba"
                }
            ],
            "commands": [{
                "type": "subroutine",
                "command": "Run function to perform action",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "targets": ["security-category--324ccb41-3306-4876-b017-
1e07a81e16de"],
            "on_completion": "action--3f0dc5a7-ffd8-57e1-8b0b-2181638f5c95"
        },
        "action--3f0dc5a7-ffd8-57e1-8b0b-2181638f5c95": {
            "type": "action",
            "name": "Encrypt Files",
            "description": "Encrypt files gathered during a previous step with
the key generated in the previous step",
            "external_references": [{
                "name": " Impact::Data Encrypted for Impact",
```

```
                "source": "mbc",
                "external_id": "E1486",
                "reference_id": "malware-behavior--d2b9f551-8477-424b-8042-
9c4289cb3cfe"
            }],
            "commands": [{
                "type": "subroutine",
                "command": "Run function to perform action",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "targets": ["security-category--191bce6e-2fea-4a7e-b4a5-
c0d96f129a8d"],
            "on_completion": "action--a7fca25a-2ee2-59c0-8df6-9f6ade83e286"
        },
        "action--a7fca25a-2ee2-59c0-8df6-9f6ade83e286": {
            "type": "action",
            "name": "Encrypt key",
            "description": "Encrypt the key used to encrypt the files with a
master key, which now becomes the victim\u2019s UID used to identify them",
            "external_references": [{
                "name": "Cryptography::Encrypt Data::RC4 (C0027.009)",
                "source": "mbc",
                "external_id": "C0027.009",
                "reference_id": "malware-method--77c46dd0-28a7-4b9b-9c62-
849e91f6306a"
            }],
            "commands": [{
                "type": "subroutine",
                "command": "Encrypt key using a public key and RC4 PRGA",
                "playbook_activity": "step-sequence"
            }],
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "on_completion": "action--e742fc09-743d-4174-9edb-1b4bcccd03bb"
        },
        "action--e742fc09-743d-4174-9edb-1b4bcccd03bb": {
            "type": "action",
            "name": "Create and display ransom note",
            "description": "Locky Bart then generates a URL on the
victim\u2019s machine. It contains the link to a TOR cloaked .onion address
where the malicious backend website is hosted. This URL has a user ID within
it. This UID is the original decryption key, in encrypted form. Display the
ransom note on the desktop with the URL to a payment page.",
            "commands": [{
                "type": "subroutine",
                "command": "Create note with URL that contains the encrypted
decryption key",
                "playbook_activity": "step-sequence"
            }],
```

```
            "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",
            "on_completion": "end--0176c66e-9dad-4008-8b4c-bc2d52264557"
        },
        "end--0176c66e-9dad-4008-8b4c-bc2d52264557": {
            "type": "end",
            "name": "Ransomware attack initiated"
        }
    },
    "agent_definitions": {
        "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8": {
            "type": "software",
            "name": "LockyBart",
            "description": "ransomware"
        },
        "group--a757ce82-b838-4c68-9e41-74b0e94211a5": {
            "type": "group",
            "name": "Adversary Group",
            "description": "The threat actor group that runs the LockyBart
malicious website"
        }
    },
    "target_definitions": {
        "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8": {
            "type": "software",
            "name": "LockyBart",
            "description": "ransomware"
        },
        "security-category--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d": {
            "type": "security-category",
            "category": ["filesystem"],
            "name": "Files on endpoint",
            "description": "File system on the victim's endpoint for which to
select files that will be encrypted."
        },
        "security-category--324ccb41-3306-4876-b017-1e07a81e16de": {
            "type": "security-category",
            "category": ["endpoint"],
            "name": "Endpoint with ransomware",
            "description": "Endpoint where the ransomware attack takes place"
        }
    }
}
```

APPENDIX B

Interview Interactions

In interview IT01, the practitioner suggested that the solution could be compared with the MISP Threat Sharing platform[12] to identify potential areas of improvements, namely integrating or developing a plugin/API that allows for the import of playbooks from other tools and solutions, which would enhance the system's interoperability and usability. Another relevant suggestion involved the system's capability to evaluate whether a similar playbook already exists within the database. For this purpose, the expert proposed a mechanism to compare the initial steps of the new playbooks with existing ones to avoid duplication and suggested an autocomplete feature to further reduce redundant efforts for playbook creation. This added feature could be integrated with a recommendation system based on the knowledge already acquired.

Additionally, they identified multiple constraints and deficiencies within the existing artifact, emphasizing concerns pertaining to the management of public and private accessibility, especially in relation to sharing protocols. Moreover, the expert also raised an important question about what criteria was defined to determine the trustworthiness of a playbook.

Additionally, the practitioner emphasized the relevant need for a robust classification and taxonomy system for playbooks. This system would facilitate the comparison of terms and improve the organization of playbooks within the system. They recommended checking for any existing classifications that could be adopted or adapted to suit the needs of the artifact development.

These added suggestions offer significant perspectives on improving the functionality and user experience of the artifact.

In interview IT02, the expert discussed the utility of the solution in the context of the Charter of Trust[13] in the context of sharing information in a structured and low-risk manner. They noted that Siemens could benefit from this solution. The expert found the approach interesting, not only for this reason, but also for internal organizational practical use, where a centralized database of playbooks could be created for everyone to manage and develop work collaboratively. Compared to other solutions used, like Confluence, which does not permit collaborative edits. The expert suggested that, in the future, natural language searches and other advanced solutions could be integrated into the KMS, which is something that Confluence does not currently support. They considered this project an excellent starting point for implementing within the company.

[12] https://www.misp-project.org
[13] https://www.charteroftrust.com/partner/siemens/

The expert also identified a significant limitation of the system, regarding it being open to the public. They highlighted the risk that active users could be identified by their activity, potentially revealing the company they work for and the types of incidents occurring within that company based on the playbooks they create. This presents a security risk due to the lack of association between the user and their company.

In interview IT03, the expert noted their familiarity with CACAO Security Playbooks, although they had no previous knowledge of the KMS concept. They found the idea of the proposed solution very interesting, emphasizing that response playbooks are essential for all organizations. The expert appreciated the concept of tool abstraction, noting its value given that organizations might use different tools over time (e.g., an organization might make the decision of using Tool A today, but tomorrow switching for Tool B) and that, in the future, this system could be used to centralize all the gathered knowledge from different tools.

The expert did not identify any specific limitations or weak points in the current artifact. They identified SOAR, Microsoft, and Palo Alto playbooks as similar tools that do not provide such an overall KMS.

The expert made several additional suggestions to enhance the artifact. They emphasized the importance of establishing a clear relationship between playbook creation and the operational implementation of the tool, posing the question of how to operationalize the proposed solution effectively, for internal organizational use. Followed by the suggested answer of focusing on the top ten solutions currently used in the industry and exploring how to translate the created playbooks to be compatible with the system.

These insights highlight the importance of ensuring that the proposed solution is adaptable to various tools and platforms, facilitating seamless integration and operationalization within different organizational contexts.

In interview IT04, the expert indicated to have previous experience with the MISP platform. They commented positively on the visual output of the playbook, noting that it significantly aids in understanding the IR workflow, particularly when dealing with different branches and added complexity.The expert identified a notable limitation concerning public and private access, specifically regarding sharing control. As an additional suggestion, it has been recommended to integrate the proposed solution with the organization's existing tools.

In interview IT05, the expert stressed the importance of ensuring that playbooks do not include specific malware behavior details, as this could potentially link back to a particular malware family, posing a security risk. The expert did not identify any specific limitations or weak points in the current artifact, nor did they provide additional suggestions.

In interview IT06, the expert highlighted the advantage of using a model similar to Stack Overflow[14] for the proposed solution, emphasizing that leveraging an already validated and approved model could transmit reliability to users. This approach would be particularly effective because the model would not be entirely unfamiliar to them. The expert found the solution to be very intuitive and suggested that it could collect more efficient feedback compared to MISP.

The expert did not identify any specific limitations or weak points in the current artifact.

Additional suggestions included integrating the solution with existing tools, as potential users would likely need to know how to incorporate it with the tools they are already using. The expert recommended moving beyond abstraction and being more concrete about integration possibilities, suggesting the development of a MISP converter. They also advised using feedback elements to continually improve the system, noting that while some features of MISP, such as voting, might not be necessary, the ability to provide and utilize feedback would be crucial.

In interview IT07, the expert emphasized the importance of the proposed concept, noting that risk situations between organizations often share similarities, depending on the business context. The relevance of defining high-level use cases and corresponding playbooks was highlighted. The expert appreciated the concept to a marketplace scenario of generic playbooks, similar to those found in SOAR and antivirus systems. However, it has been noted that the playbooks presented in the interview were more focused on providing a set of instructions based on workflow guidelines IR rather than automation. This approach adds consistency to the use of playbooks by ensuring that response methods are followed systematically.

The expert pointed out the scarcity of public repositories for specific use case playbooks, referring that the collaborative repository adds a lot of value to the solution.

One limitation identified was that detection and remediation playbooks (types of playbooks included in the system) were not connected or related to each other, which could hinder the overall effectiveness of the IR process. Additional suggestions included considering how the playbooks would be implemented in practice. The expert recommended the possibility of exporting playbooks for integration with organizational tools and evaluating how the export material could be converted for daily use. They also stressed the need for specific playbook scenarios tailored for internal organizational use, rather than generic ones.

[14] https://stackoverflow.com/

In interview IT08, the expert mentioned their familiarity with CACAO[15] playbooks and noted that their organization currently uses static playbooks. They recognized the value of transitioning from static to dynamic playbooks, emphasizing that the proposed system allows for playbooks to be dynamic and adaptable over time.

The expert highlighted that creating a playbook repository is a current focus in their IR area. They saw a significant advantage in a collaborative system within organizations, although they noted that this collaborative component could introduce a weakness, particularly if the playbooks include action steps that might lead to man-in-the-middle or DDoS attacks. They advised that external sources used in playbooks should be validated before being updated in public repositories to mitigate this risk.

The expert also commented that if the system's goal is to guide users to the right sources, the approach seems suitable for implementation.

One limitation identified was the quality of information during an incident situation, which is crucial for effective response. In the cases where a playbook is not created for an incident type actions need to be taken, the proposed solution could be a place to look for a playbook suggestion system. In these cases, the interviewer highlighted the importance of ensuring the quality of all playbooks in the KMS.

Additional suggestions included using the same system for an internal repository to transition from static to dynamic and collaborative playbooks. The expert also recommended implementing large language models (LLMs) or a semantic wiki to create a competitive advantage over solutions like Microsoft Copilot.

In interview IT09, the expert expressed strong support for the proposed solution, emphasizing its relevance to the current context of its CSIRT team. They acknowledged that many enterprises already use SOAR tools but noted that the proposed solution serves as an excellent intermediate step for organizations that have not yet reached the level of automation and API integration required by such tools.

[15] https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html

The expert compared the proposed solution to TheHive[16], which facilitates collaboration on playbooks and automates action steps via APIs. The expert compared the proposed solution to TheHive[16], which facilitates collaboration on playbooks and automates action steps via APIs. However, they highlighted that many organizations are not yet ready for such automation and interconnected systems. Therefore, the proposed solution offers a valuable transition from static playbooks, such as those based on Confluence, to a more dynamic and visual approach. This transition can help organizations identify actions that can be automated, as the visual representation of playbooks makes it easier to see which actions can be streamlined.

The expert also noted that static playbooks often lack the visual clarity and workflow consistency provided by the proposed solution. The visualization aspect helps in identifying repetitive and similar steps, making playbook creation clearer and more efficient. Additionally, the proposed solution adds value for training purposes, allowing new employees or trainees with prior cybersecurity knowledge to follow internal playbooks for a better understanding of IR procedures.

One limitation identified by the expert is the potential complexity of playbooks due to the number of action steps and conditions. They suggested including sub-playbooks in the creation process, allowing some playbooks to reference others. For incidents that involve multiple phases of response (e.g., attack, detection, engagement, investigation, mitigation, notification, prevention, and remediation), a high-level playbook should be composed of smaller, related playbooks. If the export format of a playbook is BPMN, the expert recommended including subprocesses related to the high-level playbook.

The expert emphasized that the next step for the proposed solution should be to enable interaction with external platforms via APIs. This would allow the execution of playbooks by automating action steps with the click of a button, further streamlining the IR process.

In interview IT10, the interviewee emphasized the importance of considering ISO 30401:2018[17] during the system's development, as this standard could enhance the overall quality and effectiveness of the proposed solution. They appreciated the collaborative aspect of the system, particularly in supporting CSIRTs, and highlighted that with the introduction of NIS2 directive[18], there is a growing emphasis on collaboration across the European Union. The concept of creating a community focused on playbook development was seen as highly valuable, with the added benefit of establishing a knowledge base that houses a diverse portfolio of playbooks.

[16] https://strangebee.com/

[17] https://www.iso.org/obp/ui/#iso:std:iso:30401:ed-1:v1:en

[18] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

However, the interviewee also pointed out significant limitations. They stressed that the information within the system should be specifically restricted to CSIRT users, even when shared within organizations. They recommended that such discussions could even be discussed with to the Rede Nacional CSIRT[19] (national CSIRT community), ensuring that sensitive knowledge is not broadly disseminated. Additionally, they warned that opening the community to inexperienced users could degrade the quality of the information and knowledge maintained in the system.

While no specific similar tools were mentioned, the interviewee provided insightful suggestions. One key enhancement was the introduction of the ability for users to identify which playbooks are applicable to their specific context, such as those dependent on network architecture or other non-generic elements of a playbook, for example. Furthermore, they suggested incorporating a feature that allows users to distinguish between general, more universal playbooks and those tailored to specific architectures, technologies, or other dimensions within the taxonomy used for playbook management.

[19] https://www.redecsirt.pt