Rafael Yuji Yokowo

Building a Cybersecurity Maturity Guide For Small and Medium-sized Enterprises (SME) With Open Source Solutions

São Paulo, SP

2024

Rafael Yuji Yokowo

Building a Cybersecurity Maturity Guide For Small and Medium-sized Enterprises (SME) With Open Source Solutions

Final project presented to the Department of Computer Engineering and Digital Systems of the Polytechnic School of the University of São Paulo to obtain the Engineering Degree.

Universidade de São Paulo – USP
Escola Politécnica
Departamento de Engenharia de Computação e Sistemas Digitais (PCS)

Supervisor: Prof. Dr. Tereza Cristina Melo de Brito Carvalho
Co-supervisor: Camille Toussaint

São Paulo, SP
2024

Catalogação-na-publicação

Yokowo, Rafael
Building a Cybersecurity Maturity Guide For Small and Medium-sized Enterprises (SME) With Open Source Solutions / R. Yokowo -- São Paulo, 2024.
83 p.

Trabalho de Formatura - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1.Cibersegurança 2.Pequenas e Médias Empresas 3.Guia de Maturidade 4.Open Source I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

This work is dedicated to all those who devote themselves and dream of making the world a better place.

Acknowledgements

I have always believed that I was very lucky to have two mothers who have always given me unconditional support in my decisions and personal projects.

Mãe, Ba, muito obrigado!

Abstract

This work aims to propose a tool to evaluate and better understand the cybersecurity maturity for small to medium-sized enterprises (SMEs) and propose an action plan using open source tools and knowledge. The goal is to be able to reduce the barrier that exists today and facilitate access to and use of the information available. Firstly, this work describes the methodology used to understand the problem and the existing gaps in terms of cybersecurity maturity and risk evaluation. This is achieved mainly through a literature review that points out the current solutions and the challenges faced by SMEs and other stakeholders. Since the objective is to also reach non-technical audiences, there's a dedicated session following the review that introduces cybersecurity terms and technical concepts that will help better understanding the following sections. Once it is all defined, this work introduces the main sources of open source information and tools: the main institutions, public and private organizations, current initiatives and standards in the cybersecurity field. In the end of the section, this work presents some of the existing information security open source tools organized by each of the NIST Cybersecurity Framework (CSF) functions. The proposed cybersecurity tool for SMEs is then introduced with an assessment that helps us analyze the current and target levels of maturity of an organization and what can be done to reach the established objectives based on the given answers. The developed assessment and information are available in a web application created in the scope of this project. Finally, there are concluding remarks that present the main contributions of this work, its limitations and which are the possible next steps in order to develop it even further.

Palavras-chave: cybersecurity, risk, risk management, SME, cyber maturity, risk evaluation tool, NIST, framework

List of Figures

Figure 1 – CISO Assistant analytics dashboard.
Source: Author. 52

Figure 2 – Snipe-IT dashboard.
Source: Snipe-IT Documentation. 56

Figure 3 – Keycloak interface.
Source: Keycloak website. 62

Figure 4 – Zabbix interface.
Source: Zabbix website. 63

Figure 5 – Elastic interface.
Source: Elastic website. 66

Figure 6 – New Relic interface.
Source: New Relic website. 70

Figure 7 – CyberEval's home page. 75

Figure 8 – CyberEval's questionnaire. 75

Figure 9 – CyberEval's results presentation. 76

Figure 10 – CyberEval's open source tools recommendations. 76

List of Tables

Table 1 – Comparison between different tools and solutions proposed in the literature. 20
Table 2 – Open source cybersecurity tools for each one of the CSF functions. 33
Table 3 – Comparison between open-source and commercial/paid solutions. 33
Table 4 – Web application use cases 41
Table 5 – Early Stages expected security practices 45
Table 6 – Organization Establishment expected security practices 46
Table 7 – Organization Growth expected security practices 46
Table 8 – Organization Expansion and Maturity expected security practices 47
Table 9 – SME development levels based on calculated score. 47
Table 10 – Annual costs for the proposed solutions. 73

List of abbreviations and acronyms

SME	Small and Medium-sized Entreprises
NIST	National Institute of Standards and Technology
IT	Information Technology
CISO	Chief Information Security Officer
ISO	International Organization for Standardization
CIS	Center for Internet Security
PCI DSS	Payment Card Industry Data Security Standard
COBIT	Control Objectives for Information and Related Technologies
CSF	Cybersecurity Framework
LiSRA	Lightweight Security Risk Assessment
CET	Cybersecurity Evaluation Tool
4P1C	People, Process, Product, Platform and Compliance
CIA	Confidentiality, Integrity and Availability
DoS/DDoS	Denial of Service/Distributed Denial of Service
ITIL	Information Technology Telecommunications Agency
BCP	Business Continuity Plan
BCM	Business Continuity Management
BIA	Business Impact Analysis
RaaS	Ransomware-as-a-Service
OS	Operational System
API	Application Programming Interface
IoT	Internet of Things
OWASP	Open Worldwide Application Security Project

SDLC	Software Development Life Cycle
OSINT	Open Source Intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
UI/UX	User Interface/User Experience
GUI	Graphical User Interface
GRC	Governance, Risk and Compliance
SSO	Single-Sign On
VPN	Virtual Private Network
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Contents

1 INTRODUCTION 12

1.1 Motivations and Objectives 13

1.2 Organization of This Work 13

2 CONCEPTUAL ASPECTS 15

2.1 Literature Review 15

2.2 Cybersecurity Context 21

2.2.1 Concepts and Principles 22

2.2.2 Information Technology Risks 24

2.2.3 Domains and associated standards 26

2.2.4 Training and Awareness 28

2.3 Open Source Tools and Initiatives 29

2.3.1 Cybersecurity Frameworks 31

2.3.2 Open Cybersecurity Tools 32

2.3.3 Open Source vs Commercial/Paid Solutions 32

2.4 Small to Medium-sized Enterprises 34

3 METHODOLOGY 36

3.1 Theoretical Development 36

3.2 Technical Development 37

3.2.1 Development Methodology 37

3.2.2 Development Schedule 38

3.2.2.1 September: Planning, Design, and Initial Development 38

3.2.2.2 October: Core Development and Feature Implementation 39

3.2.2.3 November: Testing, Improvements, and Deployment 39

3.2.3 Development Tools 40

4 REQUIREMENTS SPECIFICATION 41

4.1 Functional Requirements 41

4.2 Non Functional Requirements 42

5 DEVELOPMENT OF THE WORK 44

5.1 A Guide for SMEs 44

5.1.1 Cybersecurity Assessment 47

5.1.1.1 Govern 47

5.1.1.2 Identify 53

5.1.1.3 Protect 56
5.1.1.4 Detect 63
5.1.1.5 Respond 67
5.1.1.6 Recover 70
5.1.2 Estimated Costs 72
5.2 Application's Technical Overview 73
5.3 Design and Implementation 74

6 CONCLUDING REMARKS 77
6.1 Conclusions of the Graduation Project 77
6.1.1 Contributions to the existing solutions 77
6.1.2 Limitations of this work 78
6.2 Next Steps 78

BIBLIOGRAPHY 81

1 Introduction

In an era of constant and rapid changes in our daily lives, usually driven by the new technologies, it is difficult to have a real-time view of what is happening in the world. The rapid pace at which developments occur prevents us from taking the proper time to study the impact and consequences that the actions taken today will have in the future. The hype generated by the announcements of innovations coming from all sides can distract us from other aspects that are as fundamental to the implementation of new technologies as the technologies themselves, such as the necessary infrastructure, both for the provision of services and for use, social preparation and training for the correct use of the tools and finally cybersecurity.

In recent years, there has been a strong trend towards the digitilization of products and services around the world. The creation of websites, mobile applications, the use of cloud services, chatbots, things that were initially exclusive to large companies with a significant amount capital, are becoming a common reality even for small and medium-sized businesses. Today, with the increased accessibility to new technologies, many businesses are being born in totally digital environments, especially in the world of start-ups. Despite the many benefits that these changes bring to everyday life and the apparent ease with which they can be adapted to people's needs, there are numerous problems that arise as a result of such a modernization: the necessity to create new laws, rules and regulations, establish a governance structure for networks and data, guarantee the protection of privacy, among others.

For companies, especially smaller ones, understanding this reality can still seem abstract, highly technical, complex and expensive, so they are not always sufficiently prepared. Thinking about the case of start-ups, where there are even more basic aspects to be defined for their initial growth, it is understandable that security-related aspects take a back seat. However, the consequences of negligence or lack of knowledge are very real: if an attack causes your data to disappear and your IT system to grind to a halt, what can you do? What's more, small and medium-sized structures are particularly at risk: in the absence of protection systems, they are the main target of malicious agents who maximize their profits by attacking the most vulnerable. And while the best-prepared companies can recover from an attack, others are permanently affected. Despite these difficulties and the restrictions that exist for such companies, we can look at the situation in a positive light: raising awareness and encouraging decision-making from the beginning that promotes the importance of cybersecurity in the context of digital transition and modernization could bring numerous gains. They could be both in terms of avoiding future incidents and in terms of making it easier to expand one's structure without having to make major changes to what already exists.

1.1 Motivations and Objectives

Considering the elements presented, it can be stated that cybersecurity is becoming one of the main pillars that sustain services, applications and businesses in the context of technological development and digital transformation. By analyzing the literature, it is possible to identify various pieces of information that present an analysis of the current state of small and medium-sized enterprises in terms of implementing cyber security measures and policies. In addition, there are studies that even propose tools and structures that can help SMEs better understand their level of protection and identify the main points to be worked on. But, for individuals or small companies with no previous experience in cybersecurity, the task of choosing the best or most adapted approach can become a challenge, as it is difficult to identify where to start. Some of the proposed solutions and frameworks may not be sufficiently adapted to the current needs or too expensive to acquire. Beyond the mentioned challenges, the adoption of open source solutions to deal with the possible high costs of a cybersecurity infrastructure is not trivial. This situation promotes the search for a more generic solution that can act as a first step towards cyber security maturity and serve as a stepping stone to more specific tools. In addition, it creates an opportunity to evaluate the possibility of implementation and potentially harness the use of available tools and information effectively.

Taking these factores into account, this project has an objective of proposing a tool/guide to evaluate and better understand the cybersecurity maturity for small to medium-sized enterprises (SMEs) and help developing an action plan using open source tools and knowledge. The goal is to be able to reduce the knowledge barriers that exist today and facilitate access to and use of the information available.

1.2 Organization of This Work

The project is divided into four main sections that cover its development from end-to-end. It starts with i) a presentation of the main conceptual aspects through a literature review, ii) an introduction of the most important cybersecurity concepts and iii) the available open source tools and initiatives. Following the presentation, this work describes iv) the methodology adopted from a theoretical and from a technical perspectives. The former is related to the assessment and recommendations based on the gathered knowledge in the previous sections while the latter presents the implementation of the web application based on the theoretical tool.

As mentioned, this work begins with a description of the methodology used to understand the problem and the existing gaps in terms of cybersecurity maturity and risk evaluation. This is achieved mainly through a literature review that points out the current solutions and the challenges faced by SMEs and other stakeholders. Since the objective is to also reach non-technical audiences, there's a dedicated session following the review that introduces cybersecurity terms and technical concepts that will help better understanding the following sections. Once it is all defined, this work introduces the main sources of open source information and tools: the main institutions, public and private organizations, current initiatives and standards in the cybersecurity field. In the end of the section, this work presents some of the existing information security open source tools organized by each of the NIST Cybersecurity Framework (CSF) functions. The proposed cybersecurity tool for SMEs is then presented with an assessment that helps us analyze the current and target levels of maturity of an organization and what can be done to reach the established objectives based on the given answers. The assessment is firstly theoretically described and then implemented as a web application accessible on the Internet. Finally, there will be some concluding remarks that present the main contributions of this work, its limitations and which are the possible next steps in order to develop it even further.

2 Conceptual Aspects

2.1 Literature Review

According to the World Bank, in 2019, Small and Medium Enterprises (SMEs) accounted for most businesses worldwide, representing about 90% of businesses and more than 50% of employment worldwide. They play a major role in most economies, particularly in developing countries and emerging economies where formal SMEs contribute up to 40% of national income (GDP). As shown by Onwubiko and Lenaghan (2007) Heidt and Buxmann (2019), in comparison to large companies, we observe that although SMEs have usually a smaller attack surface with less devices and fewer people, they lack the resources that the former has, since big organizations tend to have dedicated staff to deal with cybersecurity infrastructure, issues, controls and policies.

One of the main problems of SMEs regarding cyber threats is due to a faulty risk perception. Renaud and Weir (2016) presents a couple of perspectives regarding how people usually face potential risks to their businesses. It is unlikely that they are unaware of the existing threat since cyberattacks are being increasingly reported in the media in the last years. In this case, it is possible to infer that either there's a miscomprehension of the extent of the risks or people are declining to acknowledge them. According to the authors, personal perspectives and experience play an important role when facing potential risks: some businesses believe that they are too small to be targeted by cyber criminals, others do not trust risk communications from industry and government entities fearing biased recommendations and some choose to deal with the issue later by prioritizing other aspects. Overconfidence can also be an issue, in a survey conducted by Arctic Wolf Networks, it was revealed that 95% of the survey's respondents said their company's cybersecurity posture was at least above average.

Another challenge faced by these businesses is the excessive available information which leads to confusion and doubt Renaud and Weir (2016), Renaud (2016), Clozel (2016). More and more, industry, government and other organizations are making resources available to improve SMEs' cyber awareness, but the wealth of information online is sometimes conflicting. Different companies or countries may prefer to adopt a particular cybersecurity framework as their standard reference, for instance, the United States prioritizes the guidelines provided by their national agency, the National Institute of Standards and Technology (NIST). Given all recommendations, it is up to the business itself to choose which approach to take, but as observed in Osborn and Simpson (2018) and Beachboard et al. (2008), SMEs are struggling with the way to adopt cybersecurity best practices into their organizations, which leaves them in a position of uncertainty.

In the current economy, SMEs adopt the Internet as one of the primary methods to showcase and develop their products and services. They usually dedicate a huge amount of capital in IT infrastructure to enhance and grow their businesses Abbott et al. (2015), but when it comes to the security, SMEs normally tend to not invest in it as much. It can be difficult for senior-level decision makers to see how the business truly gains from an investment in security technologies. It doesn't necessarily increase productivity or reduce costs but can be seen as an insurance policy. They are less likely to employ dedicated IT staff, let alone cybersecurity specialists Sangani et al. (2012). These companies also equate to fewer resources allocated toward cyber defense strategies and usually fail to adopt more advanced cybersecurity technologies due to the high costs Rawindaran, Jayal and Prakash (2021). According to a report published by Deloitte and NASCIO, 75.5% of Chief Information Security Officers (CISOs) cited lack of sufficient budget as a top challenge Deloitte (2014).

In view of these combined factors, SMEs give the impression that they generally have weaker defenses. Given their importance and presence in today's society and economy, they become a valuable target for cybercriminals for financial and political reasons. For instance, in 2017 Keeper Security global statistics, over 60% of small and medium-sized businesses reported experiencing a cyberattack in the previous 12 months. Globally and across all organizations, web application servers appear to be the most targeted IT assets in data breaches largely due to the shift towards web-based applications due to an increasing consumption of services offering cloud-based software-as-a-service platforms Widup et al. (2020). Cyberattacks have huge impacts on businesses ranging from reputational damage, lost customers and contracts, exclusion from supply chains to financial losses related to business, compliance and legal issues, impairing long-term sustainability Renaud and Weir (2016). Small businesses face disproportionately larger costs relative to larger organizations in data breach costs, having to spend about 15 times more in a ration cost per employee than their bigger counterparts Itai and Onwubiko (2018).

The challenge is to find an effective cybersecurity risk evaluation methodology. While there are many information security governance frameworks and resources including ISO, CIS, and COBIT they can be complicated to interpret and evaluate as well as expensive to implement Abraham, Chatterjee and Sims (2018). Below are some summaries and analyses of tools and methodologies proposed in the literature that may provide insights for this study.

Garba and Bade (2021) emphasizes the need for all employees to be knowledgeable about cybersecurity and highlights the importance of using established frameworks to safeguard information systems. It reviews several key cybersecurity frameworks, including NIST, COBIT, HITRUST CSF, and others, offering detailed guidance on their components and applications. The paper uses Halverson and Conradi's taxonomy to analyze these frameworks, providing a valuable resource for organizations to select and implement the most suitable cybersecurity strategies. According to the comparative analysis table elaborated in this work, most of the evaluated frameworks were developed in the United States and all are cybersecurity oriented, designed fully for cybersecurity maturity. While some frameworks target specific industry sectors such as payment (PCI-DSS) and health (HITRUST) organizations, there others that are more generic and are applicable to all type of organizations. For instance, the NIST and COBIT frameworks aims at providing guidance at a higher level, using mixed validation methods and evaluating the practices and the organization's structure. One identified issue with this paper is the fact that the implementation costs of the frameworks are not discussed.

Benz and Chatterjee (2020) highlights the critical importance of cybersecurity for organizations, particularly SMEs, by proposing tailored models based on the sensitivity of assets within different sectors in Saudi Arabia. It presents three specific models for the education, healthcare, and commerce sectors, emphasizing the need for each to gather, analyze, and respond to cyber threats effectively, while also sharing knowledge to improve overall security. To have central command and control for all SMEs, a holistic model is proposed to unify these sector-specific approaches, encouraging collaboration between SMEs to enhance cybersecurity through shared expertise and resources, ultimately strengthening their defenses against organized cyber threats.

Baskerville, Spagnoletti and Kim (2014) provides a different approach in information security strategies by employing practices in prevention and response paradigms. The authors argue that up until recently, the security measures had a prevention-oriented philosophy that although had worked well for decades, may not be fit for the increasing number of unique and one-of-a-kind attacks that we see nowadays. There are fundamental differences between both paradigms, while the prevention strategy focuses on reliable predictions based on historical events and on an exploitation approach, the response one is centered on a reactive and explorative approach on future events. A security incident is what separates the prevention from the response paradigm, the implemented measures to avoid threats were not enough and a disaster recovery plan must be put in place. This study provides a framework that supports the idea of a transition to a broader information security framework that balances both prevention and response paradigms.

Emer, Unterhofer and Rauch (2021) develops a cybersecurity assessment tool for SMEs based on four levels: prerequisites; security management and maintenance; fault management and maintenance (risk and threats management); and network management and maintenance. To fill the levels, a step-by-step procedure is proposed in which concepts and definitions are set and data is collected to determine the maturity levels of the company. This type of solution has advantages as it can be done in a comprehensible format and language and is not time-consuming, but there are some IT terminologies unknown to

SMEs and other disadvantages such as the idea of having a simple tool that may not be able to tackle a complex topic such as the cybersecurity. Among the main threats are the potential disinterest that it may cause in cybersecurity due to the factors above mentioned and the need of constantly update the tool with an exponentially growing number of new risks and threats.

Schmitz and Pape (2020) proposes a lightweight security assessment (LiSRA) to support decision-making regarding the risks an organization is exposed to. The added value of this study is that it provides a simpler and more accessible framework for small and medium-sized enterprises that takes as its input the knowledge of domain experts and the practices and organizational characteristics supplied by users. LiSRA models a framework with the organization's security activities and links them with attack scenarios that are then used to build attack-control trees with the respective security controls. Once the framework is set up, the users can provide their information which will be used in the risk computation where the attack initiation and success probabilities, the impacts and the costs are considered. Given a calculated risk, a recommender application will analyze the most effective and the most cost-efficient security activities based on the maturity level security controls provided by the user to provide recommendations to decrease the identified risk. This work has some limitations as it mainly focuses on one-shot attacks, not being able to respond as efficiently to attackers that may try different strategies while attacking. In addition, the approach is based on attack scenarios provided by the domain expert, if a not previously considered attack happens, the model may not be able to answer properly to the issue.

Nazareth and Choi (2015) provides a system dynamics model that evaluates alternative security management strategies through an investment and security cost lens, to provide managers guidance for security decisions. The model incorporates many aspects of a security practice, including attacks, detection, recovery, risk assessment and vulnerability mitigation. By considering efforts related to vulnerability remediations, recovery and risk assessments, investments in security tools and the probability of attack, this system dynamics model helps prioritizing security investments to reduce further costs and increase the global protection level. Some conducted simulations using the model indicate that investments in security tools designed to detect attacks generate a better return than prevention activities, they also indicate that it is necessary to invest in all areas of security in order to effectively protect information assets.

Ajmi et al. (2019) proposes a methodology that informs SME IT leaders about their cybersecurity risk exposure and provide strategies for risk reduction. It presents a tool and methodology built upon the National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF). While the framework does not meet all the security needs of the SME IT leader, it does offer a strong foundation to develop a useful evaluation and recommendation system. The proposed cybersecurity evaluation tool (CET) focuses on 35 of the 96 standards set by the NIST and provides recommendations under five main topics related to identity, protection, detection, response and recovery. According to the surveys conducted with SMEs, the feedbacks were mostly positive and indicated accurate results, which validates the proposed solution.

In order to have a secure environment, it is important to develop a combination of technical and human (culture and practices that value security) controls among other factors. Differently than implementing technical solutions, a cybersecurity culture in companies, by its nature, needs to be cultivated rather than rigidly designed Uchendu et al. (2021). According to the literature, the most mentioned factor to create such a culture is to have top management support, because without it, cybersecurity initiatives may not appear significant to employees in comparison to their day-to-day tasks. Among the main challenges in this context, we see that security is often viewed as an inhibitor rather than an enabler of business since it adds cost and constraints to the project development. Another aspect is related to awareness and to what extent sanctions can go to employees who fail to assimilate, it is hard to know what to do with high performer employees that perform poorly in sensibilization training for example. Besides finding a way to overcome these challenges, there needs to be a way to measure the progress made in terms of culture adoption. When examining the metrics used to assess cybersecurity culture, questionnaires and surveys are the main instrument for assessing knowledge or awareness of security policy. Although measuring such knowledge may seem useful, it cannot be assumed that it influences behavior since employees may be aware of the policy but might not implement it in their activities due to multiple reasons Fertig, Schutz and Weber (2020). To guarantee a more accurate measure of cyber awareness and culture adoption, a combination of acquiring metrics on both behavior and knowledge that produces a sufficient measurement. It can be achieved through observation methods and roundtables, analysis of policy compliance and training sessions.

In the case of startups, despite the similarities in the cybersecurity maturity level for certain frameworks, according to the systematic literature review done by Marican et al. (2023), the results revealed no singular framework that can evaluate the cybersecurity maturity level of technology startups and a lack of studies on the quantification of the return of cybersecurity investments. The size of these companies is no different from that of a SME, but startups usually rely and thrive on information technology. Adding the budgetary constraints that they face, especially in the earlier stages, the risk they're exposed to is potentially high. The gap analysis proposed by this study identifies that the existing frameworks are not adapted to the stages of the startup lifecycle and that there is no evaluation of the return of security investments which could allow management to make a proper decision when allocating the budget. As seen before, one of the most important ways to increase awareness is having the engagement of top management and the financial factor plays a major role in this context. To address these issues, the article proposes a framework based on the 4P1C (People, Process, Product, Platform and Compliance) domains and three phases (Risk Assessment and Actions, CyberSecurity Maturity Level and Cyber Quantification) which consider the particularities of startups.

Table 1 – Comparison between different tools and solutions proposed in the literature.

Reference	Line of Work	Strengths	Weaknesses
Garba and Bade (2021)	Analysis of existing cybersecurity frameworks	Provides information and a comparison regarding different existing frameworks, which helps the decision-making process.	Does not develop all of Halverson and Conradi's taxonomy, especially the implementation costs.
Benz and Chatterjee (2020)	Tailored cybersecurity models for essential industry sectors	Identifies a way of sharing process and knowledge to increase reach and efficacy of cybersecurity efforts.	The discussion is rather shallow and there's no technical information or implementation details.
Baskerville, Spagnoletti and Kim (2014)	Practices in prevention and response paradigms	Presents a different approach in information security strategies by dealing with risk with both prevention and response practices.	Finding the right balance between both paradigms varies depending on the industry and is a challenging and costly task.
Emer, Unterhofer and Rauch (2021)	Cybersecurity assessment tool	Developed in a comprehensible format and language and is not time-consuming.	It is not able to address complex security concepts and it has unknown IT terminologies to some SMEs.
Schmitz and Pape (2020)	Decision-making supporting tool for risk analysis	Provides a simpler and more accessible framework for SMEs that is adapted to the business activities.	Mainly focuses on one-shot attacks and cannot address scenarios that did not occur.
Nazareth and Choi (2015)	Analysis of security management strategies in terms of investments and other costs	Helps with business decisions by providing financial impact information to management.	Does not work as a standalone risk evaluation tool, but can be used as a complementary one.
Ajmi et al. (2019)	Methodology to inform management of risk exposure	Provides a strong foundation to develop an evaluation and recommendation system based on the NIST framework.	Does not cover all security needs essential to a SME IT leader.
Uchendu et al. (2021)	Development of a cybersecurity culture	Highlights how the adoption of a cybersecurity culture helps increasing the importance and utility of security measures within an organization.	There's no clear solution of how to achieve the objectives since it varies according to the organization's activities, size, type, etc.

Source: Author.

The discussion about the importance of cybersecurity has been growing in recent years, especially in view of the context of technological development. Through this literature review, it was possible to identify several studies that present an analysis of the current state of small and medium-sized enterprises in terms of implementing cybersecurity measures and policies. In addition, some studies go a step further and propose tools and frameworks that can help SMEs better understand their level of protection and identify the main points to work on. As indicated in multiple articles and observed in this review, there are multiple sources of information on the internet with sometimes conflicting information which can cause confusion and mistrust. For people or small companies with no expertise in cybersecurity, the task of choosing the best or most adapted approach becomes a challenge, it is hard to identify where to start. In addition, some of the proposed solutions and frameworks may not be adapted to some SMEs, raising a potential need of a more generic solution that may work as a first step towards a cybersecurity maturity and may serve as a steppingstone to the more specific tools. Finally, there's a gap in terms of the adoption of open source solutions to deal with the potential high costs of a cybersecurity infrastructure, this creates an opportunity of taking advantage of using the available tools and information in an effective way.

2.2 Cybersecurity Context

When we think of cybersecurity, the first image that comes to mind is usually of a hacker trying to break into a system or steal some kind of information, as shown in the movies. However, its definition and scope go far beyond that. Cybersecurity is the practice of protecting computers and servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also called information technology security or electronic information security. The term is applicable to a variety of contexts, from business to mobile computing, and can be divided into a few common categories such as network, applications and data security, business continuity, disaster or incident recovery, training and awareness and many others.

The world of information systems, consisting of networks, complex digital architectures and data, is taking on an increasingly important role and place in companies. We see today, especially in the media, that these systems are vulnerable and prone to attacks of various kinds, such as ransomware, unavailability of services, data theft, among others. In this sense, guaranteeing the security of information systems is no longer an additional measure, but a fundamental principle in the growth and establishment of companies.

2.2.1 Concepts and Principles

The security management concepts and principles are inherent elements in a security policy and solution deployment which define the basic parameters needed for a secure environment. They also set the goals and objectives that both policy designers and system implementers must achieve to create a secure solution. Generally speaking, the cybersecurity covers three main objectives that are usually called the CIA triad which stands for Confidentiality, Integrity and Availability as described by Carpentier (2016).

- **Confidentiality** is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources. The goal of confidentiality protection is to prevent or minimize unauthorized access to data. Confidentiality focuses security measures on ensuring that no one other than the intended recipients of a message receive it or are able to read it. Confidentiality protection provides a means for authorized users to access and interact with resources, but it actively prevents unauthorized users from doing so. A wide range of security controls can provide protection for confidentiality, including, but not limited to, encryption, access controls, and steganography.

- **Integrity** is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data. It ensures that data remains correct, unaltered, and preserved. Properly implemented integrity protection provides a means for authorized changes while protecting against intended and malicious unauthorized activities as well as mistakes made by authorized users. For integrity to be maintained, objects must retain their veracity and be intentionally modified by only authorized subjects. If a security mechanism offers integrity, it offers a high level of assurance that the data, objects, and resources are unaltered from their original protected state. Alterations should not occur while the object is in storage, in transit, or in process. Thus, maintaining integrity means the object itself is not altered and the operating system and programming entities that manage and manipulate the object are not compromised.

- **Availability** is the concept in which authorized subjects are granted timely and uninterrupted access to objects. Often, availability protection controls support sufficient bandwidth and timeliness of processing as deemed necessary by the organization or situation. If a security mechanism offers availability, it offers a high level of assurance that the data, objects, and resources are accessible to authorized subjects. Availability includes efficient uninterrupted access to objects and prevention of denial-ofservice (DoS) attacks. Availability also implies that the supporting infrastructure—including network services, communications, and access control mechanisms—is functional and allows authorized users to gain authorized access. For availability to be maintained on a system, controls must be in place to ensure authorized access and an acceptable level of performance, to quickly handle interruptions, to provide for redundancy, to maintain reliable backups, and to prevent data loss or destruction.

In addition to these three main objectives, it is worth noting that there are other important security principles that can be established as the basis of a company policy:

- **Non-repudiation** is a service that is used to assure of the integrity and origin of data in such a way that they can be verified and validated.
- **Authentication** is the process through which an individual, application, or machine goes through that verifies that they are who they say they are before gaining access to information systems.

Not only the definition of objectives is essential, but also how we manage what is created and developed. The continuity of the information systems concerns multiple subprocesses within a company such as the conception of security controls, security tests, incident management for example. Since the technology is one of the main components of most of the business processes nowadays, a high disponibility of the information systems is critical to the continuity of the services. The Information Technology Infrastructure Library (ITIL), a guide created by the British's Central Computer and Telecommunications Agency, provides a set of recommendations designed to standardize IT management practices across government functions. The latest version of the guide references the management of the continuity of the services as the practice of the services management. It establishes some base concepts and principles such as:

- Business Continuity Plan (BCP): it is a plan that describes and defines the steps to bring back up the business process after the occurrence of an incident. It also identifies the stakeholders of the organization to be informed and accountable for the actions and recovering measures.
- Business Continuity Management (BCM): it concerns the management of the risks that might have a significant impact on the business activities with the objective of bringing them down to an acceptable level and creating a progressive recovery plan in case of service unavailability.
- Business Impact Analysis (BIA): it qualifies the consequences that a business activity disruption could bring to an organization. It takes into account the elements such as who is going to take the damage of the disruption, how would the damages increase if an incident occurs, what are the vital personnel and assets to ensure the minimum business continuity and time indicators for the recovery of the critical resources.

- Continuous Improvement: it is a process that focuses on the optimization of the IT services to increase quality and performance while reducing potential risks.

2.2.2 Information Technology Risks

There are numerous threats to these security principles, we can call them cybersecurity threats or, in short, cyber threats. They are an indication that a malicious agent is trying to gain unauthorized access to a resource, such as a network, system or database, with the aim of launching a cyber attack. Cyber threats can take many different forms: a fake email indicating legal or financial irregularities linked to your name, malicious files with codes that allow someone to steal your data, an attempt to make a service unavailable, etc. The attacks are usually classified into five main categories:

- Malware: a software designed to harm computer systems or users. It's a key component in modern cyberattacks, allowing threat actors to gain unauthorized access, destroy data, steal information, and render systems inoperable. Common types include trojans, which deceive users into downloading malicious code, spyware, which gathers sensitive information covertly, and worms, which spread autonomously across devices.

  Among these attacks, one that has been gaining traction over the last few years is the ransomwares, presenting a worrying resurgence in 2023. As presented by WeForum, Hackers are increasingly targeting IT and physical supply chains, launching mass cyberattacks, and finding new ways to extort money from businesses, large and small. Ransomware activity alone was up 50% year-on-year during the first half of 2023 with so-called Ransomware-as-a-Service (RaaS) kits, where prices start from as little as $40, a key driver in the frequency of attacks.

- Social Engineering and Phishing: social engineering involves manipulating individuals to compromise personal or organizational security, often by divulging confidential information or risking financial harm. Phishing, the most common form, employs fraudulent emails, attachments, texts, or calls to deceive recipients into sharing personal data, login credentials, or money with cybercriminals, or to download malware.

- Man-in-the-middle: In this type of attack, a malicious agent eavesdrops on a network connection to intercept and relay messages between two parties and steal data.

- Denial of Service: it is a cyberattack that overloads a website, application or system with volumes of malicious traffic, making it too slow to use or completely unavailable to legitimate users. A distributed denial-of-service attack, or DDoS attack, is similar, except that it uses a network of devices or bots connected to the Internet and infected with malware, known as a botnet, to paralyze or crash the target system.

- Zero-day exploits: it is a type of cyber attack that takes advantage of a zero-day vulnerability, an unknown or yet unpatched or unpatched security flaw in computer software, hardware or firmware. "Zero-day" refers to the fact that a software or device vendor had no time to fix vulnerabilities because malicious actors can already use them to gain access to vulnerable systems.

When talking about cyberthreats, a fundamental concept to be discussed is the attack surface of a given target. An organization's attack surface is the sum of vulnerabilities, pathways, or methods - sometimes called attack vectors - that hackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack. There are two main types of attack surface to be considered when analyzing a modern organization: the digital and the physical surfaces.

The digital attack surface potentially exposes the organization's cloud and on-premises infrastructure to any hacker with an internet connection. According to IBM, common attack vectors in an organization's digital attack surface include:

- Weak passwords: Passwords that are easy to guess—or easy to crack via brute-force attacks—increase the risk that cybercriminals can compromise user accounts to access the network, steal sensitive information, spread malware and otherwise damage infrastructure.
- Misconfiguration: Improperly configured network ports, channels, wireless access points, firewalls, or protocols serve as entry points for hackers. Man-in-the-middle attacks, for example, take advantage of weak encryption protocols on message-passing channels to intercept communications between systems.
- Software, OS, and firmware vulnerabilities: Hackers and cybercriminals can take advantage of coding or implementation errors in third-party apps, OSs, and other software or firmware to infiltrate networks, gain access to user directories, or plant malware.
- Internet-facing assets: Web applications, web servers and other resources that face the public internet are inherently vulnerable to attack. For example, hackers can inject malicious code into unsecured application programming interfaces (APIs), causing them to improperly divulge or even destroy sensitive information in associated databases.
- Shared databases and directories: Hackers can exploit databases and directories that are shared between systems and devices to gain unauthorized access to sensitive resources or launch ransomware attacks.

- Outdated or obsolete devices, data, or applications: Failure to consistently apply updates and patches creates security risks.
- Shadow IT: "Shadow IT" is software, hardware, or devices—free or popular apps, portable storage devices, an unsecured personal mobile device—that employees use without the IT department's knowledge or approval. Because it's not monitored by IT or security teams, shadow IT may introduce serious vulnerabilities that hackers can exploit.

  The physical attack surface exposes assets and information typically accessible only to users with authorized access to the organization's physical office or endpoint devices (servers, computers, laptops, mobile devices, IoT devices, or operational hardware).
- Malicious insiders: Disgruntled or bribed employees or other users with malicious intent may use their access privileges to steal sensitive data, disable devices, plant malware or worse.
- Device theft: Criminals may steal endpoint devices or gain access to them by breaking into an organization's premises. After they are in possession of the hardware, hackers can access data and processes that are stored on these devices. They might also use the device's identity and permissions to access other network resources. Endpoints used by remote workers, employees' personal devices, and improperly discarded devices are typical targets of theft.
- Baiting: Baiting is an attack in which hackers leave malware-infected USB drives in public places, hoping to trick users into plugging the devices into their computers and unintentionally downloading the malware.

2.2.3 Domains and associated standards

ISO

Among the existing cybersecurity standards, the ISO 27001 has become a benchmark in terms of information systems security. The ISO 270xx standards cover multiple cybersecurity domains, setting principles and listing good practices to ensure the security of an organization or system. These standards, developed by the International Organization for Standardization (ISO), are widely recognized and adopted globally, providing a common language and set of practices for securing information systems.

The importance of these ISO standards lies in their ability to provide a structured approach to managing information security risks. By adopting them, organizations can demonstrate their commitment to protecting data, which is increasingly important in a world where cyber threats are pervasive. For instance, compliance with ISO/IEC 27001, can help organizations gain the trust of customers, partners, and regulators by showing that they have a robust information security management system in place. In big organizations, it is a common practice to analyze if external suppliers, with whom there's a desire to establish a partnership, have the proper ISO certifications. This usually indicates that such supplier is less prone to bring risks with its services and products, which is beneficial for both parties. Additionally, these standards facilitate continuous improvement, ensuring that security measures evolve in response to emerging threats and technological advancements.

In practice, organizations use ISO standards as a roadmap for developing, implementing, and maintaining their cybersecurity strategies. The process typically begins with a gap analysis to assess current security measures against the requirements of the standard. This is followed by the development of an ISMS, which includes policies, procedures, and controls tailored to the organization's specific needs and risks. Regular internal audits and reviews are conducted to ensure ongoing compliance and to identify areas for improvement.

NIST

The National Institute of Standards and Technology (NIST) is a U.S. federal agency that develops and promotes standards, guidelines, and best practices to enhance cybersecurity across various sectors. NIST's work in cybersecurity is highly regarded globally, providing a robust framework for organizations to protect their information systems and data. The published standards provide a detailed, methodical approach to securing information systems that is adaptable to organizations of all sizes and across industries. By following NIST guidelines, organizations can build robust security programs that align with best practices and regulatory requirements. In addition, among the most influential NIST publications is the NIST Cybersecurity Framework (CSF) which will be furtherly discussed.

Another key NIST standard is NIST Special Publication 800-53, which provides a comprehensive catalog of security and privacy controls for federal information systems and organizations. This publication is widely used not only by federal agencies but also by private-sector organizations looking for a thorough and detailed set of security controls. They are designed to address a wide range of security requirements, including access control, incident response, contingency planning, and system and communications protection. The publication also emphasizes the importance of continuous monitoring and assessment to ensure the effectiveness of security measures over time.

Organizations utilize NIST standards in various ways to enhance their cybersecurity posture. For example, many organizations conduct a risk assessment using the NIST Cybersecurity Framework to identify vulnerabilities and prioritize security investments and the NIST SP 800-53 as a reference for selecting and implementing security controls that address specific risks identified during this assessment. In practice, adopting NIST standards involves integrating them into an organization's overall risk management strategy. This might include developing policies and procedures based on NIST guidelines, conducting regular security assessments, and continuously monitoring and updating security controls. Many organizations also seek third-party assessments or audits to validate their adherence to NIST standards, which can be particularly important for those working with government agencies or in regulated industries.

2.2.4 Training and Awareness

Training and awareness in cybersecurity are vital for organizations of all sizes, but they are particularly crucial for small to medium-sized enterprises. Without adequate training and awareness, employees in may inadvertently become the weakest link in the security chain, leading to data breaches, financial loss, and damage to the organization's reputation. We observe that SMEs often face significant challenges in protecting their information systems due to limited resources, making them prime targets for cyberattacks. As seen in the literature review, creating and establishing a culture of cybersecurity awareness through regular training is essential to mitigating risks and it must be cultivated rather than rigidly designed. Other aspect is making top management aware of potential risks and the ways of avoiding or mitigating them, it helps guiding more budget and investments into security infrastructure.

For SMEs, where the IT staff may be limited or even non-existent, employees across all departments must understand the basics of cybersecurity. Training programs should focus on educating staff about common threats such as phishing, ransomware, and social engineering, which are often the initial attack vectors. Employees should be trained to recognize suspicious emails, understand the importance of strong passwords, and follow best practices for data protection. Additionally, awareness initiatives should highlight the role of each employee in maintaining the security of the organization, from safeguarding sensitive information to reporting potential security incidents. It is always recommended that personnel with privileged accesses or high-risk roles have advanced trainings to ensure the organization's services and assets safety.

Lately, the importance of cybersecurity training in SMEs is further amplified by the growing prevalence of remote work and cloud-based services, which expand the attack surface. Employees working remotely may be using personal devices or unsecured networks, increasing the risk of a cyber incident. Regular training helps ensure that employees are aware of these risks and know how to protect themselves and the organization, regardless of where they are working. One common example is the adoption of VPN connections to access the organization's resources while using public internet networks.

Moreover, cybersecurity awareness programs can help SMEs comply with regulatory requirements and industry standards. Many regulations, such as the General Data Protection Regulation (GDPR), require organizations to implement employee training as part of their security measures. By investing in training, SMEs not only enhance their security posture but also reduce the risk of costly fines and legal penalties associated with non-compliance.

2.3 Open Source Tools and Initiatives

Open source tools and initiatives represent a collaborative approach to software development, in which the source code is made freely available for anyone to view, modify and distribute. These projects are usually driven by communities of developers and enthusiasts who contribute their knowledge and efforts to improve the software. An important aspect of open source is transparency, as the code and the information are open to inspection by anyone, which promotes responsibility and trust. This model encourages innovation by allowing rapid iteration and adaptation to evolving needs and challenges. In software development, there is a well-known expression called Linus' law which says: given enough eyeballs, all bugs are shallow, and this is one of the great advantages of having a community working together in search of solutions.

The motivations behind the creation of open source projects vary, but generally include ideals of collaboration, democratization of technology and the desire to solve common problems. Many developers are attracted to open source because of the freedom it provides to explore and experiment with the code, as well as the opportunity to contribute to projects that align with their interests or values. In addition, open source projects can benefit from the collective wisdom and diverse perspectives of a global community, leading to more robust and secure solutions. Nevertheless, open source doesn't only apply to source code or software projects; the definition can be extended to the notion of open data where there is a sharing of knowledge around a given subject.

In the field of cybersecurity, open source tools and initiatives play an important role in improving defenses against cyberattacks. By making security tools openly accessible, experts and organizations can collaborate on developing and improving defenses against evolving threats and the transparency of open source code allows for full review and auditing, helping to identify and correct vulnerabilities more efficiently. This collective effort strengthens the cybersecurity posture for both individual users and organizations, enabling them with tools and resources to better protect their digital assets and data. In addition, open source promotes interoperability and standardization, facilitating integration between different security solutions and fostering a more resilient cybersecurity ecosystem. Overall, these initiatives serve as a stepping stone in the fight against cyberthreats, incorporating principles of collaboration, transparency and innovation. The following are some of the main initiatives and tools that exist today with a focus on cybersecurity:

OWASP

The Open Worldwide Application Security Project (OWASP) is an open community that develops open source projects including code, reference material, documentation and standards and works to improve the security of software worldwide. The OWASP is mostly known in the application security community that profits from projects such as the OWASP Top Ten which represents a broad consensus about the most critical security risks to web applications. This community is fundamental for an efficient secure Software Development Life Cycle (SDLC).

RedHat

RedHat Inc. is a software company, subsidiary of IBM, that provides open source software, storage, operating system platforms, middleware, applications, management products, support and training. The company is also present in the cybersecurity field, providing frequent reports on best practices, the state of the technologies, vulnerability alerts and compliance issues.

OSINT

OSINT stands for "Open Source Intelligence" and it concerns information that is accessible to all and unclassified, being a fundamental to intelligence operations. Very often, OSINT is put to good use in the fight against terrorism, cyberthreats, fraudulent financial practices and a whole myriad of illegal activities. It is therefore a cell of activity that is just as valuable for states as it is for companies. OSINT is not an organization or a software, but a method of gathering and analyzing information from public or other open sources with the purpose of answering a specific intelligence question. This tool can be used by companies to better understand their activities and the risk that they are exposed to, based on the experience and knowledge of others.

ANSSI

Created in 2009, the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is the national authority for cybersecurity in France. Placed under the authority of the Prime Minister and reporting to the General Secretary for Defense and National Security, it is ideally placed to deploy a global cybersecurity policy and coordinate it at interministerial level. This policy aims to defend the most critical public and private digital infrastructures. ANSSI also addresses all the players involved in the country's digital transformation and fosters the conditions for trust-based dialogue with its counterparts at European and international level. In addition to all contributions in terms of technical knowledge about cybersecurity subjects, the ANSSI also makes the access to information easier to people from other domains. Reducing the knowledge barriers creates an opportunity to increase the awareness regarding information security topics.

2.3.1 Cybersecurity Frameworks

One of the main references in the cybersecurity field in terms of standards and frameworks is the NIST Cybersecurity Framework (CSF). It is an open source tool that provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks, by offering a taxonomy of highlevel cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF has a core - a set of cybersecurity outcomes – which has 6 main functions - GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER that organize cybersecurity outcomes at their highest level.

They do not represent actions to be taken and may not be followed in a specific order, it all depends on the organization and the people responsible for the actions. Ideally, the functions should be addressed concurrently and happen continuously within an organization. Here are the descriptions provided by the NIST for each one of them:

- GOVERN (GV) — The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
- IDENTIFY (ID) — The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.
- PROTECT (PR) — Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training;

data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

- DETECT (DE) — Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- RESPOND (RS) — Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- RECOVER (RC) — Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

2.3.2 Open Cybersecurity Tools

The internet has been transforming how we approach cybersecurity, turning it into a collaborative endeavor rather than a solitary battle. The online communities composed by enthusiasts, professionals, and hobbyists alike, behind the open source tools are a testament to this shift, contribute to continuous improvement and real-time problem-solving. The collective vigilance brough by these communities ensures that these tools remain up-to-date and responsive to new threats. This approach to cybersecurity creates a culture of shared responsibility and continuous learning, which aims to make the digital world a safer place for its users. Unfortunately, there is no silver bullet solution to all the cybersecurity problems we face today. However, by pooling the contributions made by online communities, it is possible to find ways of reducing the barriers to access to a status of greater protection for systems, data and people in companies.

In order to give a better idea of how this task can be done, below are a list of several tools available today with free open source versions divided into different categories following the functions of the NIST CSF presented earlier.

2.3.3 Open Source vs Commercial/Paid Solutions

One feature of open source solutions is the possibility of acquiring a service with more functionalities for a certain fee. This is one of the ways of keeping the project funded

Table 2 – Open source cybersecurity tools for each one of the CSF functions.

CSF Function	Tool name	Use cases
GOVERN	CISO Assistant	Risk Management
	OpenRMF	Risk and Compliance Management
IDENTIFY	Snipe-IT	IT Asset Management
PROTECT	Keycloak	Identity and Access Management
	Veracrypt	Encryption (Data and Asset Security)
	openssl	Encryption (Data Security)
	Synk Open Source	Risk Management for Developers
	Zabbix	Infrastructure and Cloud Monitoring and Analysis
DETECT	ELK stack (Elastic)	SIEM
	Cacti	Monitoring and Fault Management Framework
	Wireshark	Network Monitoring and Analysis
	Maltego	Forensics
	Nmap	Network Monitoring and Analysis
	Metasploit	Pentest and IDS solution
RESPOND	New Relic	End-to-end monitoring services
RECOVER	Velero	Kubernetes Disaster Recovery Tool
	Linbit	Disaster Recovery Tool

Source: Author.

with the help of the community to develop solutions. In general, the following patterns can be observed:

Table 3 – Comparison between open-source and commercial/paid solutions.

Characteristics	**Open Source**	**Commercial/Paid Solutions**
Cost	Free	Subscription or acquisition fee
Features	Basic functionalities or complete package without support or infrastructure	Complete package with support or infrastructure
Solution Implementation	Self-managed by the user	Hosting and management done by the service
Support	Limited or no dedicated support	Base to Premium support offered according to the subscription plan
Usage	Limited access or memory	Usage levels change according to the chosen plan

Source: Author.

For most of the open source tools available, there is a free offer to use the services and functionalities, but it requires a technical understanding of these for correct implementation and use. Despite this limiting characteristic, paid-for options still present affordable choices, allowing them to be adopted even with more restrictive budgets.

2.4 Small to Medium-sized Enterprises

Small to medium-sized enterprises (SMEs) are businesses that typically fall below certain thresholds in terms of employee count, revenue, and sometimes asset size, depending on the industry and location. Generally, small enterprises employ fewer than 50 people and have annual revenues under $10 million, while medium enterprises employ between 50 and 250 people with revenues ranging up to $50 million. SMEs are widely recognized for their role in economic growth, innovation, and job creation, particularly in emerging markets. Although SMEs play a major role in the economy, they often operate with limited budgets, which can make it challenging to allocate resources toward areas outside their core business, such as cybersecurity measures.

While traditional SMEs are often characterized by steady growth and local market focus, tech-driven SMEs — especially startups — are distinguished by their technological orientation and growth potential. These modern SMEs use technology to promote innovation, scalability, and expansion, making them distinct from more conventional small businesses. As they embrace these pillars, they also face cybersecurity risks. It encompasses a broad set of practices aimed at safeguarding information, systems, and assets from various cyber threats. Cybersecurity for SMEs includes protecting computers, mobile devices, electronic systems, networks, and data from unauthorized access and attacks, and it covers several areas such as network security, application security, and data protection.

For startups and SMEs focused on innovation and product development, cybersecurity becomes essential for protecting the R&D process and services. By securing their intellectual property and sensitive data, these companies protect against threats that could lead to leaks, unauthorized access, or sabotage. This protection is crucial as these enterprises leverage advanced technologies like artificial intelligence (AI), Internet of Things (IoT), and cloud computing, which increase their attack surfaces and, consequently, their exposure to cyber threats.

In terms of digital and cloud infrastructure, SMEs and startups increasingly depend on cloud services and software-as-a-service (SaaS) platforms to streamline operations, store data, and scale rapidly. However, these infrastructures, though efficient, present vulnerabilities that must be managed continuously. Common attack vectors include weak passwords, misconfigured ports, and software vulnerabilities, which hackers exploit to gain access, spread malware, or disrupt services. To secure their digital infrastructure, these companies often implement encryption, multi-factor authentication, and continuous vulnerability assessments. Additionally, the rise of shadow IT poses a risk, as it introduces unsecured pathways that bypass traditional security protocols.

As these businesses grow and reach a wider user base, they become more, as shown previously, attractive targets for cyber threats, including phishing, ransomware, and DoS attacks. To ensure uninterrupted growth, scalable cybersecurity practices must be established early on. This includes not only technical defenses but also policies for incident response, business continuity, and disaster recovery.

3 Methodology

3.1 Theoretical Development

The methodology of this work begins with an extensive literature review to identify the current state of cybersecurity practices, objectives and perspectives from academic and industry actors with the aim of finding the existing gaps and main challenges faced by SMEs and other related stakeholders. The review covers a broad range of academic papers, industry reports, and expert opinions, aiming to provide a comprehensive understanding of the cybersecurity landscape for SMEs. The findings stress the areas where SMEs struggle the most, such as limited resources, lack of expertise, and inadequate security measures, forming the foundation for the development of this work. In addition to the existing gaps, we seek the best practices currently in place in order to use what is working well to reinforce the solution that will be proposed. To search for the papers, this work:

- used online platforms such as IEEExplore, Elsevier, arXiv, ResearchGate and Google Scholar;
- had an article selection based on the combination of some main keywords: information security, cybersecurity, risk management, open source tools, risk assessment, cybersecurity maturity, SME, startups, training and awareness, security frameworks, etc.

Recognizing that the target audience includes non-technical stakeholders, the work dedicates a session to introducing fundamental cybersecurity terms and concepts. This educational segment is crucial for bridging the knowledge gap, ensuring that all readers have a basic understanding of cybersecurity principles regardless of their technical background. By simplifying complex terminology and explaining the importance of various security practices, this section empowers SMEs to engage with the subsequent material more effectively. It serves as a guide that demystifies cybersecurity, making the subject more accessible for non-experts. The information presented comes from a combination of data found in reports from companies such as IBM, Deloitte and in textbooks on information security.

Following the introduction to cybersecurity concepts, this work identifies key open-source information sources and tools that SMEs can utilize to enhance their cybersecurity posture. It lists the main sources of reliable information from institutions recognized by the community and government organizations. As for the tools, based on the results of the literature review and other research using the keywords presented, some open source solutions that respond to security needs will be presented and organized according to the recommendations and structure of this work. In view of this, this session provides practical resources that can be directly implemented within the action plans.

Finally, the core of the methodology is presented: a comprehensive cybersecurity maturity assessment based on the NIST Cybersecurity Framework 2.0. This framework was chosen for two main reasons: The NIST documentation is freely available worldwide, which makes it the most accessible documentation for studying and understanding GRC concepts. In addition, the NIST security and privacy controls are mapped to the ISO 27000 and COBIT controls, making it possible to translate the controls between the frameworks. The tool synthesizes the insights from the literature review and addresses the identified gaps and challenges. By leveraging the structured approach of the NIST framework, it offers tailored recommendations and a potential roadmap for SMEs to elevate their cybersecurity maturity, ensuring that the proposed solutions are practical, actionable, and aligned with the specific needs of small and medium-sized businesses.

3.2 Technical Development

Based on the theoretical study and literature review carried out, this work develops a technical implementation of the concepts seen. The aim is to create a simple, but informative, web application which will serve as a tool for companies to assess their level of cybersecurity maturity and create an action plan based on the results.

3.2.1 Development Methodology

The development of the application follows an iterative and incremental approach, focusing on delivering functional and testable components in stages, allowing for continuous feedback and refinement. This methodology is designed to align with the theoretical solution and ensures flexibility in the development process. Below are the main principles of the adopted methodology:

1. Planning and Requirements Gathering

   At the initial stage, all key requirements are derived from the theoretical solution. This includes identifying core functionalities, user interface elements, and necessary interactions that the frontend must support. The main goal is to convert the theoretical concepts into concrete features for the application.

2. Component-Based Design

   With a component-based architecture, the application is divided into independent, reusable UI components. Each component encapsulates a specific functionality, which promotes modular development. This modular approach simplifies future updates and maintenance while ensuring consistency across the user interface.

- UI/UX Design: Wireframes and mockups are created to define the visual structure and interaction flow. These designs are based on user experience best practices, ensuring intuitive and efficient navigation.
- Prototyping: An interactive prototype is developed using design tools to visualize and validate the user interface with stakeholders before moving into full-scale development.

3. Testing and Validation

   Testing is integrated into each step to ensure the quality of the application. After the development, stakeholders are invited to test the application (User Acceptance Tests - UAT) to confirm that it meets the theoretical solution's expectations.

4. Feedback and Iteration

   Feedback is collected continuously throughout the development process. Based on this feedback, features are refined, new requirements are incorporated, and identified issues are resolved.

5. Deployment and Maintenance

   Once the application is fully developed and tested, it will be deployed using AWS Amplify to ensure that the application is available for use by end-users. Post-deployment, regular updates and optimizations are scheduled to incorporate new features or resolve any discovered bugs.

6. Open Source Code

   The code used for the application will be freely accessible. This ensures the application's long-term sustainability and ease of further development.

3.2.2 Development Schedule

Below is the development schedule to be followed for the implementation of the technical solution with the expected time efforts for each step:

3.2.2.1 September: Planning, Design, and Initial Development

- Project Planning and Requirements Gathering (1 week, 5 working days)
- Define scope, goals, user personas, core functionality, and the maturity model. Create a detailed project specification and final feature list. Wireframing and UI/UX Design (1 week, 5 working days)

Use Diagrams.net to design the application's layout and user flow. Ensure the design is responsive and user-friendly. Get stakeholder feedback for iterative changes.

- Technical Setup and Environment Configuration Set up the React environment using Create React App or Vite. Configure dependencies such as Formik, React Router, and charting libraries. Establish a code repository (e.g., GitHub) with branch policies. Basic Component and Layout Development (1 week, 5 working days)
- Develop core reusable components (e.g., navbar, footer, form components, card). Create the base structure (e.g., main page layout, common styles).

3.2.2.2 October: Core Development and Feature Implementation

- Questionnaire Component Development (2 weeks, 10 working days)

  Develop components for each questionnaire section (e.g., Identity Management, Network Security). Implement form handling using Formik or React Hook Form. Add conditional logic for navigating through the questionnaire sections.

- Maturity Score Calculation Logic (1 week, 5 working days)

  Implement logic to collect user answers, calculate scores, and determine maturity level. Test and validate the scoring logic to ensure it aligns with the maturity model.

- Dynamic Feedback and Explanation Implementation (1 week, 5 working days)

  Build components to display customized feedback based on scores. Use React conditional rendering to tailor the feedback.

- Action Plan and Recommendations Feature (1 week, 5 working days)

  Create an action plan feature that dynamically generates suggestions based on the maturity assessment. Provide links and resources for open-source tools for improvement.

3.2.2.3 November: Testing, Improvements, and Deployment

- Integration of UI Enhancements and Styling (1 week, 5 working days)

  Polish the UI based on design feedback. Add animations and interactions to improve user experience.

- Testing and Quality Assurance (1 week, 5 working days)

  Component Testing: Use Jest and React Testing Library for unit testing. User Testing: Gather feedback from potential users to improve usability. Browser Testing: Ensure the app works across multiple browsers and devices.

- User Feedback and Refinement (1 week, 5 working days)

  Address issues found during testing. Refine features based on user feedback.

- Deployment Preparation and Deployment (3 days)

  Prepare the build and test in a staging environment.

- Buffer Time and Final Documentation (Remaining 1 week)

  Allocate extra time for any delays or unforeseen changes. Document the app's functionality, user manual, and future recommendations.

3.2.3 Development Tools

The main code of the application is written in Typescript using the React library and the Material UI (MUI) resources. All the files related to it are stored in a GitHub repository that also provides the versioning of the project. In order to make the application accessible for the Internet, this project uses the AWS hosting services for the developed application. The AWS Amplify is connected to the GitHub repository and is able to build the application as the code is updated. To generate some of the tables and provide information for the web pages, the application uses a couple of CSV files that are stored in the AWS S3 buckets which is accessible through the requests made by the application.

4 Requirements Specification

The requirements of this project concern the technical implementation of the solution, focusing on the related aspects of software development, user experience and interface (UI/UX), data storage and application hosting and access. Below are the use cases of the web application regarding the user:

Table 4 – Web application use cases

Use case name	**Description**	**Preconditions**	**Trigger**
Access home page	Access the home page and read the presentation texts.	The website must be online, and the home page loads automatically.	User opens the website.
Check references page	Check the references by clicking the button at the top of the screen.	The user must be on the home page.	User clicks the "References" button.
Check about page	Access the about page by clicking the corresponding button, reading project motivations.	The user must be on the home page.	User clicks the "About" button.
Access the questionnaire	Navigate to the questionnaire page, read questions, and complete all 6 steps.	The user must be on the home page.	User clicks the "Questionnaire" button at the bottom of the home page.
Download results	See and read the results of the questionnaire and download a PDF file with them.	The user must have completed the questionnaire.	User clicks the "Download Results" button after completing the questionnaire.

Source: Author.

Based on the structure of the project, here are its functional and non functional requirements:

4.1 Functional Requirements

- **Home Page Access and Display**

The application must allow users to access the home page and display introductory texts when the website loads.

- **Navigation to References Page**

  The application must provide a button that redirects the user to the references page, where all references used in the project are displayed.

- **Navigation to About Page**

  The application must provide a button that redirects the user to the "About" page, which contains an introduction to the project, including its objectives and motivations.

- **Access and Completion of Questionnaire**

  The application must provide a button that navigates the user to a 6-step questionnaire. Users must be able to select answers for all questions in each step of the questionnaire.

- **Viewing and Downloading Questionnaire Results**

  After completing the questionnaire, the application must display the results to the user. Users must have the option to download the results as a PDF file.

- **File Storage**

  The application must store the CSV files of the questionnaire in AWS S3 for future access.

4.2 Non Functional Requirements

- **Performance**

  The application should load the home page within 2-3 seconds under normal network conditions.

- **Scalability**

  The application should be able to handle an increasing number of users accessing the website simultaneously, leveraging AWS Amplify's scalable infrastructure.

- **Security**

  The application must securely store and manage files in AWS S3, ensuring that they're only available for the request coming from authorized sources. The application must avoid the Cross-Origin Resource Sharing (CORS) vulnerability.

- **Availability**

  The application must be highly available, with minimal downtime, leveraging AWS Amplify for continuous uptime and deployment reliability.

- **Usability**

  The interface must be intuitive, leveraging Material UI for a consistent and user-friendly design across all pages. The application should be responsive, providing a seamless experience on both desktop and mobile devices.

- **Maintainability**

  The codebase should be maintainable, with clear version control using GitHub, allowing for smooth updates and bug fixes. TypeScript should be used to minimize errors and enhance code maintainability.

5 Development of the Work

5.1 A Guide for SMEs

Digitalization brings incredible opportunities for start-ups and SMEs, reducing investment costs, optimizing processes and bringing them closer to their customers, partners and public services. However, along with these benefits come real risks, as cyberattacks continue to increase dramatically and exposure to these attacks only grows with the modernization of services. As mentioned earlier, data leaks, ransomware, reputational damage, and sabotage pose significant threats to organizations, with potentially serious and irreversible social and economic consequences. Despite the abstract and technical nature of cybersecurity, especially for smaller companies, a lack of adequate preparation can result in operational disruptions, forcing a return to manual processes in the event of an attack. This is usually because of limited human capital and financial resources to quantify cyber risks and allocate appropriate investments to cybersecurity.

Fortunately, viewing cybersecurity as an opportunity, rather than just a challenge, can lead to positive results. By prioritizing protection measures, companies not only ensure their longevity, but also strengthen stakeholder confidence. Cybersecurity has emerged as an essential collective effort, crucial for sustainable economic development, being sustained by people and entities around the world, especially on the principles of open data. Small companies and technology startups are suppliers and vendors to governments and large organizations, they could possibly have a network connection back to the latter and might store their confidential information to some extent. In view of this, without the appropriate cybersecurity measures, SMEs may be an attack vector for malicious hackers to gain entry to the large organizations.

As identified in the literature review, the relevance of cybersecurity is well addressed and seems to be exponentially growing. To tackle information security issues, multiple solutions regarding cybersecurity frameworks with different approaches and objectives are proposed worldwide. The abundance of - sometimes conflicting - information, the lack of cybersecurity knowledge to put in place the solution and the absence of adapted solutions to some scenarios such as the one of technology start-ups are some of the main problems and gaps that are observed nowadays. Although there is no one-size-fits-all solution, the implementation of simple but essential practices can significantly reduce risks, limit damage and facilitate business continuity after an incident.

In view of this, this works aims at adapting the current solutions to the context of SMEs, adding new steps based on the identified gaps and using the existing open source knowledge and techniques to provide a kickstart for an organization that wants to improve their cybersecurity maturity. The idea is to propose a tool adapted to the different stages of an organization, be it a technology start-up or a company that is developing its IT infrastructure. Based on the following tables, we can identify the current or the target cybersecurity maturity that an organization should have based on its development stages.

To assess the current level, we're going to use an adapted version of the NIST Cybersecurity Framework 2.0 to gather information about the organization. Using the collected data, we will identify the current maturity level according to the references above and provide guidelines regarding the next steps and some quick wins that will help the company increasing its cybersecurity maturity. These next steps will consist of propositions divided into the 6 defined groups followed by some open source tools already available. Below, this project describes the different development levels of SMEs, their respective cybersecurity focuses and what is expected to be already in place in terms of cybersecurity practices for each of the NIST functions:

- **Early Stages**: Establishing Basic Security Hygiene.

Table 5 – Early Stages expected security practices

CSF Function	**Expected Cybersecurity Practices**
Govern	Create basic security policies and procedures. Conduct an initial risk assessment to identify major risks. Understand the organization's most critical assets.
Idenfity	Maintain inventory of critical hardware, software, and data assets. Assign ownership for key assets. Implement strong password policies.
Protect	Conduct basic security training for employees. Use firewall configurations and VPNs. Regular software patching.
Detect	Set up logging for key assets. Identify normal network activity.
Respond	Develop a basic incident response procedure. Identify stakeholders.
Recover	Implement regular data backups. Identify essential business processes.

Source: Author.

- **Organization Establishment**: Scaling Security Measures and Formalizing Processes.
- **Organization Growth**: Advanced Security and Full Compliance.

Table 6 – Organization Establishment expected security practices

CSF Function	**Expected Cybersecurity Practices**
Govern	Formalize risk management processes. Conduct regular risk assessments and update policies. Align governance with initial business objectives.
Idenfity	Formalize security policies and procedures. Conduct initial risk assessments. Classify assets based on criticality.
Protect	Implement IAM tools. Perform regular vulnerability assessments. Adopt secure coding practices.
Detect	Set up SIEM capabilities. Adopt IDS/IPS tools. Define monitoring responsibilities.
Respond	Develop an incident response plan and test it. Introduce network segmentation.
Recover	Formalize disaster recovery procedures (DRP). Create redundancy for critical data and services.

Source: Author.

Table 7 – Organization Growth expected security practices

CSF Function	**Expected Cybersecurity Practices**
Govern	Align security strategy with business objectives. Prepare for external audits and certifications. Enhance risk management processes with continuous assessment.
Idenfity	Use MFA for key accounts. Regularly review access permissions. Implement identity and data ownership processes.
Protect	Monitor for privilege escalation. Conduct code reviews and static analysis. Manage network logs.
Detect	Implement machine learning for threat detection. Formalize Business Impact Analysis.
Respond	Formalize Business Continuity and Incident Response Plans (IRP). Use dedicated response teams.
Recover	Diversify backup locations geographically. Continuously improve response procedures.

Source: Author.

- **Organization Expansion and Maturity**: Robust Security Framework and Proactive Measures.

Table 8 – Organization Expansion and Maturity expected security practices

CSF Function	Expected Cybersecurity Practices
Govern	Continuously update security governance to match global operations. Conduct comprehensive risk assessments. Ensure policies and governance are aligned with evolving threats.
Idenfity	Align security strategy with business objectives. Continuously update governance to match global operations. Conduct comprehensive risk assessments.
Protect	Implement zero-trust architecture. Integrate advanced identity governance tools.
Detect	Use advanced threat hunting techniques. Continuous 24/7 monitoring with automated tools.
Respond	Enhance incident response with threat intelligence. Collaborate with external teams for incident management.
Recover	Perform regular exercises for disaster recovery. Implement data loss prevention (DLP) solutions.

Source: Author.

5.1.1 Cybersecurity Assessment

For each of the functions, we can identify categories to be evaluated that cover the main cybersecurity scenarios that are present on organizations. The maturity level will be assessed on a scale of 0 to 10, with 0 being the absence of implemented practices or processes and 10 being a complete understanding and implementation of security requirements. Based on the average score obtained in each of the categories, we can estimate the SME development level and understand the main existing gaps following the table below:

Table 9 – SME development levels based on calculated score.

SME development level	Calculated score (x)
Early Stages	$x < 4$
Organization Establishment	$4 \leq x < 7$
Organization Growth	$7 \leq x < 9$
Organization Expansion and Maturity	$x \geq 9$

Source: Author.

5.1.1.1 Govern

This function determines how the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

- **How well do I understand the organizational mission, objectives and main internal and external stakeholders?**

  Know your organization's goals and key people who impact its success, both inside (employees, managers) and outside (customers, partners). Example: If your mission is to provide eco-friendly products, your stakeholders include environmental groups and your R&D team.

  - Rating 0: No understanding of organizational goals or key stakeholders.
  - Rating 5: Some understanding of organizational goals and stakeholders, but gaps in clarity or depth.
  - Rating 10: Complete understanding of organizational goals, internal and external stakeholders, and how they contribute to success.

- **Are legal, regulatory and contractual requirements regarding cybersecurity understood and managed?**

  Ensure you're aware of and following laws, regulations, and contracts regarding data security. Example: If you handle credit card data, you must comply with PCI DSS to securely process and store payment information.

  - Rating 0: No awareness or management of legal, regulatory, or contractual requirements.
  - Rating 5: Basic awareness and partial compliance with some requirements, but gaps remain.
  - Rating 10: Full understanding and management of all legal, regulatory, and contractual requirements, with continuous updates to reflect changes.

- **How mature are the cybersecurity risk management processes?**

  Assess how well-developed your processes are for identifying and managing cybersecurity risks. Example: A mature process means you not only spot risks but have protocols in place to mitigate them quickly.

  - Rating 0: No process for managing cybersecurity risks.
  - Rating 5: Basic risk management process in place, but not fully matured or consistently applied.
  - Rating 10: Well-developed, mature risk management processes that identify, assess, and mitigate risks effectively.

- **Are risk appetite and risk tolerance statements established, communicated, and maintained?**

Define and communicate how much risk your organization is willing to accept to meet its objectives. Example: A retail company might be comfortable accepting the risk of minor website downtimes but not data breaches.

- Rating 0: No formal risk appetite or tolerance statements.
- Rating 5: Some statements are in place, but they are not fully communicated or maintained.
- Rating 10: Clear, well-communicated, and maintained risk appetite and tolerance statements that guide decision-making.

- **Is the strategic direction that describes appropriate risk response options established and communicated?**

  Set clear plans for how to handle different risks, such as avoiding, mitigating, transferring, or accepting them. Example: A company might decide to buy insurance (transfer) against cyberattacks to cover potential financial loss.

  - Rating 0: No strategic direction or risk response plan in place.
  - Rating 5: Some risk response options are identified, but not formalized or communicated.
  - Rating 10: A well-communicated and strategic direction is established, covering all appropriate risk response options (avoid, mitigate, transfer, accept).

- **Do you have a standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks?**

  Use a consistent method for measuring, documenting, and ranking risks to ensure everyone has the same understanding. Example: Using a risk matrix to rank cybersecurity risks helps prioritize fixing a critical vulnerability over less urgent issues.

  - Rating 0: No standardized method for calculating or prioritizing risks.
  - Rating 5: Some risk assessments are performed, but they lack consistency or prioritization.
  - Rating 10: A consistent, standardized method is in place for calculating, documenting, and prioritizing risks across the organization.

- **Do you have a RACI matrix to identify the main stakeholders and their responsibilities?**

  Create a chart to identify who is Responsible, Accountable, Consulted, and Informed for each cybersecurity activity. Example: In managing data backups, IT is Responsible, the IT manager is Accountable, auditors are Consulted, and executives are Informed.

  - Rating 0: No RACI matrix or formal method to identify responsibilities.
  - Rating 5: A basic RACI matrix is in place, but it is incomplete or not updated.
  - Rating 10: A comprehensive RACI matrix is fully implemented and regularly updated to clarify responsibilities across the organization.

- **Do you include cybersecurity guidelines in human resources practices?**

  Integrate cybersecurity into employee management processes like hiring, onboarding, and training. Example: Conduct background checks on employees who handle sensitive data, and train them on cybersecurity protocols.

  - Rating 0: No cybersecurity guidelines are integrated into HR practices.
  - Rating 5: Some cybersecurity practices are included, but they are incomplete or inconsistently applied.
  - Rating 10: Cybersecurity guidelines are fully integrated into HR processes, including hiring, onboarding, and training, with ongoing enforcement.

- **Are policies for managing cybersecurity risks reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission?**

  Regularly update cybersecurity policies to reflect changes in laws, threats, technology, or business goals. Example: After a new data privacy law is introduced, update your policy to reflect the new requirements.

  - Rating 0: Cybersecurity policies are not updated to reflect changes in threats, laws, or technology.
  - Rating 5: Some updates are made, but policies are not consistently reviewed or communicated.
  - Rating 10: Policies are regularly reviewed, updated, and enforced to reflect changes in legal, regulatory, and organizational needs.

- **Is the cybersecurity risk management strategy reviewed and ajusted according to the organizations' needs and risks?**

  Periodically assess and adapt your risk strategy to ensure it aligns with current needs and threats. Example: A company may adjust its risk strategy to include stronger cloud security if it moves more data to the cloud.

  - Rating 0: No regular review or adjustment of the cybersecurity risk management strategy.

  - Rating 5: Risk management strategy is reviewed occasionally, but changes are not always made to reflect current needs.
  - Rating 10: The cybersecurity risk management strategy is regularly reviewed and updated to reflect changing threats, technology, and organizational goals.

- **Are cybersecurity roles and responsibilities for third-party actors established, communicated, and coordinated internally and externally?**

  Define and communicate cybersecurity roles for external partners to ensure they align with your internal teams. Example: Clarify that a cloud service provider is responsible for infrastructure security, while your team manages data encryption.

  - Rating 0: No defined roles or responsibilities for third-party actors in cybersecurity.
  - Rating 5: Some roles are defined, but communication and coordination with third parties are inconsistent.
  - Rating 10: Clear roles and responsibilities are defined, communicated, and coordinated with third parties to ensure alignment with internal security measures.

- **Are the third party risks evaluated?**

  Assess the cybersecurity risks posed by partners or suppliers before working with them. Example: Evaluate whether a vendor has adequate cybersecurity measures in place before allowing them access to your systems.

  - Rating 0: No assessment of third-party cybersecurity risks.
  - Rating 5: Some third-party risks are evaluated, but the process is incomplete or informal.
  - Rating 10: Thorough evaluation of third-party risks before engagement, with continuous monitoring of third-party security measures.

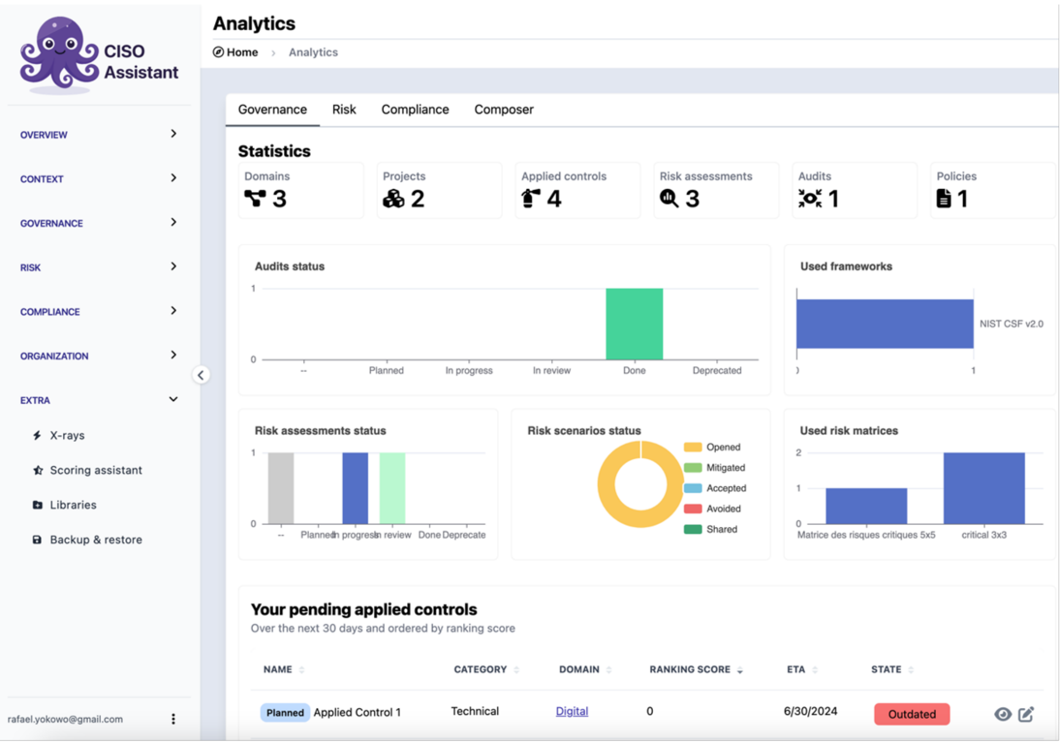
- **How integrated are the third-party risks within the organization's risk management?**

  Include risks from third parties in your organization's overall risk assessment process. Example: Consider a supplier's risk of data breaches alongside internal risks during risk reviews, to manage them comprehensively.

  - Rating 0: Third-party risks are not included in the organization's overall risk assessment.
  - Rating 5: Some third-party risks are considered, but not consistently integrated into overall risk management.

– Rating 10: Third-party risks are fully integrated into the organization's risk management processes, with regular reviews and assessments.

In terms of GRC (Governance, Risk and Compliance) management, one of the main and most useful open source tools to adopt is CISO Assistant. It is one-stop-shop approach provides a pragmatic way to handle the complexity of GRC (Governance, Risk and Compliance) that allows scaling, helps with risk assessments and security audits, streamlines IT efforts, unifies practices and controls.



Statistics

Domains	Projects	Applied controls	Risk assessments	Audits	Policies
3	2	4	3	1	1

Your pending applied controls

Over the next 30 days and ordered by ranking score

NAME	CATEGORY	DOMAIN	RANKING SCORE	ETA	STATE
Planned Applied Control 1	Technical	Digital	0	6/30/2024	Outdated

Figure 1 – CISO Assistant analytics dashboard.
Source: Author.

With CISO Assistant, you can structure an organization by defining users, user groups, projects and areas of activity. As for risk management, you can identify all the assets and their respective business values, what vulnerabilities exist and what controls can be put in place to mitigate them. For each risk assessment, we can define scenarios and carry out risk acceptances in which someone in the organization takes on the risk for some benefit. In addition to risk management, it is possible to establish policies and guidelines as to how information security is managed. The tool provides some existing frameworks and standards, such as NIST's, but you can also add your own policies if necessary.

5.1.1.2 Identify

The organization's current cybersecurity risks are understood through the knowledge of the organization's assets. This function also includes the identification of improvement opportunities for the organization's policies and practices that support cybersecurity risk management. Below are the assessment questions with the respective ratings references to evaluate the **identify** maturity:

- **Is there any inventory of assets (softwares, hardwares, services, etc)?**

  Keep an up-to-date list of all the organization's systems, hardware, software, and services to know what you have. Example: Create, if you don't have any, and automatically update a list of all devices on the network when new ones connect, like when a new laptop is used by an employee.

  - Rating 0: No inventory of assets is maintained.
  - Rating 5: A basic inventory is maintained but may not be up-to-date or cover all assets.
  - Rating 10: A complete, regularly updated inventory is maintained, and all new devices are automatically added when they connect to the network.

- **Are the assets classified according to their criticality to the business?**

  Rank assets based on how important they are to business operations. Example: Critical systems, like servers for customer data, are prioritized for updates before less important systems, like printers.

  - Rating 0: No classification of assets by their importance to business operations.
  - Rating 5: Some assets are classified, but the process is inconsistent or incomplete.
  - Rating 10: All assets are classified based on their criticality to business operations, with clear prioritization for security updates and protection.

- **Are there asset lifecycle process in place?**

  Implement processes to manage assets from creation to disposal, ensuring they remain secure throughout. Example: Securely destroy data on old hard drives before they are recycled to prevent data breaches.

  - Rating 0: No formal asset lifecycle management processes.
  - Rating 5: Some aspects of the asset lifecycle (e.g., procurement) are managed, but the process is not comprehensive.
  - Rating 10: A complete asset lifecycle management process is in place, covering creation to disposal, ensuring security at every stage.

- **Are vulnerabilities in assets are identified, validated, and recorded?**

  Identify and document weaknesses in your systems to understand and address risks. Example: Use vulnerability scanning software to find unpatched security flaws in your IT systems.

  - Rating 0: No process for identifying or documenting vulnerabilities in assets.
  - Rating 5: Vulnerabilities are identified in some assets, but documentation and validation are incomplete or irregular.
  - Rating 10: All vulnerabilities in assets are identified, validated, and properly recorded, using tools like vulnerability scanning software.

- **Do you review internal and external threats according to cyber threat intelligence?**

  Use information about cyber threats to understand what risks your organization might face. Example: Use cyber intelligence reports to learn about common attack methods and check if your systems are vulnerable.

  - Rating 0: No review of threats based on cyber threat intelligence.
  - Rating 5: Some internal and external threats are reviewed, but without regularity or full use of intelligence reports.
  - Rating 10: Cyber threat intelligence is fully integrated, and regular reviews of both internal and external threats are conducted to assess risks.

- **Are threats and vulnerabilities used to understand inherent risk?**

  Evaluate risks by considering both potential vulnerabilities and known threats to your organization. Example: Assess the impact of a vulnerability on a web server given that cybercriminals are actively exploiting it worldwide.

  - Rating 0: No assessment of inherent risks based on threats or vulnerabilities.
  - Rating 5: Some inherent risks are assessed, but vulnerabilities and threats are not always fully considered.
  - Rating 10: A thorough evaluation of inherent risks, based on all known vulnerabilities and threats, is consistently performed and documented.

- **Are risk responses chosen, prioritized, planned, tracked, and communicated?**

  Decide how to handle risks (e.g., accept, avoid, mitigate) and track your progress. Example: Mitigate a risk by applying a security patch, then document the progress until completed.

  - Rating 0: No formal process for selecting or prioritizing risk responses.
  - Rating 5: Some risk responses are chosen and tracked, but the process lacks prioritization and thorough documentation.
  - Rating 10: Risk responses are systematically chosen, prioritized, and tracked, ensuring timely and effective mitigation.

- **Are changes and exceptions managed, assessed for risk impact?**

  Evaluate the impact of changes and exceptions to policies to ensure they do not increase risks. Example: Document the risks involved when bypassing a security control temporarily and have a rollback plan ready.

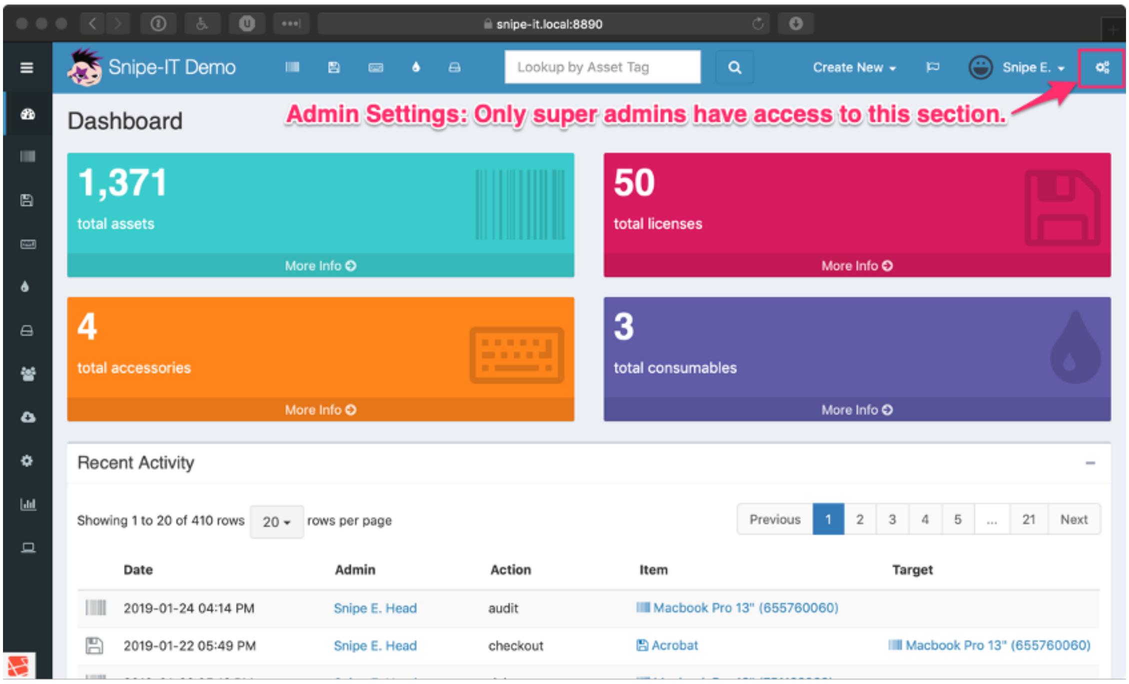
  - Rating 0: No management of changes or exceptions for risk impact
  - Rating 5: Some changes and exceptions are evaluated, but the process is inconsistent or lacks detailed assessment.
  - Rating 10: All changes and exceptions are evaluated for risk impact, with proper documentation and rollback plans in place.

- **Are Incident Response plans established, communicated, maintained, and improved?**

  Develop and update response plans for dealing with cybersecurity incidents to minimize damage. Example: After a simulated cyberattack, update your incident response plan based on lessons learned during the exercise.

  - Rating 0: No formal incident response plan exists.
  - Rating 5: An incident response plan exists but is not regularly updated or communicated.
  - Rating 10: A comprehensive incident response plan is in place, regularly maintained, communicated, and improved based on lessons learned during simulations or real incidents.

One of the biggest challenges for organizations, especially smaller ones, is to keep track of all the company's IT assets, whether they are hardware, software or other physical objects. The initial intuition is to use excel tables to store data and information, but this type of management soon proves inefficient when the number of assets grows significantly. For this purpose, the tool proposed - regarding the Identity function - for IT asset management is **Snipe-IT**. It is a free open source software that makes the way companies track, monitor and optimize their assets more efficient. With an intuitive interface and robust features, it offers a complete view of the asset lifecycle, from acquisition to retirement.



Admin Settings: Only super admins have access to this section.

Dashboard

1,371 total assets

50 total licenses

4 total accessories

3 total consumables

Recent Activity

Showing 1 to 20 of 410 rows 20 rows per page

Date	Admin	Action	Item	Target
2019-01-24 04:14 PM	Snipe E. Head	audit	Macbook Pro 13" (655760060)	
2019-01-22 05:49 PM	Snipe E. Head	checkout	Acrobat	Macbook Pro 13" (655760060)

Figure 2 – Snipe-IT dashboard.
Source: Snipe-IT Documentation.

This tool allows us to develop custom automations based on your own individual needs through a customizable API. It implements best-practices security for application design to prevent common attacks with two-factor authentications, HTTPS-only communications and brute-force prevention mechanisms. In the same way that CISO Assistant works, the basic version, with access to the codes and functionalities, is free. If the organization wishes to have support, a dedicated hosting service for the solution, among other features and benefits, there is a paid option that carries out the entire implementation, reducing the need for technical skills.

5.1.1.3 Protect

Once assets and risks are identified and prioritized, this function supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Below are the assessment questions with the respective ratings references to evaluate the **protect** maturity:

- **Are the identities and credentials for authorized users, services, and hardware managed by the organization?**

  Keep track of authorized users and devices, making sure only approved people and hardware can access systems. Example: Issue and revoke cryptographic keys when an employee joins or leaves the organization.

  - Rating 0: No system for managing user, service, or hardware identities and credentials exists.
  - Rating 5: Some users and devices are tracked, but there are inconsistencies, and manual updates are frequent.
  - Rating 10: Identities and credentials are managed and reviewed periodically

- **Are users, services, and hardware authenticated and protected?**

  Make sure users and devices are verified before accessing systems, using methods like multifactor authentication (MFA). Example: Require MFA for all employees to access critical systems, ensuring they use both a password and a code from an authenticator app.

  - Rating 0: Users and devices are not authenticated before accessing systems.
  - Rating 5: Basic authentication exists, but not consistently applied across all users and devices.
  - Rating 10: All users, services and hardware are authenticated and protected following the best practices

- **Do you incorporate the principles of least privilege and segregation of duties (SoD)?**

  Limit access to only what's necessary and separate roles to prevent conflicts of interest. Example: Only grant accounting software access to finance staff, not to employees in unrelated departments.

  - Rating 0: No consideration for least privilege or SoD in access control.
  - Rating 5: Some roles are restricted, but there are gaps in enforcing least privilege or segregating duties effectively.
  - Rating 10: Access is controlled based on the principle of least privilege, and duties are fully segregated to prevent conflicts of interest.

- **How do you manage physical access to the on-premises resources?**

  Control who can physically enter sensitive areas in your organization. Example: Use security guards and badge-controlled doors to limit access to server rooms.

  - Rating 0: No control over physical access.
  - Rating 5: Some physical access controls are in place, but they are not enforced consistently.
  - Rating 10: Strong physical security measures, including badge-controlled doors, guards, and other mechanisms, are enforced for all internal areas.

- **Are the personnel provided with awareness and training regarding cybersecurity risks?**

  Educate all employees on basic cybersecurity, including recognizing and responding to threats. Example: Train staff to identify phishing emails and report them.

  - Rating 0: No cybersecurity awareness or training provided to employees.
  - Rating 5: Basic training is provided, but it's infrequent or no follow-up is in place.
  - Rating 10: Comprehensive, regular cybersecurity awareness training is provided, covering recognition of threats such as phishing.

- **Are the personnel with privileged accesses or in high stakes roles provided with advanced and specialized awareness and training regarding the cybersecurity risks?**

  Provide specialized cybersecurity training for staff in critical positions or with sensitive access. Example: Train IT administrators on advanced security topics like threat hunting and vulnerability management.

  - Rating 0: No specialized cybersecurity training for personnel with privileged access.
  - Rating 5: Some specialized training is provided, but it's irregular or incomplete.
  - Rating 10: Personnel with privileged access receive advanced, role-specific training regularly, covering areas such as threat hunting and vulnerability management.

- **Is the CIA triad guaranteed for data in all its possible states (at-rest, in-transit and in-use)?**

  Protect data when it's stored, in transit, or being used. Example: Encrypt data stored on company servers to maintain confidentiality.

  - Rating 0: No controls in place to protect the confidentiality, integrity, or availability of data.
  - Rating 5: Some data is protected, but there are gaps in ensuring the CIA triad for data in all states.
  - Rating 10: The CIA triad is fully guaranteed for all data, including encryption of data at-rest, in-transit, and in-use.

- **Are backups of data are created, protected, maintained, and tested?**

  Create, secure, and regularly test data backups to ensure data is available in case of loss. Example: Keep encrypted backups of critical data offline to prevent loss during a ransomware attack.

  - Rating 0: No backups are created or maintained.
  - Rating 5: Backups are created, but testing or protection of backups is inconsistent.
  - Rating 10: Backups are regularly created, encrypted, securely stored, and routinely tested to ensure their integrity and reliability.

- **Is there an established process for configuration management?**

  Manage the setup and ongoing configuration of software and hardware to maintain security. Example: Regularly monitor software for deviations from secure baseline configurations.

  - Rating 0: No configuration management process in place.
  - Rating 5: Some configuration management occurs, but it's not standardized or monitored consistently.
  - Rating 10: A thorough configuration management process is in place, regularly monitoring and adjusting configurations to maintain security.

- **Do you replace hardware or software if it presents a risk to the organization?**

  Replace outdated or insecure components to maintain security. Example: Replace unsupported software versions that no longer receive security patches.

  - Rating 0: No procedure for replacing outdated or risky hardware/software.
  - Rating 5: Some hardware/software is replaced, but not consistently or proactively.
  - Rating 10: All hardware and software presenting a risk is identified, replaced, or upgraded in a timely manner to maintain security.

- **Are log records generated and made available for continuous monitoring?**

  Generate and keep logs to monitor systems for unusual or suspicious activity. Example: Set up servers to record logs and send them to a secure location for analysis.

  - Rating 0: No logs are generated or monitored for suspicious activity.
  - Rating 5: Logs are generated but not consistently reviewed or securely stored.
  - Rating 10: Logs are continuously generated, securely stored, and actively monitored for suspicious activities with alerts set up for anomalies.

- **Do you manage the installation and execution of unauthorized software?**

  Control which software can be installed to prevent unauthorized or harmful applications. Example: Allow only approved software to be installed on company devices.

  - Rating 0: No controls over the installation or execution of unauthorized software.
  - Rating 5: Some controls exist, but unauthorized software is occasionally installed or executed.
  - Rating 10: Strict control over software installations, allowing only approved and authorized software to be used within the organization.

- **Are Secure Software Development practices integrated in the software development lifecycle (SDLC)?**

  Integrate security measures throughout the software development lifecycle. Example: Run vulnerability scans on software before deploying it to production.

  - Rating 0: No security practices integrated into the SDLC.
  - Rating 5: Some security practices are integrated, but the process is incomplete or inconsistent.
  - Rating 10: Security is fully integrated into every stage of the SDLC, from planning to deployment, including vulnerability testing and code reviews.

- **Do you control the access and usage of the organization's networks and digital environments?**

  Restrict access to internal networks and ensure they are secure. Example: Use zero trust architecture to limit network access based on user needs.

  - Rating 0: No control over access to networks or digital environments.
  - Rating 5: Some access controls are in place, but they are not consistently enforced.
  - Rating 10: Access to networks and digital environments is fully controlled, with measures like zero trust architecture ensuring limited access based on user needs.

- **Are the organization's technology assets protected from environmental threats?**

  Safeguard equipment from natural threats like fire, floods, and power issues. Example: Store servers in rooms with fire suppression systems and temperature control.

  - Rating 0: No protection in place for technology assets against environmental threats.
  - Rating 5: Some protection is in place (e.g., fire alarms), but it is incomplete or insufficient.
  - Rating 10: All technology assets are fully protected from environmental threats, including fire suppression systems, temperature control, and flood protection.

- **Are there mechanisms in place to achieve the resilience requirements in normal and adverse situations?**

  Ensure systems can continue to operate during and after disruptions. Example: Use redundant power supplies to maintain service availability during power outages.

  - Rating 0: No mechanisms to ensure resilience during disruptions.
  - Rating 5: Some mechanisms are in place, but they may not fully cover normal and adverse situations.
  - Rating 10: Strong resilience mechanisms are in place, including redundant systems and backup power supplies, ensuring continuity during disruptions.

- **Is the organization capable of ensuring availability?**

  Monitor resource usage and scale capacity to ensure systems remain available. Example: Implement load balancing to distribute network traffic and avoid overloading servers.

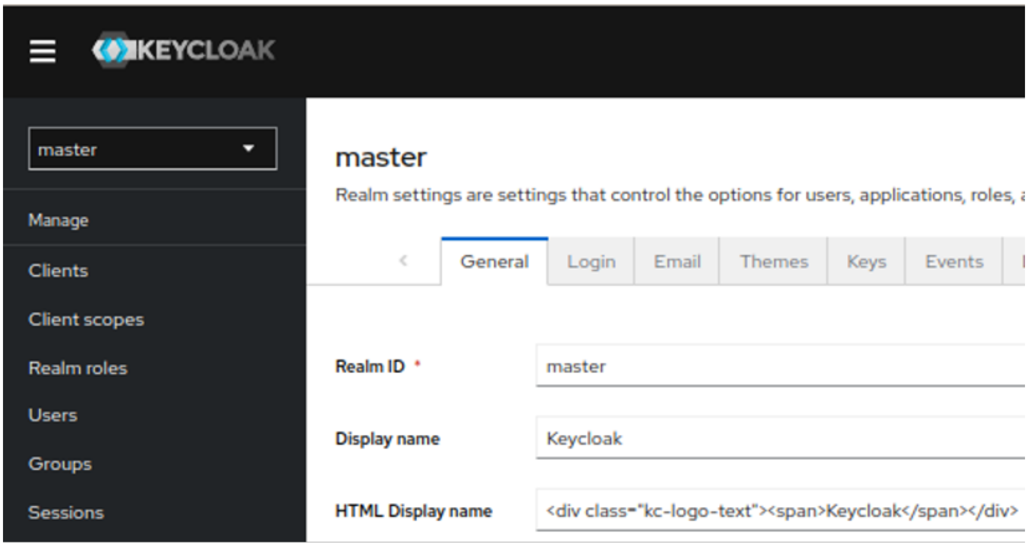
  - Rating 0: No systems in place to ensure availability.
  - Rating 5: Some systems are monitored for availability, but they may not scale to handle higher demands.
  - Rating 10: Comprehensive monitoring and scaling solutions are in place, such as load balancing and capacity planning, ensuring systems remain available at all times.

The Protect function covers multiple and different cybersecurity fronts: identity, data and platform security and technology infrastructure resilience. For each one of these fronts, a solution will be proposed:

- Identity and access management: Keycloak

  Keycloak is an open source tool created by RedHat which manages user credentials and permissions aimed at modern applications and services. It provides user federation, strong authentication, user management, fine-grained authorization among other functionalities.

  One of the main uses of Keycloak is the implementation of the Single-Sign On (SSO). With it, users authenticate with Keycloak itself and not with individual applications, so the applications don't have to deal with login forms, user authentication and user storage. Once logged in, users do not have to log in again to access a different application. This also applies to logging out. It provides a single logout, which means that users only have to log out once to exit all applications that use the



master

Realm settings are settings that control the options for users, applications, roles, a

Realm ID * master

Display name Keycloak

HTML Display name <div class="kc-logo-text"><span>Keycloak</span></div>

Figure 3 – Keycloak interface.
Source: Keycloak website.

tool. Keycloak can also be integrated with other types of logins such as with social networks and connections with LDAP and Active Directory servers.

- Data and Platform Security: **Veracrypt**, **OpenSSL** and **Synk Open Source**

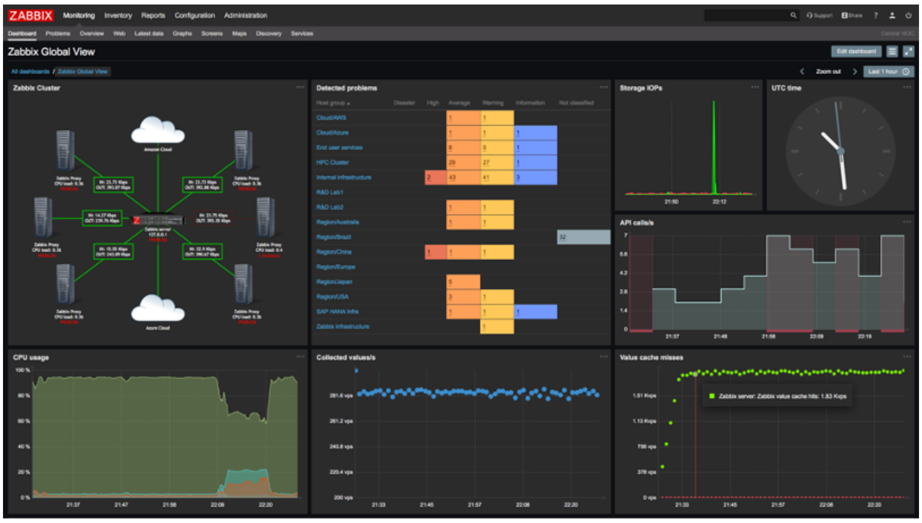
  VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. It offers advanced encryption features that can be applied to hard disk drives, partitions, USB sticks and other storage devices.

  OpenSSL is an open-source command line tool that is commonly used to generate private keys, install your SSL/TLS certificate, and identify certificate information. It is widely used by software developers and system administrators to implement secure communication and encryption in various applications, such as web servers, email servers, VPNs, and more.

  Snyk Open Source provides a developer-first SCA solution, helping developers find, prioritize, and fix security vulnerabilities and license issues in open source dependencies. It helps finding vulnerable dependencies while coding in the IDE or CLI to avoid future fixes, saving valuable development time.

- Technology Infrastructure Resilience: **Zabbix**

  Zabbix is an open source software tool to monitor IT infrastructure such as networks, servers, virtual machines, and cloud services. With it, it is possible to monitor the health and performance of Linux, Windows, MacOS and other servers, as well as a wide range of hardware devices. The tool collects the data on CPU, memory, disk and network usage to prevent bottlenecks and downtime.



Detected problems

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
Cloud/AWS			1	1		
Cloud/Azure			1	1	1	
End user services			8	5	1	
HPC Cluster			29	27	1	
Internal infrastructure		2	43	41	3	
R&D Lab1						
R&D Lab2			1	1		
Region/Australia			1	1		
Region/Brazil						32
Region/China		1	1	1		
Region/Europe						
Region/Japan			5			
Region/USA			3	1		
SAP HANA Infra			1	1	1	
Zabbix infrastructure				1		

Figure 4 – Zabbix interface.
Source: Zabbix website.

This tool can be deployed for agent-based and agentless monitoring. Agents are installed on IT components to check performance, collect data and report back to a centralized management server. This information is included in reports or presented visually in the graphical user interface (GUI). If there are any problems with what is being monitored, Zabbix will send a notification or alert to the user. Agentless monitoring performs the same type of monitoring using existing resources on a system or device to emulate an agent. Zabbix's web-based GUI allows users to visualize their IT environment through customizable widget-based dashboards, graphs, network maps, slideshows and reports. For example, a user can customize a report to show metrics associated with service level agreements and key performance indicators on CPU loads.

5.1.1.4 Detect

The practices related to this function enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. Below are the assessment questions with the respective ratings references to evaluate the **detect** maturity:

- **Are networks and network services monitored to find potentially adverse events?**

  Observe network activities to identify unusual events or behaviors that could indicate a problem. Example: Monitor wired and wireless networks for unauthorized devices connecting to your network.

  - Rating 0: No monitoring of physical access points or facilities is in place.

  - Rating 5: Basic network monitoring exists, but it's inconsistent and lacks proper analysis for adverse events.
  - Rating 10: Comprehensive network monitoring is in place, covering all network services and consistently identifying any suspicious or adverse events.

- **Is the physical environment monitored to find potentially adverse events?**

  Keep an eye on physical access points and facilities to detect any suspicious or unauthorized activity. Example: Use badge readers and security cameras to track who enters secure areas and ensure only authorized personnel have access.

  - Rating 0: No monitoring of physical access points or facilities is in place.
  - Rating 5: Some physical monitoring exists (e.g., door locks or guards), but it's not systematic or comprehensive.
  - Rating 10: Physical monitoring is thorough, including access logs, alarms, and regular reviews of access data.

- **Are personnel activity and technology usage monitored to find potentially adverse events?**

  Track employee and system usage to detect signs of misuse, insider threats, or other anomalies. Example: Use behavior analytics software to identify unusual login times that could suggest unauthorized access.

  - Rating 0: No monitoring of personnel activity or technology usage.
  - Rating 5: Some personnel activities are monitored, but without regular checks or analysis of suspicious behavior.
  - Rating 10: All personnel activity and technology usage are actively monitored using behavior analytics to detect and mitigate insider threats or other anomalies.

- **Are external service providers monitored to find potentially adverse events?**

  Track the activities of third-party service providers to make sure they follow expected procedures and don't introduce risks. Example: Monitor the maintenance activities of cloud service providers to ensure they don't deviate from approved protocols.

  - Rating 0: No monitoring of activities performed by external service providers.
  - Rating 5: Limited monitoring of critical service providers only, and it's not consistently applied.
  - Rating 10: All activities of external service providers are monitored systematically for deviations from expected behavior.

- **Are computing (hardware and software) assets monitored to find potentially adverse events?**

  Keep an eye on your systems to identify unexpected behaviors or modifications that could signal a problem. Example: Monitor software for changes from secure baseline configurations to catch any unauthorized updates.

  - Rating 0: No monitoring of hardware or software assets.
  - Rating 5: Basic monitoring is in place, but it is irregular and focuses only on critical assets.
  - Rating 10: Continuous monitoring of all computing assets for unauthorized changes or suspicious behavior, with quick detection and response.

- **Are the potentially adverse events analyzed and correlated with information from other sources?**

  Combine information from multiple monitoring sources to get a clearer picture of potential threats. Example: Use a Security Information and Event Management (SIEM) system to correlate logs from different systems to identify patterns of attack.

  - Rating 0: No analysis or correlation of adverse events with other information sources.
  - Rating 5: Adverse events are analyzed in isolation, with minimal correlation from other monitoring systems.
  - Rating 10: Adverse events are thoroughly analyzed and correlated with data from multiple sources, providing a full understanding of their nature and impact.

- **Do you estimate the impact and scope of the adverse events?**

  Evaluate how much damage a detected incident could cause and how widespread it could be. Example: Use a SIEM to estimate the scope of a breach and determine which systems and data might be affected.

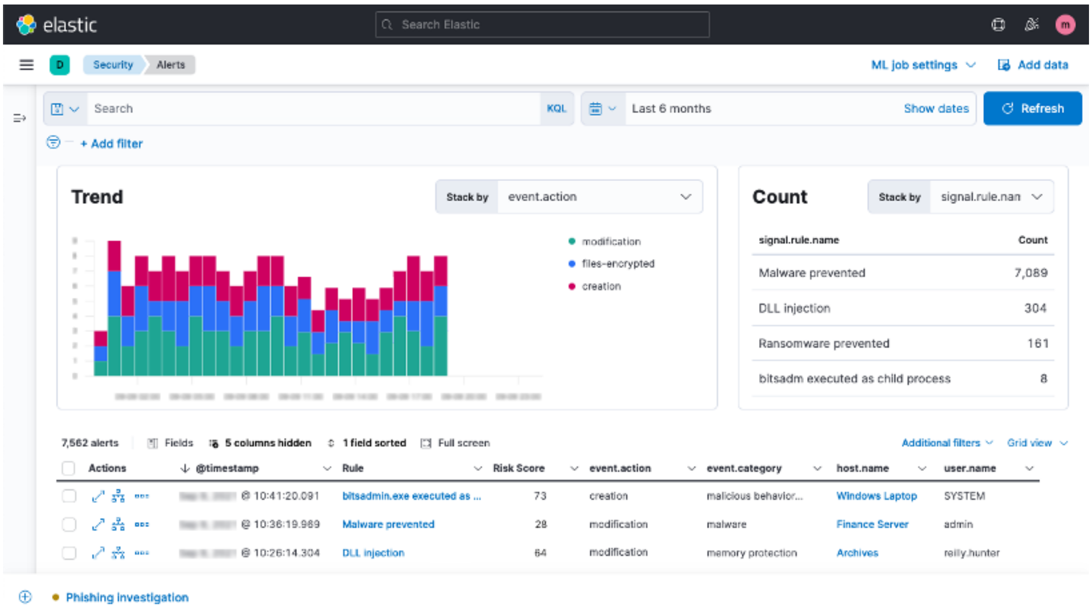
  - Rating 0: No estimation of impact or scope is performed.
  - Rating 5: The impact of adverse events is roughly estimated but without consistency or depth.
  - Rating 10: The impact and scope of all adverse events are carefully estimated and reviewed, providing actionable insights for incident management.

- **Do you have pre-established criteria for adverse events such that when incidents happen, they are declared following the protocol?**

  Define specific criteria for when an unusual event should be classified as a security incident requiring action. Example: Automatically trigger an incident response process when unauthorized software is detected on a critical server, following established protocols.

- Rating 0: No criteria are in place for declaring incidents.
- Rating 5: Some guidelines exist, but they are unclear, and incidents are inconsistently declared.
- Rating 10: Clear, well-established criteria are consistently applied for declaring incidents, ensuring timely and appropriate response.

For the detection and analysis of data involving an organization's networks and assets, a recommended type of tool is a SIEM (Security Information and Event Management). The free and open source Elastic SIEM is an application that provides security teams with visibility, threat hunting, automated detection, and Security Operations Center (SOC) workflows. It is included in the default distribution of the most successful logging platform, Elastic (ELK) Stack software and it ships with out-of-the-box detection rules aligned with known frameworks such as the MITRE ATT&CK™ one to surface threats often missed by other tools.



signal.rule.name	Count
Malware prevented	7,089
DLL injection	304
Ransomware prevented	161
bitsadm executed as child process	8

Actions	@timestamp	Rule	Risk Score	event.action	event.category	host.name	user.name
	[redacted] @ 10:41:20.091	bitsadmin.exe executed as ...	73	creation	malicious behavior...	Windows Laptop	SYSTEM
	[redacted] @ 10:36:19.989	Malware prevented	28	modification	malware	Finance Server	admin
	[redacted] @ 10:26:14.304	DLL injection	64	modification	memory protection	Archives	reilly.hunter

Figure 5 – Elastic interface.
Source: Elastic website.

Severity and risk scores associated with signals generated by the detection rules help analysts to triage issues and turn their attention to the highest-risk work. The tool is built with the speed and scalability of Elasticsearch as its underlying search platform, and according to the Elastic website, it maintains analyst velocity with:

- An overview page to show SOC status and security posture;
- Dashboards for threat hunting and situational awareness;
- Integration with Elastic Maps, Elastic Lens, and the rest of Kibana;
- A detection engine for automated detection;
- A unique timeline investigator with investigation templates for analysts.

5.1.1.5 Respond

Actions regarding a detected cybersecurity incident to be taken by the organization to contain the effects of the incidents. It concerns management, communication and coordination efforts of different teams inside an organization. Below are the assessment questions with the respective ratings references to evaluate the **respond** maturity:

- **Is there an incident response process in place (triage, validation, classification, prioritization, escalation and elevation)?**

  Have a structured approach to managing incidents, including identifying, classifying, and prioritizing them, and escalating as needed. Example: Designate an incident lead who oversees incident management, including determining if the incident is severe enough to escalate to higher authorities.

  - Rating 0: No structured incident response process is in place.
  - Rating 5: An informal incident response process exists, but not all stages are covered or consistently followed.
  - Rating 10: A complete incident response process, covering triage to escalation, is well-documented and followed for all incidents.

- **Do you coordinate the execution of the incident response plan with relevant third parties?**

  Collaborate with relevant external stakeholders (e.g., partners, vendors) to handle incidents effectively. Example: Coordinate with your cloud provider to help escalate and resolve an ongoing cybersecurity attack involving their services and your own assets and resources.

  - Rating 0: No coordination with external stakeholders during incidents.
  - Rating 5: Coordination is inconsistent and happens only when deemed absolutely necessary.
  - Rating 10: Incident response plans are routinely coordinated with all relevant third parties, ensuring smooth and prompt resolutions.

- **Are the incidents contained and eradicated?**

  Isolate and remove threats to stop them from causing further damage. Example: Use quarantine mechanisms to automatically move compromised devices to a secure network segment to prevent further spreading.

  - Rating 0: No actions are taken to contain or eradicate incidents.
  - Rating 5: Some containment actions are taken but often lack formal procedures or complete eradication.
  - Rating 10: Incidents are contained and eradicated systematically using both automated and manual methods, with minimal damage.

- **Are the internal and external stakeholders notified of incidents?**

  Inform relevant parties, such as customers, partners, or authorities, when an incident occurs. Example: Notify affected customers according to your organization's breach notification policies (e.g. e-mail, SMS, recorded phone call).

  - Rating 0: Stakeholders are not notified of incidents.
  - Rating 5: Only critical stakeholders are notified in high-risk incidents, and notifications lack timeliness.
  - Rating 10: All relevant stakeholders are notified promptly according to established protocols and requirements.

- **Do you have analysis procedures in place during incidents?**

  Analyze incidents to understand what happened, how, and why, and to prevent similar events in the future. Example: Attempt to determine if a vulnerability was exploited and which attackers may have been involved.

  - Rating 0: No procedures are in place to analyze incidents.
  - Rating 5: Analysis is conducted for some incidents, but procedures are not standardized or thorough.
  - Rating 10: A complete analysis is conducted for all incidents, focusing on understanding causes, vulnerabilities, and future prevention.

- **Are you capable of collecting data and meta data during incidents?**

  Gather data (e.g., system logs, activity details) during an incident for analysis and evidence purposes. Example: Collect and securely store all relevant data about the incident, including timestamps and system information.

  - Rating 0: No data or metadata is collected during incidents.
  - Rating 5: Some data is collected, but not consistently or securely.

  - Rating 10: All relevant data and metadata are collected, preserved, and safeguarded for evidence and analysis.

- **Are you capable of estimating and validating the magnitude of an incident?**

  Assess the extent of the damage caused by an incident to understand its impact. Example: Use a SIEM tool to estimate the scope of the incident, including the number of affected systems and data impacted.

  - Rating 0: No effort is made to estimate or validate the impact of an incident.
  - Rating 5: The magnitude is roughly estimated for only some incidents.
  - Rating 10: Impact and scope are precisely estimated and validated for all incidents using structured tools and procedures.

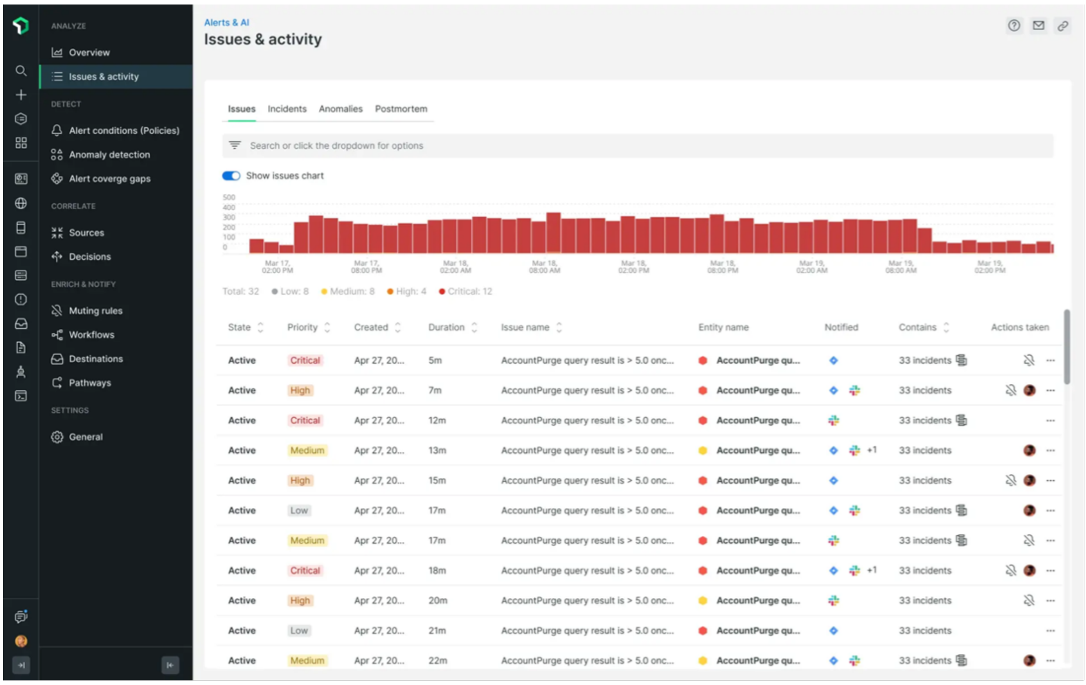
- **Can you record all actions performed during an investigation?**

  Keep detailed records of every action taken during an incident response to maintain accountability and ensure no step is overlooked. Example: Require incident responders to document all actions taken during an investigation and ensure that records are tamper-proof.

  - Rating 0: Actions during incidents are not recorded.
  - Rating 5: Some actions are recorded, but without formal procedures or accuracy.
  - Rating 10: Every action is meticulously documented and preserved in a tamper-proof format, ensuring accountability.

For this function, the most important factor is the internal actions and practices developed by the organization. It is essential to have documents that formalize incident response procedures, list all the people responsible and points of contact for taking action and define what information and tools to use and when. As incident data is essential for response actions, a solution that can generate and provide it on demand is crucial.

New Relic is an interesting tool to help with incident response management. It has an issues feed page where we find an overview of all issues, along with helpful information about them. Each issue has an option for more detail, including its analysis summary, event log, details about correlated issues and incidents. In addition, in the New Relic platform, there is a postmortem feature - a retrospective process that teams use to analyze what worked and what didn't when responding to and resolving an incident - that automatically collects data related to an incident, providing the responsible team an analysis and action items for improved responses to future incidents. With this tool, it is also possible to do a root cause analysis to find the potential causes for an issue and its impacted entities based on the deployments made and logs collected.



Issues & activity

State	Priority	Created	Duration	Issue name	Entity name	Notified	Contains	Actions taken
Active	Critical	Apr 27, 20...	5m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···
Active	High	Apr 27, 20...	7m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···
Active	Critical	Apr 27, 20...	12m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...		33 incidents	···
Active	Medium	Apr 27, 20...	13m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆ +1	33 incidents	···
Active	High	Apr 27, 20...	15m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···
Active	Low	Apr 27, 20...	17m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···
Active	Medium	Apr 27, 20...	17m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...		33 incidents	···
Active	Critical	Apr 27, 20...	18m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆ +1	33 incidents	···
Active	High	Apr 27, 20...	20m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...		33 incidents	···
Active	Low	Apr 27, 20...	21m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···
Active	Medium	Apr 27, 20...	22m	AccountPurge query result is > 5.0 onc...	● AccountPurge qu...	◆	33 incidents	···

Figure 6 – New Relic interface.
Source: New Relic website.

5.1.1.6 Recover

Assets and operations affected by a cybersecurity incident are restored. These actions support the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts. Below are the assessment questions with the respective ratings references to evaluate the **recover** maturity:

- **Do you have formalized recovery procedures in the incident response or disaster recovery plan?**

  Having clearly documented recovery procedures ensures that everyone knows exactly what actions to take during an incident or disaster, speeding up recovery and reducing confusion. Example: A disaster recovery plan includes detailed steps for restoring a critical application, ensuring the correct process is followed during a system outage.

  – Rating 0: No formal recovery procedures are documented.

  – Rating 5: Recovery procedures are partially documented but not updated or followed consistently.

  – Rating 10: Comprehensive recovery procedures are formally documented, regularly updated, and followed during every incident.

- **Do you have defined criteria regarding the recovery process (e.g. set of assets or services to be restored, minimal operational level, etc.)?**

Criteria define what needs to be recovered, which assets and services are priorities, and what the minimum operational levels should be to resume business effectively. Example: The plan specifies that critical financial services must be restored first, ensuring minimal impact on core business operations.

  - Rating 0: No criteria are defined for the recovery process.
  - Rating 5: Some criteria are defined, but they are incomplete or do not cover all critical assets and services.
  - Rating 10: Recovery criteria are clearly defined, including priority assets, services, and the minimum level of operations required to function effectively.

- **Are recovery actions selected, scoped, prioritized, and performed?**

  Actions during recovery should be chosen based on the current situation, properly scoped, prioritized, and carried out to minimize downtime and damage. Example: Restoring the payment system is prioritized first, as it has the most significant impact on business continuity.

  - Rating 0: No process for selecting or prioritizing recovery actions.
  - Rating 5: Some actions are selected and performed, but prioritization is inconsistent or ad-hoc.
  - Rating 10: All recovery actions are carefully chosen, scoped, and prioritized, ensuring effective and quick recovery in line with business needs.

- **Is the integrity of backups and other restoration assets before their restoration?**

  Ensuring the integrity of backups before restoration guarantees that corrupted or incomplete data doesn't get reintroduced, avoiding additional problems. Example: Conducting integrity checks on backup files before they are restored, ensuring data has not been tampered with or damaged.

  - Rating 0: No verification of backup integrity before restoration.
  - Rating 5: Backup integrity is checked inconsistently or only in some cases.
  - Rating 10: All backups undergo integrity checks before restoration to ensure they are complete and uncorrupted.

- **Are the recovery activities and progress in restoring operational capabilities communicated to internal and external stakeholders?**

  Keeping internal and external stakeholders informed during recovery is crucial to managing expectations and ensuring a coordinated response. Example: Regular updates are shared with customers about the progress of service restoration after a cyber incident, reducing uncertainty.

  - Rating 0: No communication is provided regarding recovery progress.
  - Rating 5: Some stakeholders are informed, but communication is inconsistent or lacks critical details.
  - Rating 10: All stakeholders are informed regularly about recovery activities and progress, with clear and structured communication.

- **Are the communications of the recovery shared through approved methods and messaging?**

  Using approved methods ensures that sensitive information shared during recovery is communicated securely and accurately, reducing the chance of misinformation or data leaks. Example: Communicating recovery details using secure messaging systems that are approved for sensitive internal communications.

  - Rating 0: No specific methods or guidelines for communication during recovery.
  - Rating 5: Communication happens, but there is no consistency or approved methods in place.
  - Rating 10: Recovery communications are consistently shared through approved, secure methods, ensuring accurate and reliable information.

In addition to the procedures and plans for disaster recovery, the use of tools that can help restore data and services is essential. LINBIT Disaster Recovery is a solution that enables asynchronous data replication from a primary site to a Disaster Recovery location, all using standard X86, ARM, or IBM Power servers. It can replicate data from the primary site to the public cloud, between campuses, or between public cloud instances to ensure protection during full site outages. The software is available for free on Github and the free open source version is the DRDB Proxy which helps creating a buffer area between the two locations, allowing your data to be transferred smoothly in case of disconnection and an off-site replica of your data is designed to protect your important information during critical site outages, natural disasters, and other unfortunate circumstances.

5.1.2 Estimated Costs

As mentioned above, the proposed open source solutions can be acquired and used free of charge, but there are certain drawbacks such as the limit on the number of functionalities and the need for technical knowledge for their implementation. In view of this, this section aims to present what the annual costs would be if an organization wished to adopt the proposed tools in order to facilitate processes and their management. The table below lists the proposed solutions and the respective prices for the basic versions of the services.

Table 10 – Annual costs for the proposed solutions.

Proposed solution	**Annual costs**
CISO Assistant (Pro SaaS)	$350
Snipe-IT (Basic Hosting)	$399
Synk Open Source (Team)	$300
Zabbix (Silver Tier Technical Support)	$3900
Elastic (Standard)	$1140
New Relic	$588
Linbit DR	License fee (not public)
TOTAL	$6675 + Linbit fee

Source: Author.

The gain in protection and cybersecurity maturity with the adoption of these tools is very significant. It can make organizations, especially SMEs, more robust in an accessible and practical way, potentially reducing risks and losses whether due to internal incidents, cyberattacks or other technical or administrative processes.

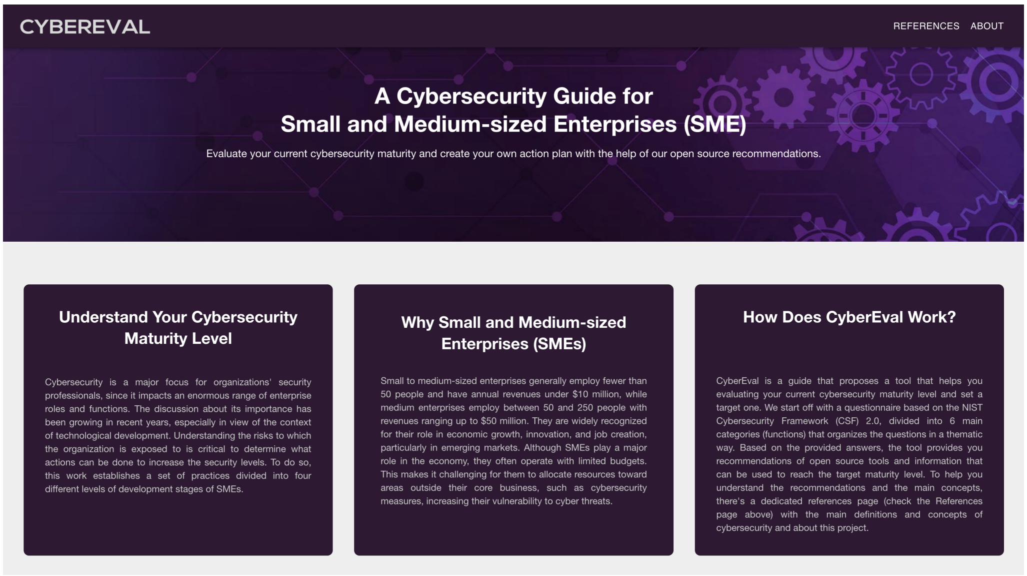
5.2 Application's Technical Overview

- User Interface (Frontend)
  - **Home Page**: Display introductory texts and provide navigation buttons.
  - **References Page**: Display the references used in the project.
  - **About Page**: Display information about the project's motivation and objectives.
  - **Questionnaire Page**: 6-step questionnaire, allowing users to answer questions and progress through steps.
  - **Results Page**: Display the user's results after completing the questionnaire and offer a PDF download button.
  - **React (TypeScript)**: For building reusable components.
  - **Material UI**: For the design and styling of the UI components, providing consistent, responsive layouts.
- Navigation Logic
  - **Buttons and Links:** To References, About, Questionnaire and Results (after questionnaire completion) Pages.
  - **React Router**: For managing navigation between pages within the single-page application.

- Data Handling
  - **Form Handling for Questionnaire**: Capturing user input and validating each step.
  - **Results Generation**: Dynamically generating results based on user input from the questionnaire.
  - **React State Management**: Using React's state or context API to manage user input and results across components.
- File Handling
  - **PDF Generation**: Creating a downloadable PDF based on the user's questionnaire results.
  - **AWS S3**: Storing generated PDFs for user access.
  - **AWS Amplify**: Facilitating connection to AWS services (e.g., S3) for file storage and management.
- Hosting & Deployment
  - **Continuous Integration / Continuous Deployment (CI/CD)**: Automatically updating the hosted application whenever changes are made to the codebase.
  - **AWS Amplify**: Hosting the frontend application and managing the CI/CD pipeline connected to the GitHub repository.
  - **GitHub**: Used for version control and managing the code repository.

5.3 Design and Implementation

The web application is implemented as a frontend-only app, only dealing with external resources to fetch the questionnaire's data and cybersecurity tools recommendations. Regarding its design, it is a straightforward application with a home page that introduces the tool and provides context to it.



A Cybersecurity Guide for
Small and Medium-sized Enterprises (SME)

Evaluate your current cybersecurity maturity and create your own action plan with the help of our open source recommendations.

Understand Your Cybersecurity Maturity Level

Cybersecurity is a major focus for organizations' security professionals, since it impacts an enormous range of enterprise roles and functions. The discussion about its importance has been growing in recent years, especially in view of the context of technological development. Understanding the risks to which the organization is exposed to is critical to determine what actions can be done to increase the security levels. To do so, this work establishes a set of practices divided into four different levels of development stages of SMEs.

Why Small and Medium-sized Enterprises (SMEs)

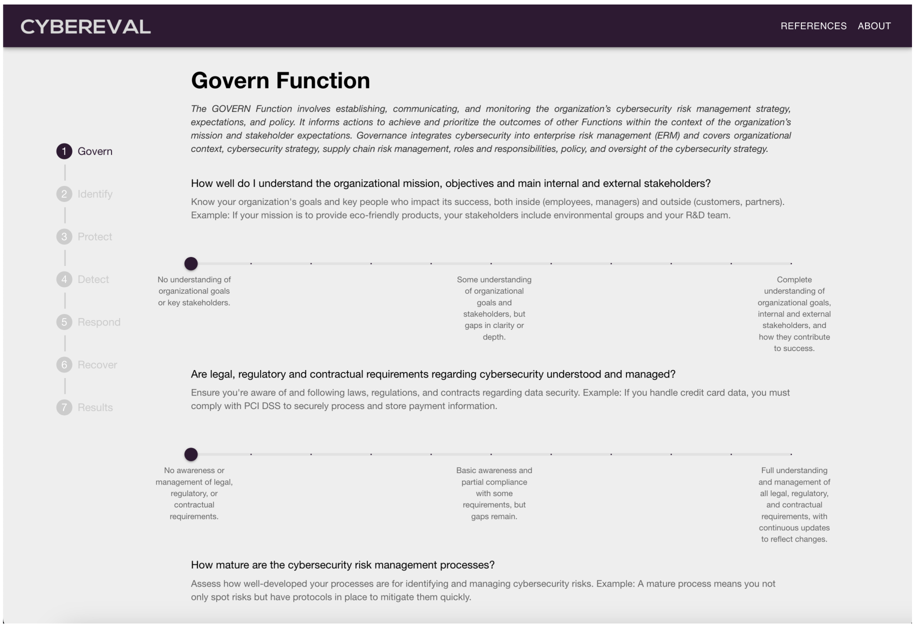
Small to medium-sized enterprises generally employ fewer than 50 people and have annual revenues under $10 million, while medium enterprises employ between 50 and 250 people with revenues ranging up to $50 million. They are widely recognized for their role in economic growth, innovation, and job creation, particularly in emerging markets. Although SMEs play a major role in the economy, they often operate with limited budgets. This makes it challenging for them to allocate resources toward areas outside their core business, such as cybersecurity measures, increasing their vulnerability to cyber threats.

How Does CyberEval Work?

CyberEval is a guide that proposes a tool that helps you evaluating your current cybersecurity maturity level and set a target one. We start off with a questionnaire based on the NIST Cybersecurity Framework (CSF) 2.0, divided into 6 main categories (functions) that organizes the questions in a thematic way. Based on the provided answers, the tool provides you recommendations of open source tools and information that can be used to reach the target maturity level. To help you understand the recommendations and the main concepts, there's a dedicated references page (check the References page above) with the main definitions and concepts of cybersecurity and about this project.

Figure 7 – CyberEval's home page.

At the end of the page, there's a button that moves the user to the questionnaire page. CyberEval's questionnaire is divided in 7 steps that concern all NIST functions and the results page. For each function, there's a description at the beginning to help the user understand what is being evaluated. Following the description, the questions are presented with descriptions, examples and the definition of the ratings.



Govern Function

The GOVERN Function involves establishing, communicating, and monitoring the organization's cybersecurity risk management strategy, expectations, and policy. It informs actions to achieve and prioritize the outcomes of other Functions within the context of the organization's mission and stakeholder expectations. Governance integrates cybersecurity into enterprise risk management (ERM) and covers organizational context, cybersecurity strategy, supply chain risk management, roles and responsibilities, policy, and oversight of the cybersecurity strategy.

How well do I understand the organizational mission, objectives and main internal and external stakeholders?

Know your organization's goals and key people who impact its success, both inside (employees, managers) and outside (customers, partners). Example: If your mission is to provide eco-friendly products, your stakeholders include environmental groups and your R&D team.

No understanding of organizational goals or key stakeholders.

Some understanding of organizational goals and stakeholders, but gaps in clarity or depth.

Complete understanding of organizational goals, internal and external stakeholders, and how they contribute to success.

Are legal, regulatory and contractual requirements regarding cybersecurity understood and managed?

Ensure you're aware of and following laws, regulations, and contracts regarding data security. Example: If you handle credit card data, you must comply with PCI DSS to securely process and store payment information.

No awareness or management of legal, regulatory, or contractual requirements.

Basic awareness and partial compliance with some requirements, but gaps remain.

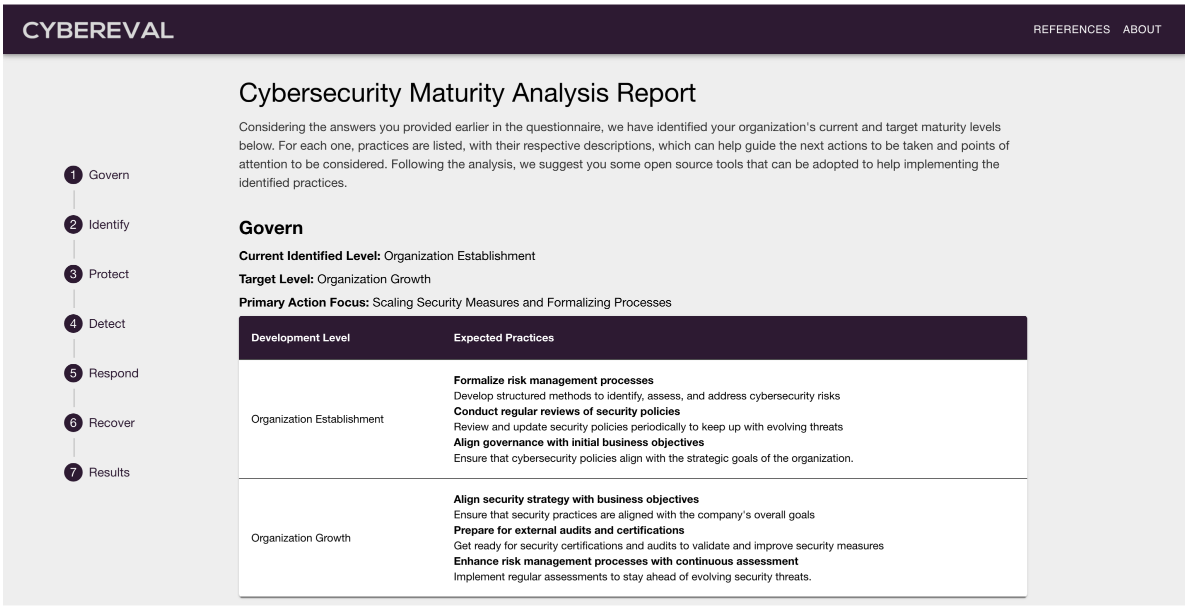
Full understanding and management of all legal, regulatory, and contractual requirements, with continuous updates to reflect changes.

How mature are the cybersecurity risk management processes?

Assess how well-developed your processes are for identifying and managing cybersecurity risks. Example: A mature process means you not only spot risks but have protocols in place to mitigate them quickly.

Figure 8 – CyberEval's questionnaire.

Once the questionnaire is completed, the results page is shown with the calculated current and target levels of cybersecurity maturity. For each function, there's a table with expected practices for both levels with a brief description of the practice. At the end, there's another table with recommendations of open source tools with examples of use cases and for which function needs they're most adapted.



Cybersecurity Maturity Analysis Report

Considering the answers you provided earlier in the questionnaire, we have identified your organization's current and target maturity levels below. For each one, practices are listed, with their respective descriptions, which can help guide the next actions to be taken and points of attention to be considered. Following the analysis, we suggest you some open source tools that can be adopted to help implementing the identified practices.

Govern

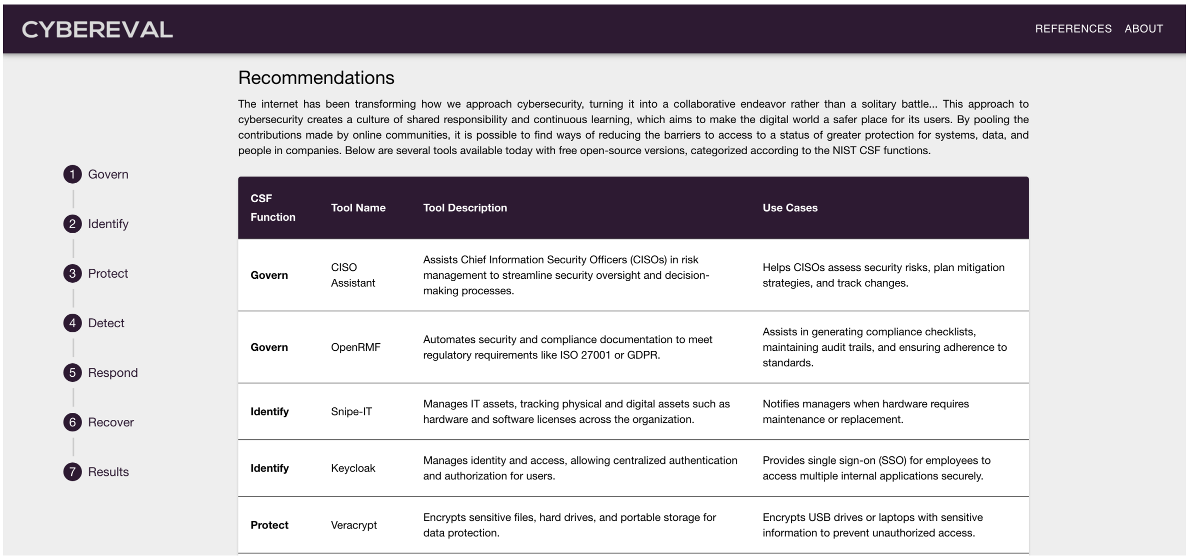
Current Identified Level: Organization Establishment

Target Level: Organization Growth

Primary Action Focus: Scaling Security Measures and Formalizing Processes

Development Level	Expected Practices
Organization Establishment	**Formalize risk management processes** Develop structured methods to identify, assess, and address cybersecurity risks **Conduct regular reviews of security policies** Review and update security policies periodically to keep up with evolving threats **Align governance with initial business objectives** Ensure that cybersecurity policies align with the strategic goals of the organization.
Organization Growth	**Align security strategy with business objectives** Ensure that security practices are aligned with the company's overall goals **Prepare for external audits and certifications** Get ready for security certifications and audits to validate and improve security measures **Enhance risk management processes with continuous assessment** Implement regular assessments to stay ahead of evolving security threats.

Figure 9 – CyberEval's results presentation.



Recommendations

The internet has been transforming how we approach cybersecurity, turning it into a collaborative endeavor rather than a solitary battle... This approach to cybersecurity creates a culture of shared responsibility and continuous learning, which aims to make the digital world a safer place for its users. By pooling the contributions made by online communities, it is possible to find ways of reducing the barriers to access to a status of greater protection for systems, data, and people in companies. Below are several tools available today with free open-source versions, categorized according to the NIST CSF functions.

CSF Function	Tool Name	Tool Description	Use Cases
Govern	CISO Assistant	Assists Chief Information Security Officers (CISOs) in risk management to streamline security oversight and decision-making processes.	Helps CISOs assess security risks, plan mitigation strategies, and track changes.
Govern	OpenRMF	Automates security and compliance documentation to meet regulatory requirements like ISO 27001 or GDPR.	Assists in generating compliance checklists, maintaining audit trails, and ensuring adherence to standards.
Identify	Snipe-IT	Manages IT assets, tracking physical and digital assets such as hardware and software licenses across the organization.	Notifies managers when hardware requires maintenance or replacement.
Identify	Keycloak	Manages identity and access, allowing centralized authentication and authorization for users.	Provides single sign-on (SSO) for employees to access multiple internal applications securely.
Protect	Veracrypt	Encrypts sensitive files, hard drives, and portable storage for data protection.	Encrypts USB drives or laptops with sensitive information to prevent unauthorized access.

Figure 10 – CyberEval's open source tools recommendations.

6 Concluding Remarks

6.1 Conclusions of the Graduation Project

The work carried out aims to propose a cybersecurity guide for small and medium-sized companies in order to assess and better understand the organization's level of cyber maturity. Based on the information collected through an assessment inspired by the NIST framework, it will be possible to draw up an action plan with a target maturity level as a reference. This target level is determined based on the tables developed in this work which define, for each of the 6 functions of the NIST CSF, the focus of cybersecurity actions and what is expected in terms of practices and infrastructure in the organization. In order to reach the target level, open source tools are proposed to help with the next steps. As this work seeks to reinforce the importance of community efforts, especially the sharing of open source tools and information, it can be accessed free of charge by people and organizations who are interested in better understanding and improving their cybersecurity maturity.

6.1.1 Contributions to the existing solutions

As noted in the literature review, there has been a growing discussion about the importance of cybersecurity in recent years, especially given the context of technological development and digital transition. Several studies have been identified that present an analysis of the current state of maturity of small and medium-sized companies in different sectors in terms of implementing cybersecurity measures and policies. Some papers go further and propose tools and frameworks that can help SMEs better understand their level of protection and identify the main points to work on.

However, at the same time as there is a wide availability of information, there are various sources of information on the Internet with sometimes contradictory details, which can cause confusion and mistrust. In addition, despite the numerous solutions proposed, when we focus on SMEs and tech startups, we see a gap in terms of the adoption of open source solutions to deal with the potentially high costs of a cybersecurity infrastructure. This creates an opportunity to take advantage of using the tools and information available in an effective way. With these elements in mind, this work brings some contributions to the existing issue:

- Centralization of information from reliable sources: the main actors in the cybersecurity field were listed, including mainly government institutions and organizations supported by the open source community.

- Focus on open source tools and information: among the constraints on establishing an information security infrastructure was the matter of the investment required. The use of open source tools and information allows us to keep up with best practices, as well as significantly reducing costs.

- Adaptation of the evaluation tool according to the degree of development and growth of a business/organization: the propositions and levels of cybersecurity maturity of SMEs are divided according to their levels of development. This was one of the problems identified in the literature that hindered the implementation of tools by startups.

6.1.2 Limitations of this work

One of the main challenges of creating a cybersecurity tool is to make it accessible to all types of public. This work reduces existing barriers by introducing basic concepts, an adaptation of existing frameworks in a more simplified format and existing tools that could be used in an organization. However, there are still some topics that require a minimum technical level, such as the implementation of the proposed solutions. Furthermore, even with easier access to information on information security, the presence of a professional with training in the area is indispensable for monitoring practices and projects, training other professionals and incorporating new tools and policies into the organization. Another problem in this work is associated with fact that declarative assessments may have a certain subjectivity in the answers. Although the tool provides useful and applicable data for increasing a company's maturity, providing answers that do not reflect reality will generate answers and recommendations that are inappropriate to the organization's real needs.

As mentioned before, this work brings together a lot of useful information and solutions for companies, but it doesn't necessarily provide the means to technically implement the free versions. A new interaction of the project could find ways to aggregate the existing tools to create a single, comprehensive solution.

6.2 Next Steps

Regarding the next steps, CyberEval's recommendations can be improven by providing more practices and examples to illustrate the cyber maturity levels. In addition, different tools may be suggested in function of the responses provided by the users instead of having a single list regardless of the level obtained.

One of the main issues identified in the literature review was that there is no evaluation of the return on security investments that would allow managers to make an appropriate decision when allocating the budget. Quantifying this is a challenging task, as the values vary depending on the type of company and the activity carried out. In addition, each type of cybersecurity incident has different financial impacts for an organization: incidents of system availability and failure, ransomware, data leaks, etc. and can only be estimated without a detailed study of each case. Despite these difficulties, with the availability of information on the internet, it is possible to use past reports and incidents to identify possible expenses and financial impacts. In 2019, IBM produced a report on The Cost of a Data Breach in which it details the main contributors, impacts, types of attacks and the vulnerabilities linked to the leaks. Among the most important discoveries are:

Lost business is the most significant contributor to the total cost of a data breach, driven largely by the loss of customer trust. In 2019, the average cost of lost business was $1.42 million, making up 36% of the total average breach cost of $3.92 million. Organizations that suffered greater customer turnover—4% or more—faced substantially higher costs, averaging $5.7 million, which is 45% above the average breach cost. This highlights the severe financial impact of customer attrition following a breach.

Data breach costs often extend beyond the immediate aftermath, with a significant portion occurring in the years following the incident. Approximately one-third of breach costs were incurred more than a year after the breach, particularly in highly regulated industries like healthcare and finance. Organizations in these sectors saw only 53% of costs in the first year, with 32% and 16% accruing in the second year and beyond, respectively. The lifecycle of a data breach — the time from occurrence to containment — has been increasing, which in turn escalates the costs. In 2019, the average breach lifecycle was 279 days, up from 266 days in 2018. Notably, breaches that took longer than 200 days to contain were 37% more expensive than those resolved more quickly. The study also found that breaches caused by malicious attacks, which are both the most common and the most costly, had a lifecycle of 314 days on average, leading to significantly higher costs compared to breaches caused by human error or system glitches.

Focusing more specifically on SMEs, we observe that the impact of data breaches on small businesses is particularly severe, as they face disproportionately higher costs relative to their size compared to larger organizations. While the average total cost of a breach for a small business with 500 to 1,000 employees was $2.65 million, this translates to a staggering $3,533 per employee, a burden that is much harder for smaller businesses to absorb. This high per-employee cost can cripple a small business's financial health, making recovery from a breach more challenging. For small businesses, where resources are often limited, a single data breach can threaten their survival, which highlights the critical need for robust cybersecurity measures and proactive risk management.

As next steps, it is possible to use this type of information source to determine the potential financial losses that an organization could face if it is the target of cyberattacks. With concrete support, based on facts observed in the market, the importance of adopting a cybersecurity stance gains strength and becomes more understandable so that decisions in favor of investing in information security can be made.

Bibliography

ABBOTT, R. G. et al. Log analysis of cyber security training exercises. *Procedia Manufacturing*, v. 3, n. 1, p. 5088–5094, 2015. Cited on page 16.

ABRAHAM, C.; CHATTERJEE, D.; SIMS, R. Muddling through cybersecurity: Insights from the u.s. healthcare industry. *Business Horizons*, v. 4, n. 62, p. 539–548, 2018. Cited on page 16.

AJMI, L. et al. A novel cybersecurity framework for countermeasure of sme's in saudi arabia. *2019 2nd International Conference on Computer Applications; Information Security (ICCAIS)*, 2019. Cited 2 times on pages 18 and 20.

BASKERVILLE, R.; SPAGNOLETTI, P.; KIM, J. Incident-centered information security: Managing a strategic balance between prevention and response. *Inf. Manag.*, v. 51, n. 1, p. 138–151, 2014. Cited 2 times on pages 17 and 20.

BEACHBOARD, J. C. et al. Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda. *Issues in Informing Science and Information Technology*, v. 5, n. 1, p. 73–85, 2008. Cited on page 15.

BENZ, M.; CHATTERJEE, D. Calculated risk? a cybersecurity evaluation tool for smes. *Business Horizons*, v. 63, n. 4, p. 531–540, 2020. Cited 2 times on pages 17 and 20.

CARPENTIER, J. *La sécurité informatique dans la petite entreprise - Etat de l'art et Bonnes Pratiques*. 3. ed. Rio de Janeiro: Editions ENI, 2016. Cited on page 22.

CLOZEL, L. *Banks get (yet another) cybersecurity framework, this time from G-7*. 2016. American Banker. Disponível em: <https://www.proquest.com/newspapers/banks-get-yet-anothercybersecurity-framework/docview/1828205806/se-2>. Acesso em: May 27th 2024. Cited on page 15.

DELOITTE. *2014 Deloitte NASCIO Cybersecurity Study*. 2014. Disponível em: <http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf>. Acesso em: June 2nd 2024. Cited on page 16.

EMER, A.; UNTERHOFER, M.; RAUCH, E. A cybersecurity assessment model for small and medium-sized enterprises. *IEEE Eng. Manag. Rev.*, v. 49, n. 2, p. 98–109, 2021. Cited 2 times on pages 17 and 20.

FERTIG, T.; SCHUTZ, A.; WEBER, K. Current issues of metrics for information security awareness. *European Conference on Information Systems (ECIS)*, v. 109, 2020. Cited on page 19.

GARBA, A. A.; BADE, A. M. An investigation on recent cyber security frameworks as guidelines for organizations adoption. *Int. J. Innov. Sci.Res. Technol.*, v. 6, p. 103–110, 2021. Cited 2 times on pages 16 and 20.

HEIDT, J. P. G. M.; BUXMANN, P. Investigating the security divide between sme and large companies: How sme characteristics influence organizational it security investments. *Inf. Syst. Frontiers*, v. 21, n. 6, p. 1285–1305, 2019. Cited on page 15.

ITAI, Y.; ONWUBIKO, E. Impact of ransomware on cybersecurity. *Int. J. Comput. Technol.*, v. 17, n. 1, p. 7077–7080, 2018. Cited on page 16.

MARICAN, M. N. Y. et al. Cyber security maturity assessment framework for technology startups: A systematic literature review. *IEEE Access*, v. 11, p. 5442–5452, 2023. Cited on page 19.

NAZARETH, D. L.; CHOI, J. A system dynamics model for information security management. *Information & Management*, v. 52, n. 1, p. 123–134, 2015. Cited 2 times on pages 18 and 20.

ONWUBIKO, C.; LENAGHAN, A. P. Managing security threats and vulnerabilities for small to medium enterprises. *Proc. IEEE Intell. Secur. Informat.*, v. 1, n. 1, p. 244–249, 2007. Cited on page 15.

OSBORN, E.; SIMPSON, A. Risk and the small-scale cyber security decision making dialogue.a u.k. case study. *Comput. J.)*, v. 61, n. 4, p. 472–495, 2018. Cited on page 15.

RAWINDARAN, N.; JAYAL, A.; PRAKASH, E. Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers 2021*, v. 10, n. 11, p. 150, 2021. Cited on page 16.

RENAUD, K. How smaller businesses struggle with security advice, computer fraud & security. *Proc. Cybersecurity Cyberforensics Conf. (CCC)*, v. 1, n. 8, p. 10–18, 2016. Cited on page 15.

RENAUD, K.; WEIR, G. R. S. Cybersecurity and the unbearability of uncertainty. *Proc. Cybersecurity Cyberforensics Conf. (CCC)*, v. 1, n. 1, p. 137–143, 2016. Cited 2 times on pages 15 and 16.

SANGANI, N. K. et al. Security & privacy architecture as a service for small and medium enterprises. *International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, v. 3, n. 1, p. 16–21, 2012. Cited on page 16.

SCHMITZ, C.; PAPE, S. Lisra: Lightweight security risk assessment for decision support in information security. *Computers & Security*, v. 90, 2020. Cited 2 times on pages 18 and 20.

UCHENDU, B. et al. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, v. 109, 2021. Cited 2 times on pages 19 and 20.

WIDUP, S. et al. Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Comput. Fraud Secur.*, v. 2020, n. 6, p. 4, 2020. Cited on page 16.