Department of Informatics

CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment

Dissertation submitted to the
Faculty of Business, Economics and Informatics
of the University of Zurich

to obtain the degree of
Doktor der Wissenschaften, Dr. sc.
(corresponds to Doctor of Science, PhD)

presented by
Muriel Figueredo Franco
from
Pelotas, Rio Grande do Sul, Brazil

approved in February 2023

at the request of
Prof. Dr. Burkhard Stiller
Prof. Dr. Aiko Pras
Prof. Dr. Lisandro Zambenedetti Granville

The Faculty of Business, Economics and Informatics of the University of Zurich hereby authorizes the printing of this dissertation, without indicating an opinion of the views expressed in the work.

Zürich, February 15, 2023

The chairman of the Doctoral Board: Prof. Dr. Elaine Huang

Abstract

The increasing number of cyberattacks and their potential disruptive impacts cause significant concerns for companies, governments, and society. A successful cyberattack can, for example, cause financial losses due to business disruption, affect the privacy of people due to data leakages, and make critical resources completely inaccessible for interested stakeholders. This puts cybersecurity at the center of a digital society and as one of the anchors to all technologies and industries that support a connected and automated society. Therefore, it is essential to look at cybersecurity not only as a technical problem, but also from the economic, societal, and legal perspectives.

Today, companies still neglect planning and investments in cybersecurity due to different factors. First, they face budget constraints and do not see cybersecurity investments as a priority. Secondly, the high amount of information and planning complexities makes implementing a cybersecurity strategy cumbersome for companies that do not have in-house expertise. Finally, companies, especially Small and Medium-sized Enterprises (SME), do not see themselves as the target of a potential cyberattack. This utterly wrong view makes SMEs one of the main targets of cyberattacks worldwide, since the likelihood of successful cyberattacks is higher than companies with a well-defined cybersecurity strategy. Therefore, there is still a need for approaches that support companies, especially SMEs, during the cybersecurity planning and investment phases. These phases include supporting the understanding and definition of cybersecurity requirements, the definition of the budget and investment path to achieve a proper level of cybersecurity, and the selection of protections with a positive return on investment, while also satisfying specific business demands.

This PhD thesis addresses these gaps in cybersecurity planning and investments by proposing the *CyberTEA* approach. This approach is composed of a five-phase methodology, a framework, and a set of solutions for cybersecurity planning and investment, considering the technical requirements of cybersecurity and its economic dimensions, such as the potential economic impacts of cyberat-

tacks and the cost-benefit of protections available on the market to protect against specific threats. The methodology describes the key phases to consider during the cybersecurity planning and investment, while the framework maps and implements the components needed to be considered to support the tasks required in each phase. A set of new solutions are also designed and implemented to *(i)* simplify the risk assessment of companies, *(ii)* analyze and classify cyberattacks, *(iii)* calculate the optimal investment in cybersecurity, and *(iv)* recommend protections based on businesses profile. Furthermore, supplementary solutions for cybersecurity planning are placed to contribute to additional aspects and challenges faced by the cybersecurity market, such as information sharing, cyber insurance, and marketplaces for protection.

Quantitative and qualitative evaluations were conducted to analyze different aspects that give evidence of the feasibility, accuracy, and performance of the proposed solutions. These experiments were adapted for each solution according to its dimensions and features under evaluation. The results highlight *(a)* the potential of simplified risk assessment in companies using selected attributes, *(b)* the feasibility and benefits of visualizations to understand and investigate cyberattacks traffic, *(c)* the capacity of ML-based techniques to classify cyberattacks and predicts risks correctly, *(d)* the role of conversational agents as an ally for cybersecurity awareness and risk management, *(e)* the benefits of solutions that integrate cybersecurity metrics during the decision process, and *(f)* the feasibility of protection recommender systems. Finally, an end-to-end case study is conducted to show the application of the proposed methodology in a company, supported by the information obtained with each one of the solutions implemented as part of this PhD thesis.

All of these evaluations and contributions show evidence of scientific advances in cybersecurity planning while highlighting and paving the path for stakeholders (*e.g.*, decision-makers, developers, researchers, and companies) to implement more cost-effective solutions and strategies related to cybersecurity. This also contributes to understanding the relationship and dimensions of economic and technical aspects of cybersecurity, thus, providing directions for further advances in the field and its multidisciplinary facets.

Kurzfassung

Die zunehmende Zahl von Cyberangriffen und ihre potenziell störenden Auswirkungen geben Unternehmen, Regierungen und der Gesellschaft Anlass zu großer Sorge. Ein erfolgreicher Cyberangriff kann beispielsweise finanzielle Verluste aufgrund von Geschäftsunterbrechungen verursachen, die Privatsphäre von Menschen durch Datenlecks beeinträchtigen und kritische Ressourcen für interessierte Akteure völlig unzugänglich machen. Damit steht die Cybersicherheit im Mittelpunkt einer digitalen Gesellschaft und ist einer der Anker für alle Technologien und Branchen, die eine stärker vernetzte und automatisierte Gesellschaft anstreben. Daher ist es wichtig, Cybersicherheit nicht nur als technisches Problem, sondern auch aus wirtschaftlicher, gesellschaftlicher und rechtlicher Sicht zu betrachten.

Heute vernachlässigen Unternehmen aus verschiedenen Gründen noch immer die Planung und Investitionen in die Cybersicherheit. Erstens sind sie mit Budgetbeschränkungen konfrontiert und sehen Investitionen in die Cybersicherheit nicht als Priorität an. Zweitens macht die große Menge an Informationen und die Komplexität die Umsetzung einer Cybersicherheitsstrategie für Unternehmen, die nicht über internes Fachwissen verfügen, mühsam. Schließlich sehen sich Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), nicht als potenzielles Ziel von Cyberangriffen. Diese völlig falsche Sichtweise macht KMU zu einem der Hauptziele von Cyberangriffen weltweit, da die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs höher ist als bei Unternehmen mit einer gut definierten Cybersicherheitsstrategie. Daher besteht nach wie vor ein Bedarf an Ansätzen, die Unternehmen, insbesondere KMU, bei der Planung und Investition in die Cybersicherheit unterstützen. Zu diesen Aufgaben gehören die Unterstützung beim Verständnis und der Definition der Cybersicherheitsanforderungen, die Festlegung des Budgets und des Investitionspfads, um ein angemessenes Cybersicherheitsniveau zu erreichen, und die Auswahl von Schutzmaßnahmen mit einer positiven Kapitalrendite, die gleichzeitig alle geschäftlichen Anforderungen erfüllen.

Die vorliegende Dissertation schließt diese Lücke, indem sie den *CyberTEA*-Ansatz vorschlägt. Der Ansatz besteht aus einer Fünf-Phasen-Methodik, einem Rahmenwerk und einer Reihe von Lösungen für die Cybersicherheitsplanung und -investition unter Berücksichtigung der technischen Anforderungen der Cybersicherheit und ihrer wirtschaftlichen Dimensionen, wie z. B. der potenziellen wirtschaftlichen Auswirkungen und des Kosten-Nutzen-Verhältnisses der verfügbaren Schutzmaßnahmen. Die Methodik beschreibt die wichtigsten Phasen, die bei der Cybersicherheitsplanung und -investition zu berücksichtigen sind, während der Rahmen die Komponenten abbildet und implementiert, die zur Unterstützung dieser Phasen und Hauptaufgaben zu berücksichtigen sind. Darüber hinaus wurde eine Reihe neuer Lösungen entwickelt und implementiert, um *(i)* die Risikobewertung von Unternehmen zu vereinfachen, *(ii)* Cyberangriffe zu analysieren und zu klassifizieren, *(iii)* die optimale Investition in Cybersicherheit zu berechnen und *(iv)* Schutzmaßnahmen auf der Grundlage des Unternehmensprofils zu empfehlen. Darüber hinaus werden ergänzende Lösungen angeboten, um zusätzliche Aspekte und Herausforderungen des Cybersicherheitsmarktes zu bewältigen, z. B. Informationsaustausch, Cyberversicherungen und Marktplätze für Schutz.

Es wurden quantitative und qualitative Bewertungen durchgeführt, um verschiedene Aspekte zu analysieren, die Aufschluss über die Machbarkeit, Genauigkeit und Leistung der vorgeschlagenen Lösungen geben. Diese Experimente wurden für jede Lösung entsprechend ihrer Dimensionen und Merkmale, die bewertet wurden, angepasst.

Alle diese Bewertungen und Beiträge belegen wissenschaftliche Fortschritte in der Cybersicherheitsplanung und zeigen gleichzeitig den Weg für die Beteiligten (Entscheidungsträger, Entwickler, Forscher und Unternehmen) auf, kosteneffizientere Lösungen und Strategien im Bereich der Cybersicherheit umzusetzen. Dies trägt auch dazu bei, die Beziehung und die Dimensionen der wirtschaftlichen und technischen Aspekte der Cybersicherheit zu verstehen, und gibt so die Richtung für weitere Fortschritte in diesem Bereich und seinen multidisziplinären Facetten vor.

This thesis is dedicated to my family and friends, especially those who supported me with love and courage during the journey. It is essential to chase our dreams but always know the road that will lead us home again.

Acknowledgments

First and foremost, I would like to thank my family. My father Luis Eduardo and my mother Rosana gave me love and taught me essential pillars that guide my life. If I achieved something in my life, it was because of you. Thank you for everything. Also, I can't forget to thank my loved grandfather Milton and grandmother Marlene (in memorian). They were celebrating and proud of all my achievements since I was a kid but also teaching me valuable lessons about life. Also, a big thank you to my brother and best friend Pablo (aka Bolacha) and my sister-in-law Paula. I am fortunate to have my brother and his wife as great friends. They were of utmost importance during these years, participating in all good and bad moments. I am grateful for your friendship. My eternal gratitude to my beloved fiancee and future wife, Mariana. She has been with me since my bachelor studies, supporting me in all steps and helping me to surpass all barriers with her kind and calm personality. Even with the distance, I felt you with me every day. Thank you very much, baby. Finally, thanks to the entire "Familia Franco" for all your love and support. This achievement also belongs to all of you. Thanks also to all my friends for being my daily connection with home.

A quote says that a thousand-mile journey begins with one step. My research journey started end of 2010 at the University Federal de Pelotas (UFPEL). Prof. Dr. Anderson Ferrugem and Prof. Dr. Antônio César Silveira allowed me to work during four years as their undergraduate student researcher. These years working with such brilliant professors and - most important - extraordinary human beings made it crystal clear to me that this journey was the one I would like to be on. Thank you for all the opportunities, support, and guidance.

During my master's degree at the Federal University of Rio Grande do Sul (UFRGS), I worked directly with Prof. Dr. Lisandro Z. Granville. I will always be grateful for all opportunities and valuable lessons Lisandro gave me. Professors can change lives, and Lisandro changed mine. From a professional point of view, I had the chance to work with outstanding researchers and see cutting-edge research being done. Also, I learned a lot about one of the most important things for a scientist: research methodology. From a personal point of view, during this time at UFRGS, I had insightful

discussions and made friends for life. A special thanks to everyone that was part of the discussions in Lab 210, especially to the unforgettable "Papers Machine" team composed of Dr. Eder Scheid, Dr. Ricardo Santos, Dr. Ricardo Pfitscher, Dr. Arthur Jacobs, and me. It is an honor to have all these guys as friends.

I want to express my deepest gratitude to my PhD supervisor Prof. Dr. Burkhard Stiller. Besides guiding me during this exciting and challenging journey, Burkhard gave me incredible opportunities I had never expected in life. I am grateful for your trust in me for all business, teaching, and research activities. The opportunities that Burkhard and the Communication Systems Group (CSG) gave me were fantastic. I hope everyone can have the chance to have a mentor that provides freedom, support, and tools needed for professional and personal development, as Burkhard gave me. Thank you very much for that, professor.

I found a second family in the CSG, even a thousand kilometers from home. It was terrific to know many new people and cultures. I met many friendly, intelligent, competent, and interesting people there, and I am sure I made friends for life. It was several hours of random discussions about work and life and several liters of coffee and beers. This results in an incredible number of scientific publications, but more important: laughs, friendship, complicity, and lessons for life. I want to thank my friends Dr. Eder Scheid, Christian Killer, Dr. Alberto Huertas, Jan von der Assen, and the new generation Chao Feng and Katharina Mueller. You made this journey much better, funny, and meaningful. It was terrific to meet extraordinary scientists and human beings like you.

Thank you to all 28 students I supervised during their successful bachelor's or master's thesis at the University of Zurich. It was amazing to have the opportunity to work with brilliant developers and computer scientists. I have learned a lot from you, and I did my best to make your journey along your thesis worthy. A special thank you to Erion Sula, Jan von der Assen, Luc Boilat, Bulin Shaqiri, and Christian Omlin, whose contributions were very relevant to developing the CyberTEA approach. Last but not least, I would like to thank the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project. The CONCORDIA project and its community were essential for developing this work and my professional maturity.

I am proud of the journey that has brought me to this point. I hope to contribute to society as the best professional and person possible, ever in the light of science, critical thinking, and honesty. Quoting the Brazilian poet Sergio Vaz: "Revolucionário é todo aquele que quer mudar o mundo e tem a coragem de começar por si mesmo". This motivates me to look for new challenges daily to be a better person and professional for the world and everyone close to me. It is time to continue life's journey with the same enthusiasm and resilience that moved me here.

Contents

In the long run men only hit what they aim at. Therefore, though they should fail immediately, they had better aim at something high.

Henry David Thoreau

1 Introduction

CYBERATTACKS determine a rising threat for governments and companies. As businesses become more digital, they are exposed to an increasing number of threats [63]. Thus, beyond compromising companies' and their customers' security and privacy, malicious attackers can negatively impact the economy of businesses or services supported by digital systems [75, 197]. Predictions from Cybersecurity Ventures, the world's leading researcher for the global cyber economy, indicate that cybercrime damages will hit US$ 10 trillion annually by 2025 [200]. Such damages comprise both direct and indirect costs, including those involved with the loss of critical data, asset theft, business disruption, and reputation harm [105]. In 2019, for example, a ransomware attack impacted the National Health System (NHS) of the United Kingdom, resulting in a loss of US$ 100 million and 19,000 appointments canceled, including necessary procedures, such as exams and surgeries [165]. Based on such facts, it is clear that cybersecurity can no longer be seen just as a technology issue but must also be watched from an economic, societal, and legal perspective.

In the current scenario of several different cyberattacks, Distributed Denial-of-Service (DDoS) attacks remain one of the most dangerous threats to service providers. DDoS attacks are responsible for most of the occurrences impacting service downtime and performance degradation [16]. This kind of attack can also be amplified by using networks of bots (*i.e.*, botnets) composed of infected

devices that are in the attackers' control [97]. For example, the large number of vulnerable Internet-of-Things (IoT) devices eases the spreading of botnets to launch massive attacks on service providers [2]. Although DDoS attacks are a concern, diverse cyberattacks (*e.g.*, code injections and phishing) are evolving with different purposes, and they are dangerous to the targeted system as well [235]. Threats directly related to data are one of the main concerns for the following years [122], resulting in data leakage or even business disruption due to the unavailability of critical data. For example, different types of malware and ransomware attacks can affect the confidentiality, integrity, and availability of companies' data and systems [202]. Threats to data are also one of the key concerns for IoT scenarios that need to handle a massive amount of data and have strong privacy requirements.

In response to this rising number of cyberattacks, efforts increased to evolve traditional protections and develop novel cybersecurity solutions (*e.g.*, based on artificial intelligence and blockchains). Currently, large companies invest in solutions and response teams to ensure availability and protect critical services and infrastructures. Thus, the cybersecurity market is worth billions of dollars [199] and investments are steadily rising. According to reports [22, 78], the global cyber security market is currently worth around US$ 145 billion and is set to increase by 86% by 2026.

Figure 1.1 highlights the cybersecurity investment trend from 2012 until 2026, according to actual data and predictions. Also, it is important to mention that the biggest of these investments is for external managed security services. Only approximately 25% of these investments are for internal security, such as full-time cybersecurity employees, training, and in-house solutions. Therefore, companies that does not have dedicated teams and internal security tend to spend much more money outsourcing cybersecurity and with external consultancy to understand companies' needs and requirements in terms of cybersecurity.

Even though large companies and governments are increasing their investments in cybersecurity, many of the problems plaguing cybersecurity are of economic nature. Often, systems fail because the organizations do not bear to assess the total costs of a failure nor the risks involved [159]. This problem is prevalent in companies with a small budget to invest in cybersecurity and also show a lack of technical expertise, such as Small- and Medium-size Enterprises (SME). The European Union (EU) classifies a small-sized enterprise as a company with fewer than 50 employees and a medium-sized enterprise as one with less than 250 employees. In addition to small and mid-size companies, there are micro-companies, which employ up to 10 employees [60]. These three kinds of companies (*i.e.*, SMEs and micro-companies), for example, make up over 99% of the Swiss companies and are responsible for two-thirds of the jobs in Switzerland [184].

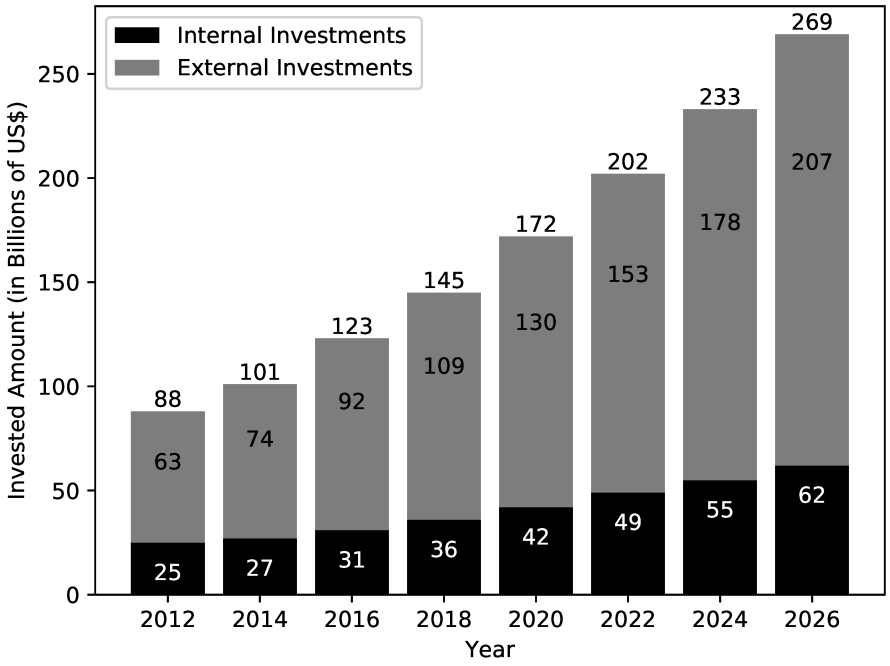


Figure 1.1: Evolution and Prediction of Amount of Cybersecurity Investments along the Years, based on [22]

Among the cyber threats for SMEs, the most prominent malware is ransomware attacks [202, 232], which rely on social engineering skills, vulnerabilities, and misconfiguration of systems to control companies' critical data, thus, resulting in business disruption and data breaches [19]. Different approaches are recommended to prevent and/or recover from a ransomware attack, including effective backup strategies, staff security awareness training, up-to-date software, and monitoring tools. However, SMEs frequently neglect these approaches, primarily due to a lack of economic and technical resources, including an insufficient budget, limited personnel skills, and reduced cybersecurity knowledge [43].

Besides, many SMEs falsely believe that they are not a target for cybercrime [36]. These SMEs do not run a proper risk assessment on their businesses, thus, relying on wrong assumptions, which make them unaware of the actual risks. For example, while 60% of the United States and United Kingdom SMEs think that their businesses are unlikely to be targeted by cyberattacks, the reality is the opposite, with a significant amount of breaches and cyberattacks targeting SMEs [233]. This reality is not different in the Swiss SMEs scenario [42], with companies also missing adequate risk assessment and cybersecurity awareness. This leads to a not well-defined or even absent cybersecurity strategy for SMEs. Thus, based on this scenario, cybercriminals tend to see SMEs as a preferred target due to a higher likelihood of a successful compromise of the attacker's target [73].

A cybersecurity strategy can be defined as a plan of actions designed to improve the security and resilience of companies' Information Technology (IT) infrastructures and services [66]. The strategy has to consider, for example, the most common threats for the company and adjacent sector, its specific risks, and the possible impacts of a cyberattack on the business. Also, the company's environment has to be considered as key for the definition of an efficient and, most importantly, feasible strategy. The environment can be composed of different elements, such as the company's culture, the employees' skills, the financial capacity to invest in cybersecurity, stakeholders, and governance aspects.

Currently, the guidelines for investments in cybersecurity focus on the adoption of traditional solutions (*e.g.*, firewall, backups, and antivirus), the business continuity and disaster recovery plans, cybersecurity training for employees, and cloud-based protections (*e.g.*, DDoS attack protections, end-point antivirus, and monitoring solutions) [71]. Since the cybersecurity market is becoming very profitable and shows a growing trend for the following years [199], financial incentives attract new providers to enter the market by offering cost-efficient protection solutions (*e.g.*, related to the deployment, configuration, and operation of services). These solutions may, for example, include the acquisition of physical appliances, software licenses, training services, and cloud-based protection. Besides, cyber insurers can also have an essential role in such a market [140], since effective economic strategies might involve investment not only in protections, but also in reducing risks of financial loss if an attack damages critical services or data. However, as more approaches and solutions become available, the decision process for SMEs becomes even more complex for planning and investing in cybersecurity, which may result in resources (*i.e.*, money, time, and personnel) allocated inefficiently. This may result in an inadequate level of protection, effectively over- or under-investing in key cybersecurity elements, and exposure to several potential economic impacts caused by cyberattacks.

It is possible to identify at least three fundamental areas to focus on for the planning of cybersecurity strategies and investment decisions: People, Process, and Technology. *People* have to be aware of the risks and their roles in the company. *Processes* must be defined to promote and enforce a robust cybersecurity strategy (*e.g.*, security policies, governance, and compliance). Finally, *Technology* has to be used to fulfill the requirements defined in the cybersecurity strategy. Figure 1.2 highlights these fundamental areas and shows examples for each one of them. With these areas as a core, it is possible to make cybersecurity an ally and conduct key investments for SMEs placed in the digital world, thus, helping to minimize possible economic and societal impacts of cyberattacks on both companies and society.

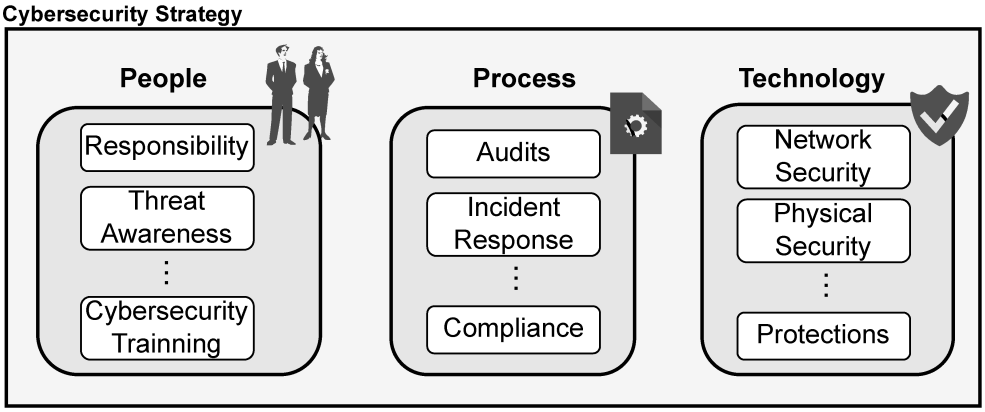


Figure 1.2: Fundamental Areas for Building a Cybersecurity Strategy

1.1 Problem Statement

The common underlying challenges of SMEs are related to the management awareness and commitment to a cybersecurity strategy. These challenges are directly related to the complexities in defining a cybersecurity strategy, including the investment budget, human and technical resources allocation, and effective plan and deployment of cybersecurity practices.

The European Network and Information Security Agency (ENISA) published a survey [70] conducted within 249 SMEs from 25 European member states, which highlighted that cybersecurity is a key concern for 85% of the participants. Also, most interviewed SMEs were relying on basic security controls, such as backup, antivirus, and firewalls. Less than 30% of the participants have a business continuity and disaster recovery plan in case of a cyberattack happening. The most significant challenges for SMEs identified by the survey can be summarized as follow:

- Low cybersecurity awareness of the employees and lack of cybersecurity experts;
- Inefficient risk assessment of threats and inadequate protection of sensitive information and systems;
- Insufficient budget allocated for cybersecurity; and
- Lack of knowledge and support for the planning, deployment, and management of cybersecurity strategies.

Cybersecurity research started to consider SMEs after 2005, grabbing researchers' attention in recent years [176]. However, the number of researches considering SMEs and their specific demands

is still significantly reduced compared to the total number of researches on the cybersecurity field (*e.g.*, monitoring, identification, and mitigation of cyberattacks). Today, SMEs need clear guidelines for implementing existing cybersecurity standards [62] and establishing an efficient cybersecurity strategy [10]. However, the cost of acquiring and implementing these standards or solutions is still a problem for SMEs. Thus, it is key that novel approaches focus on addressing the tasks that involve the planning and investments in cybersecurity, such as risk assessment, threat identification, and budget allocation for effective deployment and management of cybersecurity. Therefore, cybersecurity approaches must consider the reality of SMEs, which frequently do not have in-house knowledge, personnel, and budget for dedicated and expensive cybersecurity tasks. Figure 1.3 gives examples of tasks required to be performed for defining and deploying an efficient cybersecurity strategy. These tasks are not trivial, since they involve a different set of previous knowledge and expertise for accurate and efficient planning to protect the businesses.

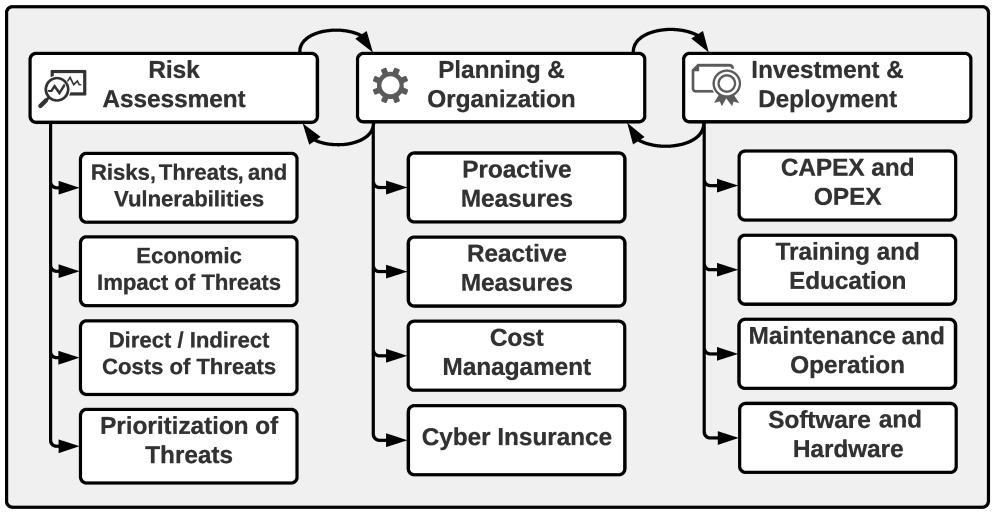


Figure 1.3: Example of Tasks Required for the Definition and Deployment of an Efficient Cybersecurity Strategy

Thus, the problem addressed is the lack of approaches supporting cybersecurity planning that considers and reduces the complexity of cybersecurity tasks (*e.g.*, risk assessment, planning, and investment) for SMEs and companies without expertise in cybersecurity. A set of sub-problems is also tackled, which includes: *(i)* the lack of risk assessment approaches considering the economic nature of cybersecurity, *(ii)* the limited number of cybersecurity tools tailored for SMEs, and *(iii)* the gap

in guidelines and examples to support the evolution of cybersecurity planning and investment taking into account the technical and economic demands of businesses.

1.2 Research Questions

This PhD thesis tackles the outlined challenges in Section 1.1 by providing an approach that addresses the relevant steps, from a technical and economic view, required for the planning and implementation of an efficient cybersecurity strategy, thus, supporting companies with technical and economic constraints to achieve a suitable level of protection for their information and systems. Within this context, five Research Questions (RQ) were defined to guide the research conducted in this PhD thesis. Thus, this PhD thesis is driven by the following RQs:

RQ1 - Which technical and economic aspects have to be considered during the planning and investing process to adopt cybersecurity strategies in SMEs?

This RQ1 involves the analysis of the different requirements to be considered before decisions to invest in a specific cybersecurity measure. The work on RQ1 will assess the current SME scenarios, considering their requirements. A deep understanding about the market, its cybersecurity culture, and main threats is required to map the most important steps of the cybersecurity planning in SMEs.

RQ2 - What are and how to organize and simplify the key steps, information, models, and techniques required for an effective definition of a cybersecurity strategy in SMEs?

This RQ2 focuses on mapping and selecting the essential steps into phases to guide the SME to plan and define a cybersecurity strategy. The inputs from RQ1 have to be used to provide a methodology that supports SMEs to address all the different requirements, steps, and challenges involved in cybersecurity planning and investment.

RQ3 - What are the necessary architectural components and actors to satisfy key steps and to allow SMEs to implement cost-effective cybersecurity strategies?

This RQ3 focuses on the challenge of determining how to integrate different cybersecurity planning solutions in a framework with a well-defined flow, components, and actors. This integration also has to consider the different information that has to be processed by specific components to be used as input for the different solutions. Thus, this RQ3 determines a technical path to be followed by the solutions proposed to answer the RQ5.

RQ4 - How to determine the optimum amount of resources (*e.g.*, money, personnel, and time) an SME should invest in cybersecurity based on their specific technical and economic demands?

This RQ4 consists of the analysis of the trade-offs between investments and protection. This RQ focuses on investigating the amount of money and the level of protection appropriate for a cost-effective cybersecurity strategy. Thus, the focus is on understanding whether there is a maximum or minimum budget for cybersecurity in SMEs (*e.g.*, based on the company's yearly revenue). Also, from an economic perspective, it is important to understand whether known risks can be assumed or shared, instead of investing more money in cybersecurity.

RQ5 - How to provide cybersecurity solutions capable of abstracting technical details to guide SMEs during the plan and execution of a cybersecurity strategy?

This RQ5 focuses on the proposal of solutions sustained by proof-of-concepts implementations to show the benefits for SMEs and the feasibility of these solutions, focusing on supporting SMEs' adoption of better cybersecurity strategies. The proposed solutions have to fulfill the different elements identified in RQ1, RQ2, and RQ3.

In order to answer these RQs listed above, three major aspects have to be considered and investigated during the research, design, and development of this PhD: *(i)* the critical steps and information for conducting cybersecurity planning and investment, *(ii)* the technical and economic requirements for a feasible cybersecurity strategy, and *(iii)* the features required for solutions to address the current gaps of SMEs during the process of protecting their business.

1.3 Thesis Contributions

This PhD thesis provides contributions to the advancement of the state-of-the-art in the cybersecurity field, most specifically those challenges related to cybersecurity planning and investments. These contributions are summarized as follows:

- **A methodology with well-defined steps to guide SMEs in the process of cybersecurity planning and investments.** A methodology is proposed with the technical and economic key steps mapped for SMEs to conduct cybersecurity planning and investments, including the information and complexities related to risk assessment, definition of technical requirements, cost management, and deployment of cybersecurity strategies.
- **A framework to address SMEs challenges using different solutions.** A technical framework is designed to address the steps determined by the methodology, thus, highlighting all

different stakeholders, components, and interactions required to achieve an ecosystem that covers and supports the most relevant cybersecurity planning and investments processes.

- **Novel solutions to support the decision-making processes of SMEs toward a better cybersecurity strategy:** the design of architectures and development of novel and refreshed cost-efficient solutions are done to provide features that implement core components of the proposed framework while fulfills key steps mapped by the defined methodology. Examples of these solutions include a protections recommendation system, a conversational agent for cybersecurity management, intuitive risk assessment tools based on companies' configuration and specific sectors, threat identification based on the visualization of network traffic, and decentralized cyber insurance models.

Figure 1.4 summarizes the main contributions of this PhD thesis by highlighting the different pieces of work (*i.e.*, methodology, framework, and solutions), from the more general to a more specific level, that compose the Cybersecurity Technical and Economic Approach (CyberTEA). Those contributions improve the understanding of SMEs' cybersecurity planning and investment processes, such as the definition of business profiles, demands, and key aspects to consider during the planning and deployment of a cybersecurity strategy. Further, providing a framework that allows for the integration and simplification of the different cybersecurity steps involved. Finally, novel solutions (*i.e.*, systems and tools) can support the decision process for planning and investing in cybersecurity while also reduces the complexities of understanding businesses risks and cyberattack behavior.

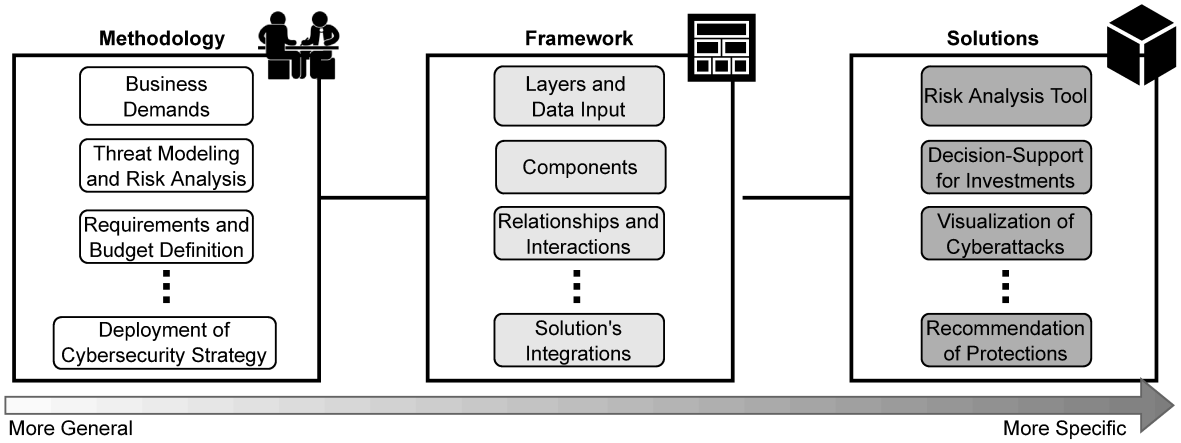


Figure 1.4: Overview Contributions of This PhD thesis

Thus, the *CyberTEA* approach provides a clear path, which can be adapted according to companies demands and processes, to plan, define, and deploy an efficient cybersecurity strategy in a cost-

efficient way (*i.e.*, taking adequate decisions to invest in the cybersecurity solutions that offer an adequate level of protection while also reduce the risks of economic impacts in a business).

It is essential to mention that this PhD thesis considers the concept of the framework defined in Computer Science for software development [126, 154], which means a supporting structure that describes how solutions can be built and also how they do interrelate. This includes, for example, different support programs, applications, toolsets, and Application Programming Interfaces (API). Therefore, the framework proposed by this PhD thesis, using the concepts from computer programming, provides an abstraction to show generic functionality that can be selectively changed by adding additional pieces of code.

This concept is relevant to clarify, because this PhD thesis covers business dimensions also. In the field of business, a framework is defined slightly differently [190, 250]. A framework for the business means a process and fundamental base to guide a business or organization during the operating or planning strategies [185]. It helps by defining well-structured flows for making decisions about processes, projects, and product development in organizations. Therefore, if looking at the contributions of this PhD thesis (*cf.* Figure 1.4) from a business perspective, the methodology proposed becomes a framework, while the framework becomes an architecture that satisfies the framework. A discussion regarding the terminology used is provided in Section 2.5.

1.4 Thesis Outline

This PhD thesis is organized in seven chapters as shown in Figure 1.5. **Chapter 2** provides the theoretical foundations and key concepts of cybersecurity planning and investments, required for a complete understanding of this thesis. This includes the analysis of the most common threats, risks, and their impacts, the most important concepts and goals of cybersecurity economics, and the challenges faced by different companies' sizes and sectors.

Next, **Chapter 3** focuses on the investigation and discussion of the literature regarding cybersecurity planning and investments. For that, a review from an economic view is conducted to map models, frameworks, systems, and tools that address the cybersecurity challenges to provide cost-efficient approaches to reduce the technical and economic impacts of cyberattacks in companies while also addresses challenges of SMEs (*e.g.*, insufficient budget and lack of expertise).

Then, the approach proposed by this PhD thesis is presented in **Chapter 4**. In this chapter, which introduces the *CyberTEA* approach, all its elements are discussed, including the introduction of a methodology for cybersecurity planning and investments, the definition of a framework to address

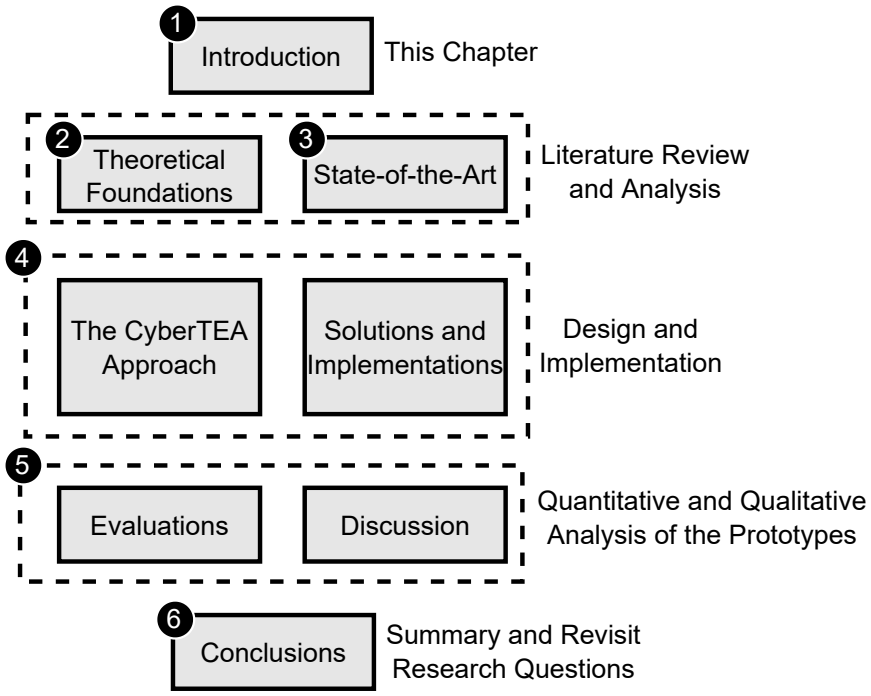


Figure 1.5: Organization of This PhD Thesis

the different steps mapped by the methodology, and the proposal of solutions that fulfills the framework's requirements. These solutions include the risk assessment with an economic bias, threats analysis, investments in cybersecurity, recommendation and deployment of protections, cyber insurance, and information sharing of economic impacts. Details of the implementation of each one of the solutions proposed to be part of the *CyberTEA* are also provided in Chapter 4. This highlights technologies, implementation, code examples, and technical decisions for implementing the solutions proposed and designed beforehand.

After that, **Chapter 5** shows extensive quantitative and qualitative evaluations for each one of these solutions, including a case study that show evidence of the benefits and feasibility of the methodology, framework, and solutions during the planning of a cybersecurity strategy. These results are supported by specific sections, with discussions of all findings, challenges, and limitations identified during the development of this PhD thesis and based on the evaluations conducted.

Finally, **Chapter 6** concludes this PhD thesis by providing a summary, revisiting the RQs detailed in Section 1.2, and presenting suggestions regarding future research work.

Knowledge, like air, is vital to life. Like air, no one should be denied it.

Alan Moore

2

Theoretical Foundations

THIS chapter focuses on the convey the different concepts, information, and facts required to motivate and understand this PhD thesis. Thus, this chapter introduces SMEs' most important threats and risks, highlighting their technical, societal, and economic impacts. Also, the concepts of cybersecurity economics are presented, and its nuances are explained to show how the intersection between cybersecurity and the economy can be used for the different decisions during cybersecurity planning and investments. Furthermore, the cybersecurity strategies and investments of both Small- and Medium-size Enterprises (SME) and Multi-National Enterprises (MNE) are discussed regarding their main differences and the challenges for the different sectors. Finally, the concepts of blockchains and Smart Contracts (SC) are provided, since it is used as an enabler for trust and automation for some of the solutions proposed in this PhD thesis.

In addition, it is essential to state that the terminology used for this PhD thesis is defined based on standards, literature, and concepts from the scientific community, industry, and standardization agencies. Important concepts used during the development of this thesis, such as the definition used for terms like approach, methodology, framework, solution, and cybersecurity strategy, are defined in the Glossary (*cf.* Appendix E). Also, Section 2.5 discusses the differences between terminologies

used in the business and computer science fields. It is important for a clear understanding of the scenario and thesis' contributions, more specifically for Chapter 4.

2.1 Cybersecurity Threats, Risks, and its Impacts

In order to understand all of the nuances that involve cybersecurity strategies, it is essential to know what threats are targeting companies and which are possible direct and indirect impacts. This section describes the current scenario of threats and their classifications, highlighting the most frequent and dangerous ones for SMEs. Also, the likelihood of a specific threat is explained, and the different factors that make a company more vulnerable to cyberattacks are discussed.

2.1.1 Threat Landscape

Cybersecurity can impact every Information and Communication Technology (ICT) domain. This means that different solutions have to be considered and implemented considering different domains (*e.g.*, User-, Network-, and Device-Centric security), which are defined considering different levels of abstractions, characteristics, and threats targeting them. These domains, based on the review of cybersecurity threat analysis literature [15, 18, 67], are summarized in Figure 2.1.

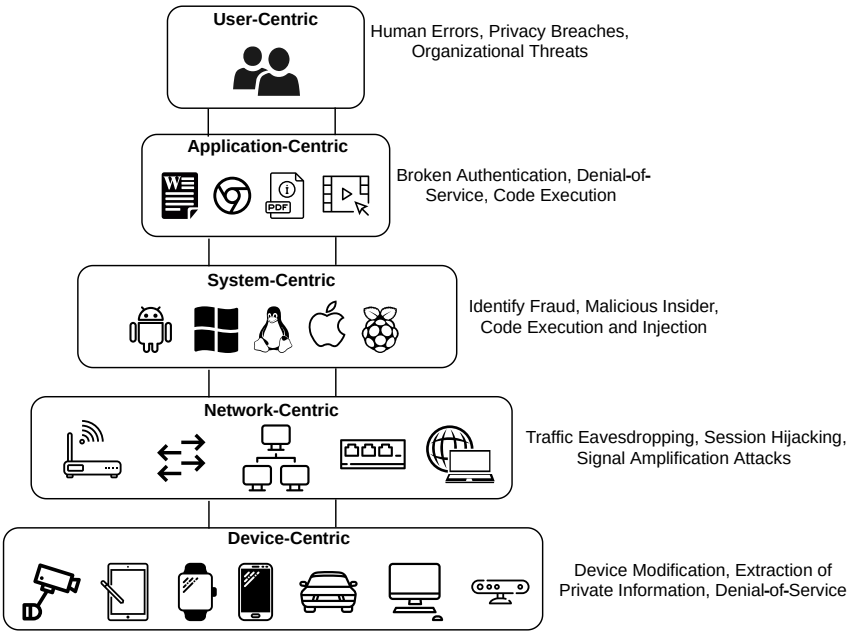


Figure 2.1: Cybersecurity Domains based on [15, 18]

User-Centric Security

The first domain considered is the *User-Centric* security, which focuses on humans as the central actor that operates ICT systems. For this domain, users have to be considered as the main target of cyberattacks, such as disinformation attacks and phishing campaigns [73]. Therefore, protections have to be defined to reduce the risks of exploring one of the most significant vulnerabilities for an ICT: the human that operate and manage the systems.

The common threats of this domain are those targeting the lack of training and cybersecurity expertise inside a company, also amplified by humans' good faith. For example, human errors when using a system, managing a network, handling physical assets (*e.g.*, laptops and pen drives), or even reading e-mails can become a door to devastating attacks. One of the most frequent cases is when attackers apply social engineering techniques combined with phishing attacks to spread malware that might affect the security and privacy of the companies' services and customers. Also, access privileges are often misused, and credentials are poorly managed. This becomes key for this domain, since malicious insiders in a company (*e.g.*, employees unsatisfied or spies) can access systems and data they do not need to. Even legit employees can have their good faith exploited by attackers to reveal sensitive information or access systems.

Application-Centric Security

In the second level of this classification, there is the *Application-Centric* domain. The threats in this domain focus on the applications being used for different purposes on top of host systems. Examples of these applications include Internet browsers, document readers and writers, video and audio players, and specific applications developed to solve the demands of a company (*e.g.*, logistics, customer database, and payment processes). Cyberattacks can then explore vulnerabilities, failures in configurations, or misuse of applications to obtain illegal benefits and information regarding the users, the systems, and the company.

Examples of attacks in this domain are those based on exploits scripts (*i.e.*, scripts with specific automated instructions to explore a particular vulnerability) that explore the weakness of an application and take advantage to compromise the Confidentiality, Integrity, and Availability (CIA) triad of a resource or system. These cyberattacks include rootkits, Structured Query Language (SQL) injections, and buffer overflow, resulting in broken authentication, Denial-of-Service (DoS), and arbitrary code execution.

Protections for this domain have to monitor and analyze vulnerable applications to cyberattacks. To avoid most cyberattacks in this domain, companies can focus on good security practices during

the development of the tools (*e.g.*, Security-by-Design and Security-by-Default) [138], an adequate risk assessment and training before the application in the company environment, and applying update patches ever then available. Still, this domain is one of the most dangerous, since applications emerge every day for different purposes and with many features that companies might adopt due to its benefits, thus creating a dynamic and complex scenario from the cybersecurity perspective.

System-Centric Security

The *System-Centric* domain shows measurable similarities with the application-related one, since it focuses on the underlying systems, which can be affected by or affect the application domain. However, cyberattacks can result in a malicious attacker's total control of the environment in this domain. Systems in this domain's context are used as a synonym for Operating Systems (OS) or, in a more general way, described as software that allows applications to use the computation capabilities of the hardware (*e.g.*, connectivity, processing, and storage).

Threats in this domain can also be related to virtual environments, such as those relying on cloud computing and virtualization techniques to support the usage of applications by the users. Besides traditional OSes, like Microsoft Windows, Apple iOS, and Linux, there has been a trend in the last years of companies migrating their services to cloud environments [12, 208], thus, relying on their data, communications, and consequently, their businesses on public and private clouds (*e.g.*, based on Openstack, Cloudstack, and Kubernetes) [34, 80].

Considering the importance of the system's domain, it is crucial, when conducting the cybersecurity planning, to understand all elements involved to avoid negative impacts due to cyberattacks on companies. Cyberattacks can result in information leakage or loss due to problems in cloud servers or backup incidents. Also, the inadequate design and planning of cloud-based systems can result in security problems for the companies. Besides malicious code and threats already discussed, this domain can be a target for Distributed Denial-of-Service (DDoS) attacks to affect the availability of the systems and, consequently, affect other domains. DDoS attacks, in summary, try to exhaust the resources of systems (*e.g.*, processing capacity, memory available, and network bandwidth) to cause performance decrease, loss of data, and service interruption.

Network-Centric Security

The fourth domain on *Network-Centric* covers communications of companies happen in both inside and outside directions. Many different devices (*e.g.*, Hubs, Switches, and Routers) establish and handle communications between devices, systems, and applications in this domain. Also, although Local

Area Networks (LAN) are desired for internal communication, the communication with the external world depends on the Internet's underlying infrastructure, which is composed of variations of these types of devices. So, a network composed of trustworthy systems without backdoors is desirable to prevent malicious attackers from obtaining, extracting, and processing information related to the companies' communications.

The threats on the Network-Centric domain involve, for example, *(i)* traffic eavesdropping, where malicious users can collect and analyze the communications between two points, *(ii)* session hijacking, which is a method of taking over a session by pretending to be an authorized user using his/her session ID, and *(iii)* signal amplification attacks, which allows for attackers to receive transmitted signals and copy it for malicious usage (*e.g.*, eavesdropping and unlock assets protected by radio-frequency transmitters). Therefore, protections in this domain have to consider sensitive information shared during communications, including the information used by the different layers that compose the Open Systems Interconnection (OSI) model and its adjacent protocols (*e.g.*, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Domain Name System (DNS)). These protocols are part of the core of what we know as Internet and LANs today, being used for many purposes, such as authentication, data transfer, and interactions with fetching resources.

A commom protection mechanism for this domain is the usage of encryption schemes like the Secure Sockets Layer (SSL), which can provide a certain level of confidentiality and integrity in communication using the HTTP protocol. Also, a suitable configuration of network devices is required to avoid weak credentials, reduce risks related to network services like DNS poisoning, and also better physical security has to be considered (*e.g.*, malicious users that have access to network devices might be able to be part of the network as a legit and trustworthy user).

Device-Centric Security

Lastly, the *Device-Centric* domain comprises all hardware in use, running systems, and users applications. These devices can have different sensors to process external information to be used during decision processes, such as in the case of IoT devices. In this domain, one fundamental aspect is to ensure the integrity of devices, which defines that the device's behavior is precisely what it was supposed to be and not tampered with by malicious attackers.

Different techniques can be used, for example, for identifying behavioral fingerprints of these devices [203] to monitor misbehavior. Still, mechanisms that protect devices against different attacks are required. In case of extraction of private information, encryption schemes can be deployed. Also, protection against physical attacks can be placed to avoid the access of malicious users to critical components or features of a device. Suppose someone has direct access to key components of a device

(*e.g.*, interfaces, circuits, or storage chips). In that case, it might cause data leakage or even a DoS run against devices, which results in a disruption of the entire chain that relies on the device to operate (*i.e.*, users, applications, systems, and networks).

Common Threats for SMEs

Based on these discussed domains, many different threats can impact businesses. Today, there are specific sectors that have been the target of specific threats, and also, there are threats more common than others. For example, businesses that handle more critical services and information (*e.g.*, hospitals, universities, and finance) tend to be more targeted by ransomware attacks, which encrypts the data to make all systems unavailable. Due to the critical services and challenges of recovering from an attack (which need days or even weeks), these businesses tend to pay for the rescue asked for the attackers [202].

Although there are businesses more prone to specific attacks, in general, attackers tend not to spend too much time focusing on one specific business but on exploring vulnerabilities in any IT infrastructure and business characteristics they see as potential weaknesses. This happens in the case of SMEs, which are the focus of general attacks (*i.e.*, not tailored for a specific company), because attackers know most of SMEs lack training, expertise, and budget for cybersecurity.

Table 2.1 summarizes the most common threats reported by the 249 SMEs interviewed during the survey conducted by ENISA in Europe in 2021 [70]. As highlighted in the table, the most common threat is phishing, in which 41% of the interviewed SMEs had at least one attack of this kind in the year 2020. It is followed by Web-based attacks and general malware, which 40% and 39% of the SMEs reported being a target.

Phishing is one of the main doors for other attacks. Many phishing campaigns focus on SMEs' employees to steal credentials or execute malicious code in the company infrastructure. One of most common factors that increase the chance of success of these attacks is companies' lack of knowledge and training about this kind of cyberattack. Thus, it is possible to affirm that phishing attacks are directly related to the education of employees and factors that involve human behaviors that can be mitigated with adequate training [7].

Also, massive Web-based attacks are conducted by attackers in order to find and explore vulnerabilities as much as possible. Then, in case of success, these attacks reveal sensitive information or even give access to companies' servers. Besides that, malware are one of the dangerous threats, since it can have many different forms, purposes, and actions. One of the most well-known examples is the case of ransomware. Nevertheless, also there are, for example, malware implemented to infect computers to give control to attackers to create a network of bots to execute attacks against others

(*i.e.*, botnet for distributed attacks) [97]. In the case of SMEs, malicious insiders are not expected due to the company's nature. These attacks are more frequent in huge enterprises with unsatisfied employees and infiltrated attackers. Other companies of governments frequently fund malicious insiders, and they use techniques of social engineering to obtain sensitive information (*e.g.*, customer database, finance information, or industrial patents) that can be used in favor of the concurrence or against the company itself.

Table 2.1: Summary of the Most Common Threats for European's SMEs According to the Survey Conducted by ENISA [70] within 249 SMEs from 25 European Member States

Threat	Description	Domain	Reported SMEs
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information	User-Centric	41%
Web-based Attack	Exploit of vulnerabilities in code or features of Web sites to gain access to a server or sensitive information	Application-Centric	40%
Malware	Malicious code that explores vulnerabilities of systems to compromise their functions or act in the benefit of the attacker	Application and System-Centric	39%
Malicious Insider	Legit employees and users that use their access to act maliciously against the company (*e.g.*, steal information or sabotage)	User-Centric	19%
Denial-of-Service	Interrupt the service or operation of a business by overloading its computer resources with malicious usage	Application, System, and Network-Centric	12%
Social Engineering	Set of techniques to manipulate people to obtain benefits, steal sensitive information, and access critical resources of a company (*e.g.*, buildings, devices, and servers	User-Centric	11%
Compromised/Stolen Device	Theft of unencrypted devices or usage of infected devices by legit employees in the company's systems	Device-Centric	7%

Lastly, DoS attacks is one of the most devastating threats, especially in its Distributed form (*i.e.*, DDoS) [157]. However, this threat tends to be very customized and targeted to specific companies. Thus, although this is an issue of concern for SMEs, it is not the most frequent attack on these companies. If a DDoS attack targets a company, it will likely cause an interruption in systems, Web sites, and communications, thus, directly affecting the services provided or used by a company.

Besides understanding the threat landscape and the different kinds of attacks affecting the companies, it is also important to understand the likelihood of these threats and their possible impacts. Thus, the rest of this section will discuss the risks and impacts of cyberattacks on SMEs.

2.1.2 Risk Definition and Management

The term *risk* is generally used to indicate a possibility of loss and/or damage. It usually involves some degree of uncertainty, and the resulting outcome is challenging to predict. Depending on the context, various types of risk can be found, such as business risk, economic risk, and safety risk [136]. On a quantitative level, a general risk (R) can be further expressed as a triplet $R =< s, p, c >$.

This quantitative definition indicates that a risk (R) is generally a combination of a scenario (s), *i.e.*, what can go wrong, the probability (p) it will have, and the severity of impacts (c), *i.e.*, amount of damage caused. In the field of Information Technology (IT), a risk, also called cyber risk, is usually described as a situation or configuration that can expose the system's vulnerability, causing, for example, economic and reputation losses. A threat, in this case, can be represented by cyberattacks that might explore a given risk or vulnerability, such as ransomware and phishing. In a study, Aven and Krohn [23] proposed an informal model about risk in general by extending the definition with a knowledge dimension (k). More specifically, in different scenarios with equal probability, knowledge has been an important factor in supporting the decision-making process, such as in the case of SMEs and their particularities.

Risk assessment is the necessary process of identifying, analyzing, and evaluating risks from different perspectives. In the context of cybersecurity, the assessment process focuses on cyber risks and the likelihood of threats. Risk assessment is a key stage of the entire risk management lifecycle, and, in practice, it includes three main tasks: risk identification, analysis, and evaluation. Figure 2.2 provides an overview of a general risk management framework, highlighting the different steps involved in risk management and assessment.

In essence, risk management is an ongoing process of assessing, treating, and monitoring risks. In the first phase, the scope for the entire risk management process and the criteria against which the risks will be assessed are set. Afterward, the assessment phase is initiated. This stage involves identifying possible risks followed by comprehensive analysis and evaluation. It is important to note that putting insufficient effort in the first stage of the risk assessment process may cause potential risks to be omitted from further analysis, resulting in unpredictable outcomes. After being prioritized, risks are treated based on their type, nature, and priority. However, developing a good and effective treatment plan has proven difficult. In such cases, having an extensive collection of past projects and the corresponding risk history can help develop more proactive treatment strategies.

Lastly, an effective risk management strategy involves regular monitoring and surveillance for potential threats. Results should then be recorded, reported internally (*e.g.*, team and board members), externally (*i.e.*, stakeholders), and reviewed.

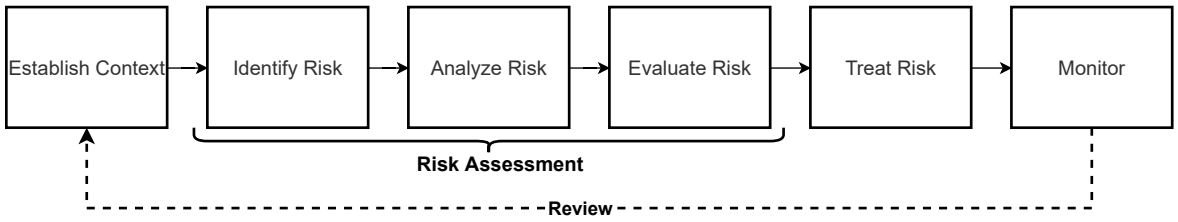


Figure 2.2: Overview of the General Steps Considered by Risk Management Frameworks

Institutions also propose different frameworks to support risk management. These frameworks differ in the different steps required, such as the ISO 27005, ENISA ISMS, and NIST CSF [102]. One of the biggest obstacles SMEs face is the deficiency of necessary resources for implementing this kind of framework. However, independent of the nuances of each framework, the *risk* can be described singly and straightforwardly, as presented in Equation 2.1.

$$Risk = Impact \times Likelihood \tag{2.1}$$

In this straightforward risk formula (*i.e.*, Equation 2.1), the *Impact* means the size (*e.g.*, financial loss due to business disruption and indirect costs) of a cybersecurity incident resulting in a company (in both quantitative and qualitative way), and the *Likelihood* is how likely is the event (*i.e.*, threat) to happen based on the company's profile and previous observations (*e.g.*, sector, past attacks history, and known vulnerabilities). Thus, risk can be defined as the probability of direct or indirect impacts (*e.g.*, financial loss, damage to an organization's reputation, or business disruption) resulting from the failure of companies' information technology systems due to a malicious attacker. The *Impact* and *Likelihood* increase according to the company's dependency on technology, since more attack vectors are possible, more vulnerabilities are introduced, and more worthy and feasible for cybercriminals.

In order to determine a risk, each underlying system of a company (*e.g.*, databases, softwares, and controls) requires an analysis of its potential security/safety threats and measures to respond to these threats. Figure 2.3 summarizes the different relationships and aspects, from a more technical to economic level, to analyze within the company ecosystem. A rational approach to defining an adequate cybersecurity strategy includes the *(i)* identification of risks by examining potential vulnerabilities and their chances of successful exploitation, *(ii)* cost (both direct and indirect) involved if vulnerabilities are exploited, and *(iii)* cost of mitigating vulnerabilities. The risk analysis is the fundamental stage toward mapping costs associated with cybersecurity incidents. It is used then for determin-

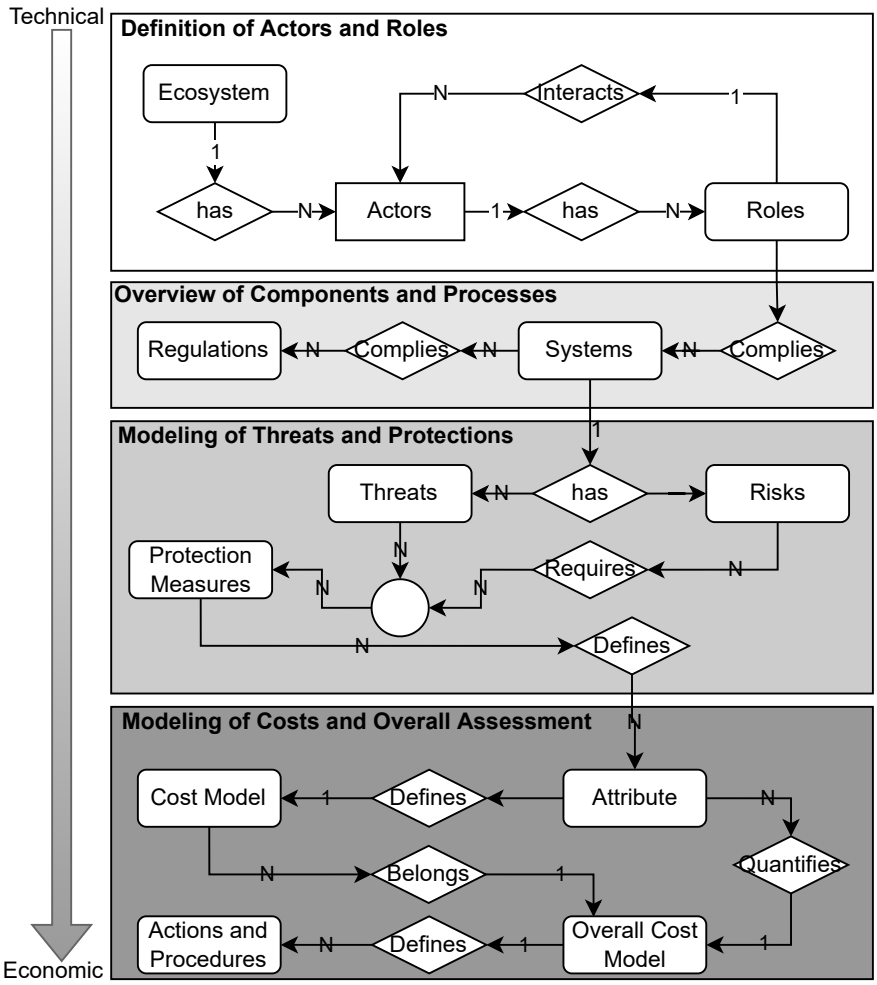


Figure 2.3: Entity-Relation Model for Risk Assessment from an Economic Perspective

ing, proactively or reactively, possible solutions/measures that will compose a cybersecurity strategy against the mapped vulnerabilities/threats that may occur according to their likelihood.

2.1.3 Impacts of Cyberattacks

Figure 2.4 provides an overview of the different impact domains of a cyberattack on companies. First, the *Economic* domain involves all direct and indirect costs related to a cyberattack. As financial loss is one of the major concerns of companies as of today [200], the focus of cybersecurity campaigns can use this as a powerful argument for why care about cybersecurity. Next, there are *Legal* impacts of cyberattacks, which move the cybersecurity cases to the legal sphere, regulations, and governance

aspects. Also, the legal sphere can directly impact economic factors, since the collateral effects are costs with lawyers, compliance, and penalty fees applied by regulatory bodies.

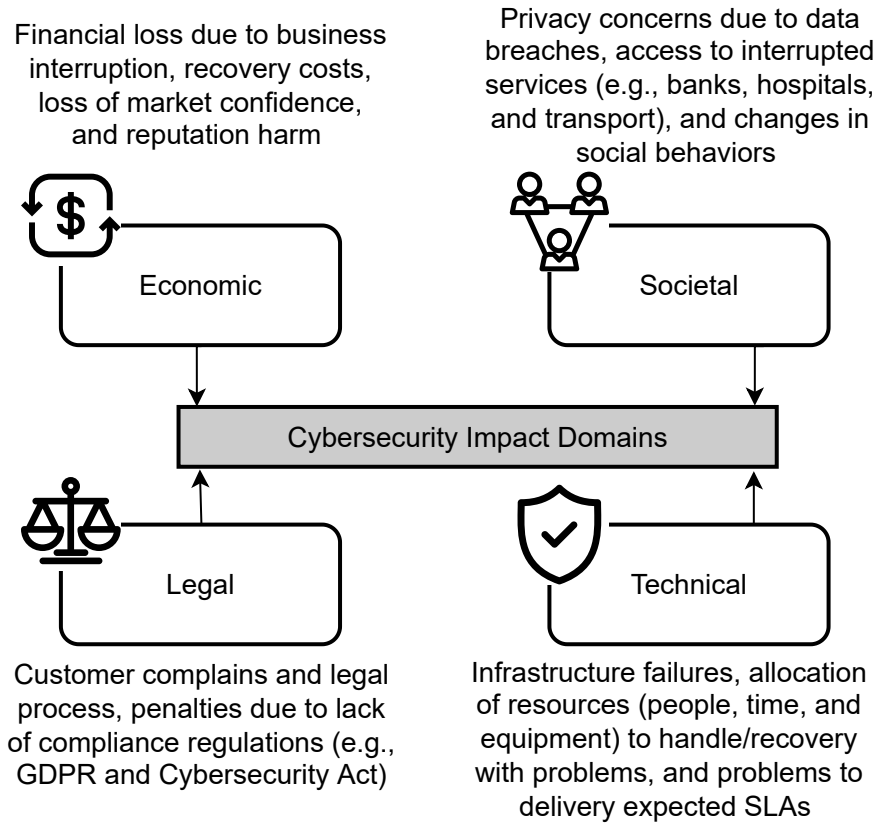


Figure 2.4: Overview of the Different Domains of Impacts due to Cybersecurity Incidents

Furthermore, there are different *Societal* impacts, since cyberattacks interfere directly with the life of people and social structures. For example, cyberattacks can be responsible for a crash in the health system of a country like in the case of the National Health System of United Kingdom [165] or affect the lives of people by interrupting critical services like food supply [188] and critical infrastructure of countries [129]. Besides that, the high number of cyberattacks that explore the good faith of humans (*e.g.*, social engineering techniques and different types of phishing) impacts changing social behaviors, which makes people much more afraid even when they are facing legit interactions [181].

Lastly, *Technical* impacts are the precursor of all of the other impacts mentioned before, since economic, legal, and societal impacts come only because the company was not technically able to avoid or mitigate the attack in total. One can say that focusing only on technical aspects can be the right decision. However, this is a naïve view, since cybersecurity is a dynamic and complex world in which

cyberattacks evolve every day, and achieving utmost protection is almost impossible. Therefore, it is essential to look at cybersecurity from its different potential impacts, measuring them and making decisions to avoid as much as possible the impacts that might cause more problems for companies.

Regarding the different costs of cyberattacks, in 2020, a data breach costs to MNEs, on average, US$ 1.09 million, compared to US$ 1.41 million in 2019, while SMEs had to pay on average US$ 101,000, compared to US$ 108,000 in 2019 [109]. A business can reduce the cost of data breaches in different ways. For example, a quick breach detection can lower the loss by 32% in MNEs and by 17% in SMEs due to savings in direct and indirect costs. Also, a proactive disclosure to customers and stakeholders that a data breach has happened can lower the financial damage by 28% in MNEs and by 40% in SMEs.

Another factor in reducing the costs of cyberattacks is up-to-date software and hardware. Suppose an efficient strategy for updating critical elements within a company is not placed. In that case, it can increase the cost related to cyberattacks by 47% in MNEs and by 54% in SMEs [109]. In the case of ransomware affecting a company, the average costs for remediation are US$ 761,106 in 2021 [202], which include costs to mitigate, recovery, and business disruption due to attacks. Payments directly to the criminals are becoming more frequent to recover the data, which payments go from a few thousand to millions of dollars depending on the company's size. The average in 2021 was US$ 233,817 paid per attacked company for cybercriminals. The costs also are very high from a societal and governmental level, which makes the United States governments push in the fight against ransomware gangs, including, in 2021, putting a US$ 10 million reward for information that helps to catch a ransomware gang named DarkSide [27].

The predictions regarding costs say that worldwide cybercrime costs will hit US$ 6 trillion annually by 2021, with US$ 20 billion being only for ransomware attacks [200]. Besides the costs of cyberattacks, there are also many costs related to fines imposed by governments and entities for companies that do not follow cybersecurity regulations. For example, from July 2018 to November 2021, the General Data Protection Regulation (GDPR) resulted in 837 fines in Europe [46], with a total sum of € 1.2 billion in penalties. The most common type of violation was the insufficient legal basis for data processing (299 fines), insufficient technical and organizational measures to ensure information security (179), and non-compliance with general data processing principles (178 fines).

2.2 Cybersecurity Economics

This section provides an introduction to cybersecurity through the lens of economic principles. Thus, this section gives an overview of the concepts of cybersecurity economics, including examples of well-known metrics used for cost analysis and investments in cybersecurity are presented and discussed.

2.2.1 Overview and Principles of Cybersecurity Economics

The cybersecurity field is a thriving and fast-moving field that covers many aspects (*e.g.*, technical, legal, societal, and economic) from different perspectives (*cf.* Section 2.1.1). Cybersecurity economics is one of its sub-fields, which can be described as the intersection between cybersecurity and economics that investigates cyberattacks, strategies, and protections with an economic optic. Therefore, focusing on understanding, measuring, and reducing the potential effects of cyberattacks on companies' financial health while also helping to find the optimum amount of investments required for an adequate level of protection (*i.e.*, a cybersecurity strategy that fits the needs of a company with the minimum budget possible).

Although discussion on economic impacts of technology started a long time ago, cybersecurity economics as we know it today has its start at the beginning of the 21st century. Figure 2.5 shows a timeline of the evolution of cybersecurity economics and the rising of the most well-known models used today. In 1990, the discussions on economic impacts of Internet security started [111], with a focus on the growing role of the Internet in the world economy.

Still, in the 90s, [13] presented and discussed the results of a survey of failures in banking systems, thus, showing that most frauds were caused due to implementation errors and management failures. This survey contributed to the paradigm-shifting in cybersecurity (*i.e.*, instead of worrying about what might go wrong, focus on a systematic study to identify what is likely to happen) and discussed the potential economic impacts of cyberattacks in the years to come.

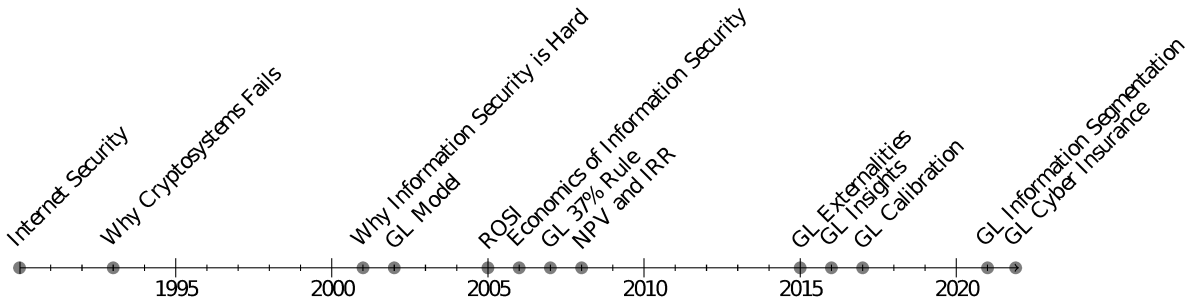


Figure 2.5: Timeline of the Evolution of Cybersecurity Economic Discussions and Models

At the beginning of the 21st century, the main discussions and models for cybersecurity economics rose. [14] argued that the information insecurity is at least as much due to perverse incentives. Therefore, many cybersecurity problems could be explained using microeconomics concepts, such as network externalities, asymmetric information, and moral hazard. One year later, in 2002, the Gordon-Loeb (GL) model [103] was proposed as an economic model that determines the optimal amount to invest in protecting a given set of information.

After a few years, the Return On Security Investment (ROSI) model [239] was introduced in 2005 to be used as a benchmark methodology to support cybersecurity decisions by performing a cost-benefit analysis of protections. These two models are the most used today, but with different refinements available, especially for the GL model. [4] provided an insightful discussion regarding the advances and challenges of cybersecurity economics, highlighting that cybersecurity economics goes into more general areas, such as system designs, legal aspects, and privacy concerns.

Examples of other metrics applied within the context of cybersecurity economics are the Net Present Value (NPV) and the Internal Rate of Return (IRR). Both are used for general economics calculations and applied in the business world to understand the potential financial return of an investment or project. It was shown in [187] that both NPV and IRR could be used for strategic decisions for cybersecurity economics. According to a survey conducted in 2010 among corporate information security managers [30] in the United States, ROSI was being used by 44% of the participants, while NPV and IRR were used by 26% and 23% respectively. Also, different frameworks have been investigating ways to measure economic impacts of cybersecurity along the years, such as the SEConomy [197] proposed in 2019 as a step-based framework to measure economic impact of cybersecurity activities in a distributed ecosystem with several actors.

The GL model, after its introduction, was the topic of discussion, and different researchers tried to provide proof to invalidate the model. However, [247] provided strong proof that the 37% rule stated by the GL model (*i.e.*, investments in cybersecurity should never exceed 37% of the potential

loss) is valid. The GL model's refinements and different applications have become more common since 2015, with the original authors of the GL model providing interesting new work regarding the model.

In [104], Gordon and Loeb extended the GL model to consider externalities (*i.e.*, costs for third-parties) within the model. [105], published in 2016, Gordon and Loeb also provided an insightful review of all findings and observations since the first release of the GL model in 2002. [163] is another exciting work proposed to help companies to calibrate the GL model parameters according to the needs and reality of the company. Finally, in 2021, Gordon and Loeb extended the GL model again to support the concept of information segmentation within companies [144]. Also, [112] proposed in 2021 that the use of the GL model can support the calculation of premiums and risks for the cyber field insurance. This work is an example of how the GL model evolves with different applications and scenarios.

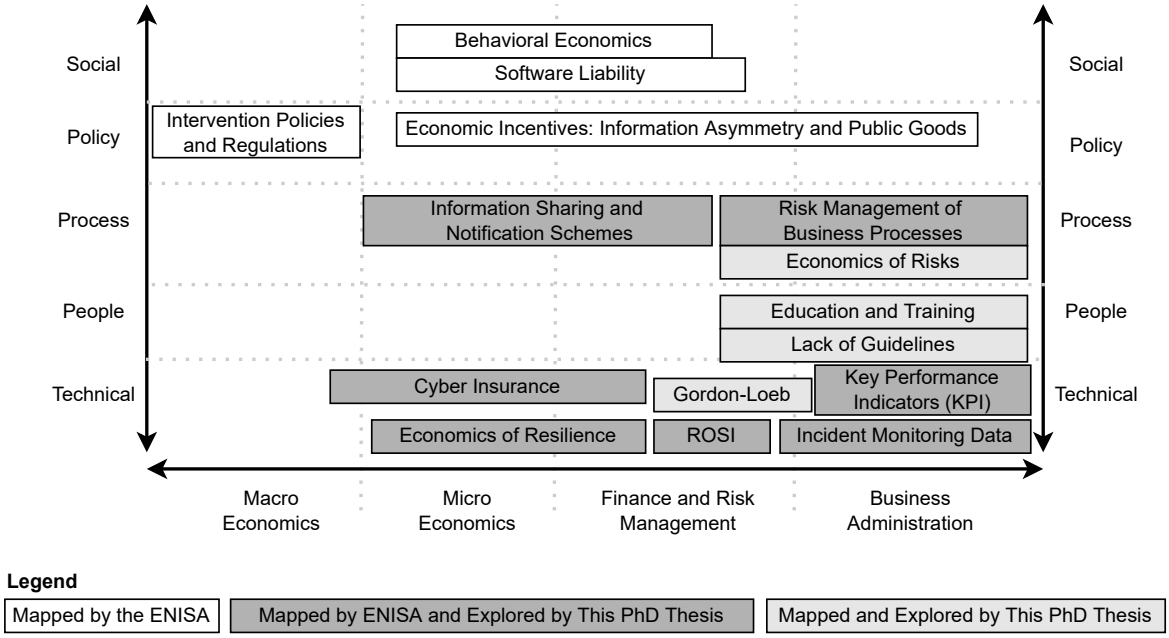


Figure 2.6: Overview of the Relevant Topics Related to the Fields of Cybersecurity and Economy Identified by ENISA [64] and During the Development of this PhD Thesis

Over the last years, many discussions regarding the economic role and dimensions of cybersecurity have been happening in Europe [64, 85]. Figure 2.6 highlights those main topics of cybersecurity economics for Europe, organized from research to technical contexts and from its place in the economic field (*i.e.*, from Macro Economics to the Business Administration). This figure is based on the

Working Group investigation established by ENISA to study the priority topics related to Cybersecurity Economics [64] and extended with the knowledge obtained during this PhD thesis.

The X-axis shows different economic areas. On one hand, the closer to the Macro Economics area, the stronger its relationship is to the theoretical economic field. On the other hand, the closer to the Business Administration area, the stronger its relationship with specific business practices applications. The context of the different topics is represented by the Y-axis. The closer a topic to Policy, the greater its relevance to political decision-making (*e.g.*, regulations and state-sponsored actions). The closer a topic to the Technical topic, the more it can be addressed by using existing (or possibly to be developed) technical approaches.

In Figure 2.6, the topics identified initially by ENISA but not explored by this PhD thesis are highlighted in white. The dark gray highlights those the topics covered by this PhD thesis, and that were mapped previously by ENISA in [64]. Finally, the additional topics mapped and covered by this PhD thesis are highlighted in light gray.

At the process level, one topic considered is *Information Sharing*. This is related to the information sharing between partners to create a trusted community that can plan and mitigate cyberattacks based on the experience of others. Also, the *Economic of Risks* focuses on understanding the economic impacts if a threat happens. In the same direction, the *Risk Management of Business Processes* helps to map risks within a company and helps to apply mitigation measures to optimize cybersecurity (in terms of costs and performance) and reduce potential economic impacts on the business.

Next, two topics focusing on people were identified as relevant: *(i)* Education and Training and *(ii)* Lack of Guidelines. For *(i)* it is clear the impact of the misinformation and lack of expertise in companies. Therefore, this is one of the pillars for an efficient cybersecurity strategy in the short- and medium-term. Also, *(ii)* means that standardization, frameworks, and clear guidelines have to be placed to help decision-makers decide about the cybersecurity required for a business.

There are different topics to consider at the technical level in the context of cybersecurity economics. *Cyber Insurance (CI)* is one of them, since it helps companies reduce their possible economic impacts by contracting insurance for specific coverage against cyberattacks. This topic impacts the microeconomics level primarily due to the economic nature of the insurance market to benefit individuals (*i.e.*, companies). Thus, it helps avoid financial loss, while reducing a business's risks (from an economic perspective). CI can also impact the overall economy of a country. Therefore, it also relates to the the macroeconomics field.

Also, from a microeconomics view, the *Economics of Resilience* has the role of understanding how companies can invest and develop strategies to mitigate and recover from cyberattacks. *Key Performance Indicators (KPI)* and the *Monitoring and Processing of Incident Data* also have a relevant role in

cybersecurity economics, since it gives quantitative data for better analysis and understanding of the behaviors and impacts of cyberattacks.

Finally, two well-known cybersecurity economics metrics are the ROSI and GL model and ROSI, as introduced earlier in this section. Over the years, different models have been proposed to guide investment in cybersecurity, but there is still no generally accepted model. An explanation for this open issue is the need for sufficient data and accurate risk assessment that can be used as input for quantitative and qualitative analysis of economic impacts in companies. Among the models available for cybersecurity economics, two are the most well-accepted and prominent: GL and ROSI.

2.2.2 Gordon-Loeb (GL) Model

The GL model is an economic model used to analyze the optimal investment level in cybersecurity. The model was proposed in 2002 by Gordon and Loeb [103] and takes into account the vulnerability of a system and also the potential financial loss due to a cyberattack. One of the ideas behind the model is that a company should not necessarily invest in mitigating threats in more vulnerable systems. Besides that, a company should focus its efforts on systems with a medium level of vulnerabilities (not on the extreme cases), which is realistic to mitigate risks without substantial financial investments. Also, the analysis conducted by the authors of the model suggests that only a tiny percentage of an expected financial loss due to a cyberattack has to be spent on cybersecurity. Thus, GL provides an economic analysis that provides insights for investment in cybersecurity, but it is still clear that it is not a trivial task, since different elements have to be considered for a precise analysis, such as technical aspects, cyberattacks behaviors, and specific business configurations (*e.g.*, sector, maturity, employees, and IT infrastructure).

Figure 2.7 shows, based on the investigation conducted in [103], that after a certain threshold, the investments in cybersecurity start to be not worthwhile if compared with the expected loss in case no investments are made. An optimal investment is where the difference between benefits and costs, *i.e.*, the Expected Net Benefit of Investment in Information Security (ENBIS), is maximized. Therefore, an investment starts to become good when ENBIS > 0 and the optimal amount invested in cybersecurity is the maximum *ENBIS* for a given security breach probability function.

The ENBIS is calculated in relation to the Expected Benefit of Investment in Information Security (EBIS) and the amount invested. The EBIS is defined as the reduction in the company's expected

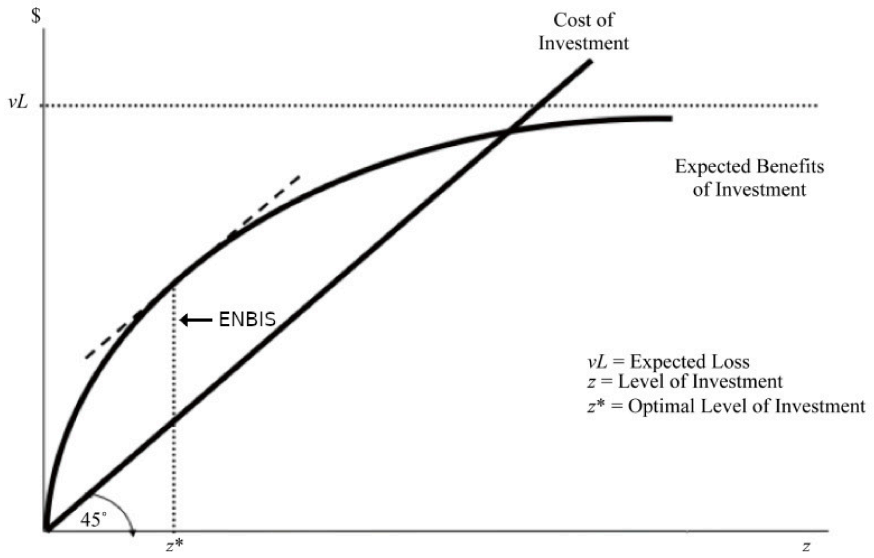


Figure 2.7: Level of Investment in Cybersecurity [105]

loss because of the additional investment made in cybersecurity, which can be described as provided in Equation 2.2.

$$EBIS(z) = [v - S(z, v)]L \tag{2.2}$$

Then, the ENBIS can be calculated as the net benefit of the investment made in cybersecurity, which means reducing the expected loss minus the amount invested in cybersecurity. Thus, the ENBIS calculation is shown in Equation 2.3.

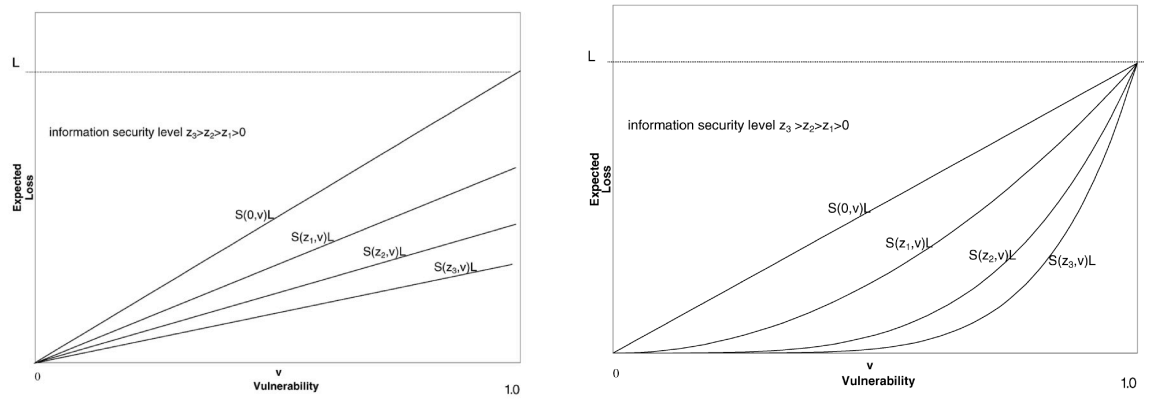
$$ENBIS(z) = EBIS - z \tag{2.3}$$

A security breach probability function is defined as $S(z, v)$, which denotes the probability of a system with a vulnerability v being breached, given that the company has made a cybersecurity investment of z. There are two measures used for the productivity of cybersecurity. These measures are determined as $a > 0$ and $\beta \geq 1$.

[103] defines two different security breach classes (*i.e.*, definitions for $S(z, v)$) to show the performance of the GL model to estimate the optimal investment in cybersecurity. For that, three assumptions (A) are made also in [103], which the two classes have to satisfy:

- **A1.** If $v = 0$ (*i.e.*, invulnerable), then the system will remain fully protected doesn't matter how much investment (z) in security is made, including $z = 0$

- **A2.** if $z = 0$ (*i.e.*, no investment in security), the probability of a security incident is inherent to the value of v
- **A3.** As much the investment increases, more secure is the system. However, it happens in a decreasing rate. It also implies that there is not sufficient amount of investment that can make a vulnerable (*i.e.*, $v > 0$) system become perfectly secure ($v = 0$)



(a) Class 1 **(b)** Class 2

Figure 2.8: Expected Value of Financial Loss as Vulnerability Increases at Different Amount of Cybersecurity Investments for Two Classes of Security Breach Probability Functions Defined by [103]

The purpose of a cybersecurity investment is to lower the probability that a system within the company will have a financial loss. Thus, the GL model is proven valid using the two classes of security breach probability functions. The first class (*cf.* Figure 2.8 (a)) refers to a linear vulnerability. The security breach probability function $S(z, v)$ for Class 1 is determined by Equation 2.4. The optimal investment for Class 1 (z^*_{class1}) is calculated according to Equation 2.5.

The second analyzed class (*cf.* Figure 2.8 (b)) is concave (*i.e.*, the slope of the graph line increases gradually from left to right). Equation 2.6 provides the security breach probability calculation for the Class 2. The optimal investment (z^*_{class2}) for this class can be calculated using Equation 2.7. It is important to note that, based on the analysis conducted, the optimal investment in cybersecurity is always $\leq \frac{1}{e}$, where e is the Euler's constant (*i.e.*, ≈ 2.71828). This means that the optimal investment is always $\leq 37\%$ of the expected loss (vL) without investments.

$$S_{class1}(z, v) = \frac{v}{(a \times z + 1)^{\beta}} \tag{2.4}$$

$$z^*_{class_1} = \frac{(a \times \beta \times v \times L)^{\left(\frac{1}{\beta+1}\right)} - 1}{a} \tag{2.5}$$

$$S_{class_2}(z, v) = v^{a \times z + 1} \tag{2.6}$$

$$z^*_{class_2} = \frac{\ln \frac{1}{-a \times v \times L \times (\ln v)}}{a \times \ln v} \tag{2.7}$$

In summary, GL determines, in a general way, that the maximum investment (z_{max}) in cybersecurity should not exceed 37% of the expected loss (vL) for all functions part of the classes investigated by [103]. It relates to how much the system is valued (λ), how much the data/system is at risk (t), and the probability that an attack on the data/system is going to be successful (v). Equation 2.8 describes how to use this information for the calculation.

$$\begin{aligned} vL &= \lambda \times t \times v \\ z_{max} &= vL \times 0.37 \end{aligned} \tag{2.8}$$

However, although this defines the maximum amount, it does not determine the optimal investment. In order to calculate the optimal amount, it is needed to use the productivity of a cybersecurity investment, which may vary for different scenarios, depending on specific concerns surrounding a particular set. Another finding from the GL model is that the amount of investment does not always increase based on the level of vulnerability [105]. For example, a company can focus more on protecting a system with a medium level of vulnerability than one with a high level of vulnerability. This is a consequence of the productivity of incremental investments in cybersecurity, which means that a given $S(z, v)$ can determine that after or before a certain threshold of vulnerability, investments are not efficient (*e.g.*, it will not reduce the chance of a system being attacked or breached).

In another work, [130] provided a counterexample for the GL model by constructing a scenario where an investment up to 50% can be needed. However, [247] shows that the 37% rule is valid by proving that security breach functions are not only convex but log-convex (*i.e.*, $\log S(z, v)$ is convex for both GL $class\_1$ and $class_2$). Therefore, the GL model is valid for any family of functions that is part of the classes investigated in the original work [103]. Thus, as can be seen, the GL has been discussed and improved over the years, making it not perfect but the most well-accepted model for the estimation of cybersecurity investments. However, it is still challenging to precisely determine the optimum investment due to different complexities and nuances involving the cybersecurity domain,

such as cybersecurity externalities not mapped in the model when it was proposed and the difficulty of conducting parametric estimations for different real-world scenarios.

Also, the original GL model [103] has been refined to consider externalities [104] and the authors provided a new extension to include the concept of information segmentation [144] during the GL calculation. Besides that, the challenge of calibrating GL parameters (*e.g.*, a and β) for specific real-world scenarios have been considered by different approaches, such as estimating the GL model parameters [163] and using the GL security breach functions to determine the probability of an insurance claim [112].

Externalities

Network insecurity is comparable to a certain extend to air pollution. People do not bear the full consequences of their (or lack of) actions [4]. For example, people might use insecure machines plugged into the Internet or companies' networks. This means that does not matter the obstacles created (*i.e.*, protections) or cybersecurity techniques involved; the security can be impacted due to misbehaviour or external factors outside the company's control (*i.e.*, externalities). Also, cybersecurity breaches can impact different stakeholders, such as other companies part of the supply chain or customers' privacy impacts due to data leakage. Therefore, externalities can be defined as cybersecurity effects an individual's actions can have on others. Examples of factors that can result in externalities include *(i)* lack of protection due to economic or market challenges a company is facing, which might impact the supply chain the company is part of, and *(ii)* usage of software with security flaws that could have easily been prevented during its development.

The GL model was modified in [104] to incorporate such externalities, taking into account not only direct costs but also indirect costs due to externalities (*e.g.*, customers or other companies who were affected by a company security breach suing the company). For that, let L^E represent the externality costs, defined as the total loss to customers and partners, while L^P is the private costs for the company. Based on that, Equation 2.9 determines the social costs (L^{SC}) as the sum of private and externality costs.

$$L^{SC} = L^P + L^E \tag{2.9}$$

As an example, based on the concepts of the GL model, suppose a company with a $v = 0.54$, the parameters $a = 10^{-5}$ and $\beta = 1$, with a direct loss from a cybersecurity breach equal to US$ 500,000. Thus, by applying the equation for the z^*_{class1} (*cf.* Equation 2.7) it is possible to obtain the optimal investment in security equalling US$ 64,316 (*i.e.*, 12.8% of the expected loss). Suppose now that the

externality costs were defined as 15% of its private costs, which means $L^E = 75,000$. By using the Equation 2.9, the total potential loss (direct and social loss) is equals US$ 575,000. Then, by applying the equation again to find the optimal investment, the social welfare-maximizing investment equals US$ 76,210. Therefore, if the company used only considering its private costs as an example, it would result in an under-investing in cybersecurity of 15% (*i.e.*, $ 11,894).

Information Segmentation

Companies often have several information areas at their disposal, which makes information segmentation inevitable. Segmentation of networks, information, and databases is a practice that facilitates information access to specific individuals while also implementing access control to define who can access specific systems and or information. Different segments cover systems and information with particularities and, consequently, specific values and interests for both company and attackers. For example, a company's financial department might have access to customers' databases and payment systems to handle sensitive information that is very worthy and costly if leaked or compromised. This has to be considered when investing in cybersecurity, since a specific segment might be directly related to the potential benefits of cybersecurity investments.

Thus, based on the GL model, the optimal amount (z_i^*) to invest in a specific information segment i depends on the value of the information (L_i) that is part of the segment. Also, the vulnerability of each segment (v_i) has to be considered for the calculation of the productivity of additional investments in cybersecurity for each segment. Therefore, the total cost of investment results in the sum of each segment calculated individually. Hence, it is possible to prioritize segments based on cost-benefits and achieve a better overall cybersecurity investment. In order to find the optimal investment per segment, four steps are required [144]:

- **Step 1**: Estimating the value and therefore the potential loss (L) of each segment.
- **Step 2**: Estimate the probability (v) of each segment's information falling victim to a successful cyberattack.
- **Step 3**: Create a grid with all possible combinations of Step 1 and Step 2. Each cell of this grid represents the expected loss (L) without cybersecurity investments. The expected loss represents the potential benefit that can be gained by investing in cybersecurity. This means to estimate the productivity of the investments by calculating $S_i(z_i, v_i)$.
- **Step 4**: Derive the level of cybersecurity investment z_i^* by increasing the investment as long as the benefit of the additional investment is greater than or equal to the cost of the additional

investment. Since not all investments in cybersecurity have the same productivity, the optimal amount for investments in different segments will vary.

Since each information segment is a subset of the total information, the GL model assumes that the effectiveness of cybersecurity investment in a segment is inversely related to the proportion of the value of the information in a segment given the total company's value of information. Equation 2.10 determines the breach probability function of a segment *i*.

$$S_i(z_i, v_i) = S(\frac{z_i}{\frac{L_i}{L}}, v_i) \tag{2.10}$$

The security breach probability function can be defined according to the company. The function used by [144] is based on an estimation that a Chief Information Officer (CIO) and a CISO of a hypothetical company did together. This is shown in Equation 2.11. Also, the Equation 2.12 shows how to calculate the optimal investment z_i^* for a given segment *i*. This means that the optimal investment has to satisfy this equation.

$$S(z, v) = \frac{v}{1 + \frac{1}{L \times a} \times z}, \text{where } a = 0.001 \tag{2.11}$$

$$S(\frac{z_i^*}{\frac{L_i}{L}}, v_i) \times L + 1 = 0 \tag{2.12}$$

The GL model is mainly considering the information segmentation to assist companies in deriving the investment in cybersecurity with a more cost-benefit and accurate perspective. As stated by [144], companies need to understand that cybersecurity investments are best viewed as a process that focuses on preventing breaches when possible and minimizing the losses from breaches that occur. Therefore, information segmentation can be an efficient approach to help companies better understand how to invest in cybersecurity. Also, it is not realistic to achieve perfect cybersecurity, especially from an economics perspective, even with information segmentation. Thus, part of the cybersecurity investments should be considered to have also an efficient recovery plan in case of cyberattacks surpassing the company's cybersecurity.

2.2.3 Return On Security Investment (ROSI)

The concept of ROSI is slightly similar to the Return on Investment (ROI). However, while ROI focuses on measuring the benefits/profits made from a particular investment, ROSI focuses on the loss prevented by a cybersecurity investment. ROSI is a cybersecurity economics metric that helps to identify when a given solution (*e.g.*, Firewall, Antivirus, or Cybersecurity-as-a-Service product) is

cost-efficient or not [65, 239]. Also, this metric is beneficial when comparing two different solutions with similar characteristics to determine which one should be acquired from an economic perspective.

A desirable result is ever a ROSI ≥ 1, which means that the payback is positive. If ROSI is ≤ 1, there is no cost-benefit in investing in the specific solution. Therefore, the higher ROSI, the better the investment in a solution. ROSI general calculation is provided in Equation 2.13. As can be seen, for the calculation of ROSI, it is needed to quantify the monetary risk of a cyberattack. Therefore, analytical approaches have to be in place to help companies determine the possible financial losses due to a cyberattack.

$$\begin{aligned} ROSI = \frac{Risk_{Reduction} - Solution_{Cost}}{Solution_{Cost}}, \text{where} \\ Risk_{Reduction} = ALE \times Mitigation_{Ratio} \end{aligned} \tag{2.13}$$

Besides the solution's cost and efficiency (*i.e.*, mitigation rate), ROSI uses the Annual Loss Expectancy (ALE) as input. The calculation of ALE is shown in Equation 2.14. For that, it is needed to estimate the Annual Rate of Occurrence (ARO) of cybersecurity incidents and also the Single Loss Exposure (SLE), which means that an analysis of the company has to be made in order to understand the history of the attacks to identify its behaviors and impacts in the company.

$$\begin{aligned} ALE = ARO \times SLE, \text{where} \\ \text{ALE: Annual Loss Expectancy} \\ \text{ARO: Annual Rate of Occurrence} \\ \text{SLE: Single Loss Exposure} \end{aligned} \tag{2.14}$$

SLE can be described as the cost of a loss due to a single incident. As it is the sum of the losses, the value of the loss has to be very objective from company to company. Also, the loss has to include the direct costs (*e.g.*, business disruption and recovery) of a cybersecurity incident and indirect costs (*e.g.*, reputation and legal impacts).

ARO is the probability of an incident happening in a year. This probability depends on several factors (*e.g.*, level of cybersecurity, sector, and market behaviors), and it changes from company to company. If this information is not available within the company, it is possible to use entire sectors (*e.g.*, Healthcare, Financial, or Telecom) as a benchmark to support the decision.

For an example of ROSI calculation, suppose an e-commerce company XYZ with an average loss due to cyberattacks of approximately US$ 30,000, including financial loss due to business interruption, investigation costs, and third-party losses. The past attacks history shows that phishing is the

leading cause of the incident in the company, and it strikes roughly three times a year. An anti-phishing product is offered to the company at the price of US$ 25,000 and the promise to reduce the number of successful attacks by 50%.

In order to verify if this security product is cost-efficient (*i.e.*, the cost of the product is lower than the potential financial loss that the product can avoid), the company uses the ROSI model. ARO, in this case, is equal to 3 (number of times attacks strike the company), and SLE is equal to US$ 30,000 (average loss due to a single cyberattack). The solution cost is US$ 25,000, and the mitigation ratio is 0.5 (*i.e.*, reduction in 50% of the cyberattacks).

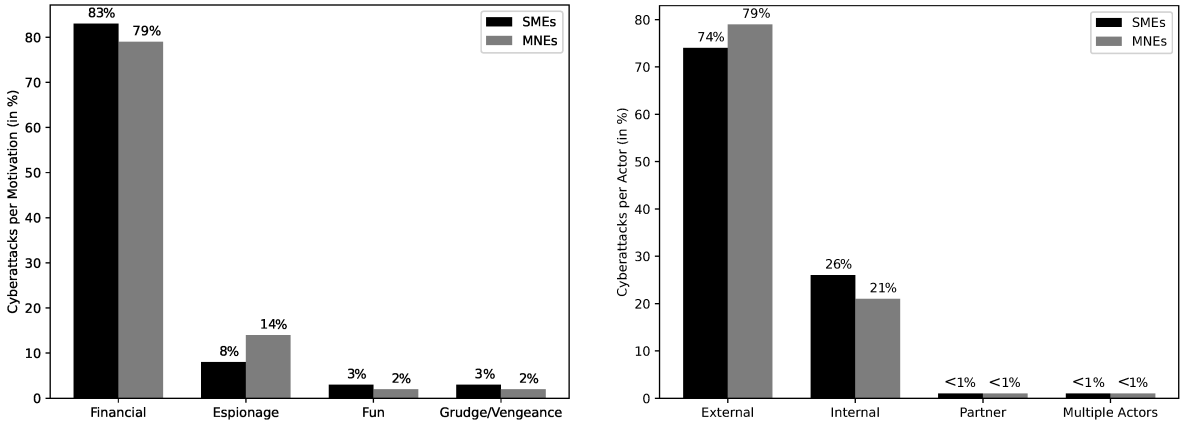
Equation 2.15 shows the calculation for the example explained above. As it can be seen, the value of the calculated ROSI is 0.8, which means that the solution is not cost-effective, since a ROSI ≥ 1 is the goal.

$$\begin{aligned} ROSI &= \frac{(ALE \times Mitigation_{Ratio}) - Solution_{Cost}}{Solution_{Cost}} \\ ROSI &= \frac{(3 \times 30000) \times 0.5) - 25000}{25000} \\ ROSI &= 0.8 \text{ (\textit{i.e.}, not cost-effective)} \end{aligned} \tag{2.15}$$

2.3 The Cybersecurity of SMEs and MNEs

SMEs and MNEs differ in many aspects regarding their organization and governance, such as the number of employees (up to 250 employees are considered SMEs [71]), amount of revenue, and business processes. Also, there are differences between digital innovation and cybersecurity adoption by these different type of companies. Both SMEs and MNEs face various challenges and similar risks regarding cybersecurity investments. The significant difference is the scale at which the risks are encountered, the budget, and the technical expertise available in-house to handle these risks. Therefore, there are aspects in which SMEs are lagging behind MNEs, as MNEs often have more resources (*e.g.*, people, technical expertise, and budget) to tackle cybersecurity threats.

Regarding differences between SMEs and MNEs, data breaches are more than twice as common in larger companies than in small ones. However, there are also similarities regarding the attackers. The proportions of threat actors are distributed somewhat similarly in both MNEs and SMEs. In an investigation conducted by Verizon [201] with more than 5,250 confirmed data breaches, it was identified that the motivation behind a cyberattack for both SMEs and MNEs is economical and



(a) Motivation Behind Cyberattacks **(b)** Actors Involved in Cyberattacks

Figure 2.9: Motivation and Actors Involved in Cyberattacks against SMEs and MNEs based on the Investigation within 5,250 Data Breaches Conducted in [201]

conducted by externals. Figure 2.9 summarizes its findings and shows that the motivation and actors involved are independent of the size of the company.

As highlighted by Figure 2.9, external actors comprise above 70% of the total data breaches, internal actors are above 20%, and partners include only 1% of the total actors. Furthermore, actors' motivations are also distributed uniformly: attackers perform cyber crimes primarily due to financial motivation (79-83%), for espionage purposes (8-14%), for fun (2-3%), and because of a grudge/vengeance (2-3%). When it comes to compromised data, it is also a comparable situation in both SMEs and MNEs: they are mainly credentials (above 50% of the reported cases), personal data (roughly 30%), and then internal data (12-14%). Moreover, the two most frequent incidents targeting both SMEs and MNEs are an inappropriate use of IT resources by employees and malware infection of company-owned devices [137].

SMEs form the backbone of the European economy, comprising, together with micro-companies, 99% of European companies and accounting for two-thirds of the total European employment. Despite their vital role in the economy and society, SMEs are still late compared to MNEs in the adoption of specific technologies. For example, in 2019, only 12% of SMEs used some big data source compared to 33% of large enterprises. A staggering technology gap would require at least five million SMEs to adopt a specific technology to close the gap before the entire ecosystem benefits from its adoption. In this sense, information regarding the adoption of cybersecurity, IoT, and big data in European's SMEs are provided by the European Digital SME Alliance and the European Commission of Executive Agency for Small and Medium-sized Enterprises [43].

There are several barriers that SMEs face in adopting new technologies. As a significant strength of SMEs lies in the ability to quickly serve a niche or specialized markets, significant parts of SMEs' human resources are comprised of domain specialists. This specialization leads to poor personal coverage in more generic functions, which are beneficial in spotting new business opportunities and trends outside of the respective domain in which SMEs operate. Compared to SMEs, MNEs have sufficient employees to cover more generic functions without sacrificing specialized personnel.

Both SMEs and MNEs are affected by a growing shortage of qualified IT specialists in the labor market. This skills shortage is severe for SMEs as they have difficulties competing with MNEs for scarce digital talent. Therefore, companies must invest in training strategies for their employees. This is not a small hurdle to overcome, given that improving more basic digital skills is already challenging enough. These strategies are currently overlooked by SMEs, with less than 10% of SMEs providing training to ICT specialists and less than 20% of SMEs offering training to other employees. Thus, over 90% of Europe's SMEs see themselves behind MNEs in terms of digital innovation.

Besides these challenges regarding digital innovation and acquisition of IT talent facing SMEs, these companies struggle with cybersecurity. Only 32% of European SMEs have been found to have a formally defined cybersecurity strategy in place, meaning that about 17 millions of SMEs in Europe alone did not have the needed cybersecurity skills in their organization. Thus, these companies must acquire cybersecurity skills by investing in new processes, people, and technology. Examples of these investments include training personnel, dedicated cybersecurity staff, and solutions that simplify the planning and investment in cybersecurity. Also, SMEs can support consultancy companies with the know-how to guide them toward an efficient cybersecurity strategy.

In a threat landscape published in 2021, analyzing data from April 2020 to July 2021 [73], ENISA highlights that SMEs discover breaches later than MNEs. According to this report, SMEs discover breaches within days in 47% of the cases, and MNES discovers in 55%. Also, it highlights that MNEs have significantly improved their cybersecurity since 2019, while SMEs have stayed the same in this period. However, SMEs are better in a few aspects when compared to MNEs. One clear example is the time to fix vulnerabilities and bugs, which is lower in SMEs. As SMEs have to handle less complex environments (*e.g.*, in terms of size, bureaucracy, and technical demands) than MNEs, SMEs fix their problems on an average of 75 days versus 88 days required by MNEs. Another relevant aspect to highlight is that contrary to common belief (which, surprisingly, also comes from the leaders of SMEs), not only large enterprises are targeted by cybercrime. It becomes much more frequent that SMEs fall victim to cyber threats, with many owners of SMEs still underestimating the likelihood of their company becoming a target of a cyber-attack. At the same time, SMEs become increasingly dependent on their IT systems and networks to provide services and products to their customers. A majority of

SMEs rely on some form of an information system. Many have an online presence as electronic communication networks, interconnected information systems, and digital services become essential for their business models.

2.3.1 Cybersecurity Trends and Challenges for Selected Sectors

The sectors of SMEs and MNEs that are the current target of more attacks are *(i)* Public Administration/Government, *(ii)* Healthcare/Medical, and *(iii)* Finance/Banking. These three sectors together represented roughly 40% of all the 1134 incidents analyzed by ENISA from April 2020 to July 2021 [73]. Besides those sectors, the digital service providers and the general public (*i.e.*, users) were also frequent targets. Due to the importance of these sectors from a cybersecurity perspective, the cybersecurity investments of both SMEs and MNEs operating or offering services in these sectors are analyzed and discussed.

Healthcare

Although the healthcare sector has been quick to adopt new technology, the same thing cannot be said when talking about taking up the responsibility of protecting newly acquired technologies against cybersecurity threats. Despite the importance of cybersecurity in the healthcare sector, findings of the sector's current state are alarming. While under-staffing or even the non-existence of cybersecurity-related positions is in no way isolated to the healthcare sector only, the scale of these problems seems to be especially large in proportion to the involved risks. Three out of four hospitals do not have a designated employee for addressing cybersecurity troubles [225].

While healthcare organizations dedicate sufficient funding to become more integrated, there is insufficient spending on keeping software updated and systems secure. This issue is further exaggerated by the general lack of cybersecurity expertise in the industry as well as the consequences following substantial expense incurred by the scarce and desired cybersecurity personnel that there is [47, 231].

The market for healthcare cybersecurity is expected to rise to US$ 125 billion between 2020-2025, according to a report by Cybersecurity Ventures [49]. This is due to the fastest-growing cyberattacks in this field, also affected by the COVID-19 global pandemic, which started at the beginning of 2020 and moved the world to a race to develop not only medicines but also technologies to support the monitoring of the viruses [84]. The pandemic added the healthcare industry to the radar of cybercriminals as never in history. Also, the report states that 62% of hospital administrators interviewed feel inadequately trained to plan or react against cyber threats that may impact their hospital.

Cybersecurity breaches in healthcare arise mainly from malware and insider threats. As malware (*e.g.*, ransomware [165] and specific medical equipment attacks [158]), is typical for this sector, the healthcare industry is focusing on investing in protecting themselves against this threat, especially those affecting IoT devices, which is a cause of attention for the following years.

Finance

A survey conducted by Cyber & Strategic Risk Services team at Deloitte & Touche and the Financial Services Information Sharing and Analysis Center (FS-ISAC) pointed out some facts regarding how digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions [124]. Table 2.2 provides an overview of cybersecurity investments in the finance sector in 2019 and 2020. These investments are also a trend for SMEs that want to offer services or products for the financial market or even be part of the supply chain of large banks. The financial organizations reported an increase in cybersecurity spending in the last years. It went up from 0.34% of revenue in 2019 to 0.48% of revenue in 2020. This also means that total IT spending rose from 10.1% of revenue in 2019 to 10.9% of revenue in 2020. Financial utility companies spend most of their revenue on cybersecurity out of all financial institutions. In 2020, the European Central Bank [59] conducted a study to identify the main risk factors that the Eurozone banking system is expected to face over the following years, which include digitization of financial services, obsolescence of specific information systems, and interconnection with third-party and clouds systems.

Table 2.2: Overview of Cybersecurity Investments of the Finance Sector in 2019 and 2020, based on the Survey Conducted by Deloitte and FS-ISAC [124]

Investments in Cybersecurity	**2019**	**2020**
Percentage of the Revenue	0.3%	0.5%
Percentage of the IT spending	10.1%	10.9%
Average per Full-time Employee	US$ 2,337	US$ 2,691
Top Investments per Type	Monitoring, Endpoint and Network security, and Access Management	Same as of 2019
Key Concerns for the Management Board	Overall cybersecurity strategy, review of threats and risks, analysis of cybersecurity program progress	Same as of 2019

According to the International Data Corporation (IDC), a global market intelligence and advisory services provider, the financial sector is expected to spend over one-third of its IT budget on managing

security services by 2023. However, today companies are still focusing more on detection than the prevention of cyberattacks. Among a survey with 400 security experts working in financial services, 56% reported that their organization could detect cyberattacks, while only 31% said their companies are preventing attacks [182].

Moreover, for the last three years, firms have identified rapid IT changes and rising complexities as their main cybersecurity challenge, and a lack of skilled cyber professionals as the second one. The third most significant challenge in 2020 is business growth and expansion. The next one is difficulty prioritizing options for securing the enterprise tied with inadequate functionality and interoperability of security solutions. Furthermore, for the past three years, the top two business challenges with security implications for MNEs have been embedding security into new products and services and introducing new channels. In 2019 and 2020, the third business issue with security implications for MNEs has been cost reduction, probably highly affected by the COVID-19 crisis, which started in the first quarter of 2020.

Additionally, companies mentioned cloud and data analytics as top cybersecurity investment priorities in 2018-2020. In 2020, the IT choices for innovations and adoption of cybersecurity by the Finance sector were artificial intelligence, process automation (*e.g.*, biometry and other physical security devices), and mobile solutions. The reasons behind this are the need for access control, protection solutions, and data security. The latter has become more and more significant over the past three years.

Telecommunications and Digital Service Providers

The telecommunications sector sees the lowest annual cost of cybersecurity and cybercrime with an average annual cost of US$ 9.21 million faced by the communications and media sector in 2018 – a 22% increase compared to US$ 7.55 million in 2017 [8]. Telecom operators' skills and expertise can partially explain this relatively low cost of cybercrime and success in protecting their networks. It is also important to note that most cyber adversaries utilize telecommunications infrastructure as their primary transport method when carrying out their attacks and therefore rely upon a robust network.

Massive cybersecurity investments in these sectors have been made in the past, allowing us to anticipate many threats and support solutions to mitigate the most dangerous for the sector and its customers with nonstop action and vigilance. However, there is still a need to evolve on this matter. This is a concern, for example, for the next generation of mobile telecommunications, such as threats affecting 5G networks and their sensitive functions (*e.g.*, network slicing, orchestrators, controllers, and virtualized infrastructure) [107]. A study supported by the EU Member States highlights that

the security challenges for 5G networks are linked to *(i)* the wide range of services and applications enabled by this technology and *(ii)* the role of suppliers in building and operating the network [172].

Due to the vast cybersecurity threat landscape that the telecommunications sector faces, investments into cybersecurity measures alone will not suffice to ensure telecommunications the security and availability of telecommunications infrastructure. This is especially visible when one looks at the telecommunication sector's supply chains, lack of resilience, and the resulting problems. Telecommunications companies need to understand whom they do business with to mitigate the threats arising from vulnerable supply chains. They need to prioritize and risk-assess each supplier and focus on redundancy, flexibility, and the technical and procedural ability to switch out a supplier if necessary. Furthermore, they need to map and assess the risks of each component and/or service offering within the supply chain and manage operational security accordingly. The strengthening of the robustness of telecommunications supply chains can be facilitated by building business continuity plans that consider the removal of critical vendors.

The future of telecommunications sector also goes toward emerging topics to build a responsible Internet [116], which proposes more transparency and trust within networks, independent of vendors and countries that run the underlying infrastructure. Thus, it is clear that the telecommunication sector has a place to ensure secure communication and a key role in the digital sovereignty.

Telecommunications also ought to work with local legislators and regulators to better understand how potential decisions concerning supplier bans could affect them. They should also support and engage with international standardization to promote better cybersecurity by developing and adopting new technologies (*e.g.*, 5G networks and the next generation of communications). Some companies (*e.g.*, Verizon, Akamai, and Cloudflare) work close to the telecommunication sectors to provide the most effective protection against DDoS attacks and other cyberattacks for digital content providers. Also, many telecommunication companies provide their solutions to protect users and companies that rely on their services.

Thus, based on these facts and current numbers, it is possible to state that the telecommunication sector is the one that invests more in cybersecurity and is aware of the different threats in the digital world. This sector employs many cybersecurity experts, which allows the development of state-of-the-art solutions. Novel solutions are frequently coming from this sector as an ally to protect other sectors and digital providers around the globe.

2.3.2 Overview of Cybersecurity Investments

According to Kaspersky, MNEs cut their cybersecurity spending from US$ 18.9 million in 2019 to US$ 14 million in 2020. The root cause of this reduction is due to COVID-19-related expenses.

However, the proportion of the budget spent on IT security has grown. In a different move, SMEs increased their average yearly cybersecurity budgets from US$ 267,000 in 2019 to US$ 275,000 in 2020. For this survey, Kaspersky interviewed 5,266 respondents across 31 countries about the state of IT security in their companies, the threats they face, and the post-attack costs they incurred [109].

At the same time, the predictions are that the total cybersecurity investments will increase over the next three years in 71% of companies. Regardless of company size, respondents said that this increase is due to the rising complexity of IT infrastructure and the need to increase employees' capabilities. Nevertheless, about 12% of companies are considering budget cuts due to overall optimization or the belief that previous investments already helped resolve their risks.

Another trend comes from the investors' side. It is possible to see that venture capitalists are increasing their funds to invest in startups that offer cybersecurity solutions [5]. This shows that the market sees the high demand for cybersecurity products as potentially becoming more substantial and worthy in the following years.

Therefore, the role of cybersecurity is clear for companies and society in the following years (or even decades). Companies have to carefully consider all of these investments in cybersecurity, since the threats can be considerably reduced by doing correct investments and planning (*e.g.*, based on risk assessments, threats landscape, and reliable metrics). A survey sponsored by IBM Security states that cybersecurity response planning is slowly improving. However, cybersecurity in companies is becoming too complex due to the use of many different tools without sufficient knowledge [182].

At this point, it is possible to understand that the cybersecurity risks that SMEs and MNEs face are pretty similar. However, according to the company, some specific threats are more common (*e.g.*, data breaches are twice as common in larger companies as in smaller companies). The significant difference lies in the ability of SMEs and MNEs to handle these risks. Despite technological advantages for larger firms, both MNEs and SMEs face challenges when it comes to recruiting new cybersecurity talent, with the labor market for such experts being scarce.

Thus, both MNEs and SMEs have to apply up- or re-skilling strategies to fill the skills gap. It has also been noted that SMEs are getting targeted more and more often by malicious actors whose goal is to enter a supply chain's information system through the weakest link. Thus, besides cybersecurity solutions, critical investments have to be made to increase cybersecurity staff and promote more cybersecurity awareness for their general employees. Also, companies have to make sure they can detect and mitigate cyberattacks effectively, with a clear cybersecurity strategy tailored for the reality of the company (*e.g.*, personnel culture, size, sector, and budget) while covering all relevant facets of cybersecurity (*e.g.*, detection, mitigation, and recovery plans).

2.4 Blockchains as a Trust Enabler and Automation Platform

A Blockchain (BC) is an ordered list of blocks, where its cryptographic hash identifies blocks. Each block is chained to the block that came before it, creating a dependency between them. Suppose an attacker wants to change a data or transaction in a block. In that case, the attacker must spend a massive amount of computational resources to change every subsequent block from the one he/she modified [162]. Thus, once a block is created and appended to the BC, the transactions in that block virtually cannot be changed or reverted. That ensures the integrity of the data and transactions in a BC. Figure 2.10 shows an example of a BC structure in which three different blocks are chained based on the hash of the previous block. Each block has its hash, a pointer to the previous block's hash, the different transactions recorded in the block, and a proof-of-work provided by the block's miner.

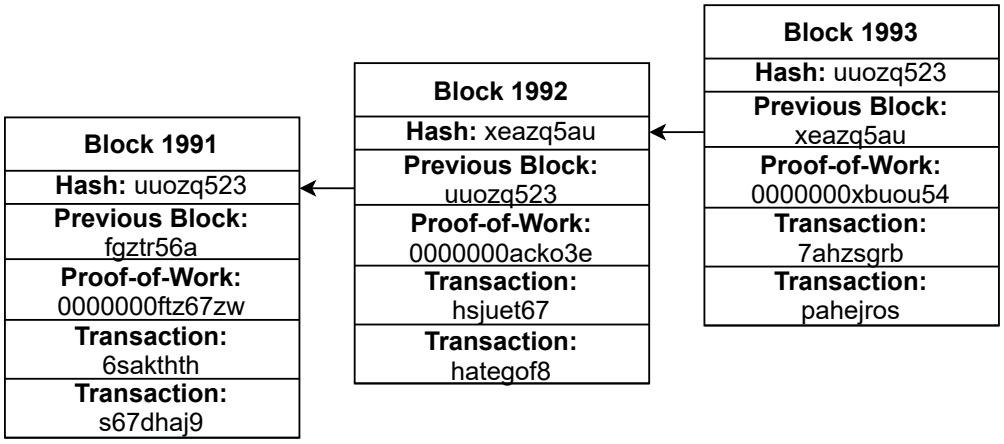


Figure 2.10: Blockchain Example

BC was initially conceived as a distributed ledger to be the backbone of the Bitcoin cryptocurrency [162]. However, its capacity to provide trustworthy, decentralized, and immutable records has attracted the attention of both industry and academia in the last years [205, 207]. BC has several benefits, which include: *(i) decentralization*, which results in transactions validation without the need of trusted intermediaries, *(ii) transparency*, to everyone observe what is on the BC and, thus, allowing auditing of the records, *(iii) immutability*, which means that once a data has been recorded into the BC, it is almost impossible to be changed without leaving traces, and *(iv) high availability*, ensured by a BC replication on thousands of nodes in a peer-to-peer network.

BCs can vary in characteristics, such as the consensus protocol used to validate transactions (*e.g.*, Proof-of-Work or Proof-of-Stake), the transaction fees, and the permission to write and read from

the BC. Although a BC is supposed to be permissionless and public (*i.e.*, anyone can read and write on that), there are different implementations (*e.g.*, Hyperledger Fabric and Corda) that allow for private implementations of BCs (*i.e.*, Distributed Ledgers) with specific characteristics that improve the performance of BC but at the cost of reducing or even the loss of the decentralization. Figure 2.11 summarizes the different deployment types of BCs.

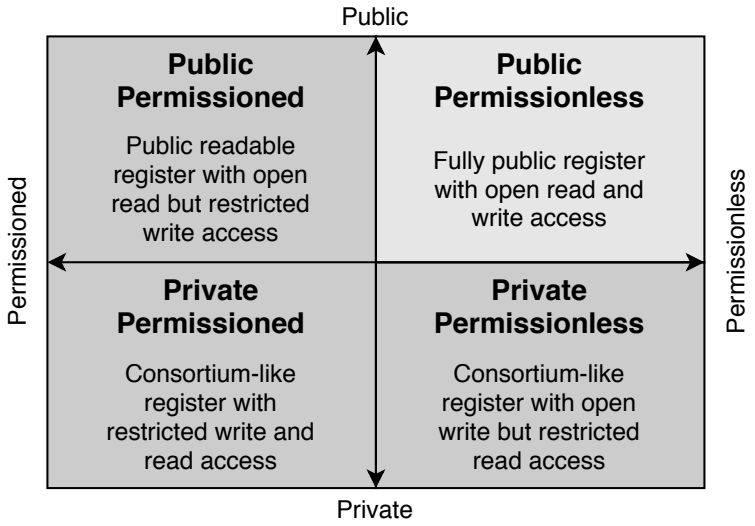


Figure 2.11: Blockchain Deployment Types [205]

Based on BC properties (*i.e.*, decentralization, transparency, and immutability), different approaches and systems can be developed to establish communication between stakeholders having no single point of trust. Also, it is possible to store information that can be validated regarding its integrity by anyone interested in it, which supports the identification of misbehavior and fraud when manipulating information. Thus, the cybersecurity market can use BCs as an enabler for trust and automation (mainly using SCs) when developing novel solutions to achieve a certain level of decentralization and integrity. For different solutions proposed during this PhD thesis, the Ethereum BC has been used due to its popularity and features that allow for a fast and efficient test and deployment of new applications running on the BC.

2.4.1 Ethereum and Smart Contracts (SC)

Ethereum [38] originated with the intent of creating a public BC platform on which general distributed applications can be built. The main drivers for such a proposal and the development of

Ethereum were the limitations of Bitcoin's scripting language, which does not provide for Turing-completeness or even states. These limitations were solved in Ethereum by relying on *(i)* an account-based BC, which is different from a UTXO model used in Bitcoin, since it modifies the state of an account, and *(ii)* an underlying built-in Smart Contract (SC) language providing the capability to developers to write Turing-complete programs, which can operate as SCs [244].

Blocks in Ethereum are smaller and are created faster (on average every 14 seconds) compared to Bitcoin's block creation time being on average at 10 min. Thus, the overall Ethereum BC size grows faster, too. To alleviate this increase in size, Ethereum implemented, apart from full nodes, which store the entire BC data, two other node types: *(i)* fast nodes and *(ii)* light nodes. Fast nodes only store block headers, and light nodes rely on full nodes to retrieve blocks when necessary. However, full nodes are always required to perform the mining and execution of SCs. Further, Ethereum's consensus mechanism "ethash" was developed to tackle the danger of centralization imposed by mining pools in Bitcoin [196]. These mining pools exist because the PoW algorithm of Bitcoin can be implemented and performed by Application-Specific Integrated Circuits (ASIC). Miners retrieve block headers from a central pool and perform the PoW on these headers without needing to maintain the entire BC. Ethash tackles this problem by being more memory-hungry, which is quite expensive in ASICs, and asking for miners to fetch random blocks, which requires the storage of the entire BC.

The Ethereum BC implements the concept of SC, which are executable code that run inside a BC to facilitate, execute, and enforce the terms of an agreement [11]. An SC can be described as a computerized transaction protocol that executes the terms of a contract agreed between the parties involved. This notion was proposed long before the arrival of BCs [220]. BCs resolved the lack of a decentralized infrastructure by providing a suitable approach to removing intermediates. SCs then became implementable, since BCs outline the perfect distributed environment for operation.

As discussed in [205], the goal of an SC is to *(i)* satisfy common contractual conditions as with any regular paper-based contracts, *e.g.*, in terms of payments, liens, confidentiality, or even enforcement, *(ii)* reduce malicious and accidental handling, and *(iii)* avoid any trusted intermediaries. Thus, the SCs concept is a viable path to automate and ensure agreements reliably and more efficiently than paper-based contracts. As specifically designed from scratch in Ethereum, the BC has proven to be a highly appropriate infrastructure for the fully decentralized and transparent execution of a mutual agreement between parties. It is worthy of mentioning that not only does Ethereum implements SC, but many new generations of BCs (*e.g.*, Cardano, Tezos, and EOS) have support or have a roadmap the plan to support SC.

In an SC, data structures and algorithms can be developed to store information and execute tasks when the specified conditions are met, such as transferring a determined value between users as a

punishment when part of an agreement is not accomplished or when one pre-defined trigger is activated. Different programming languages are available to build SC (*e.g.*, Solidity and Liquidity) [180]. The choice of a language depends directly on the objectives and BC support.

After being implemented, the code of an SC for Ethereum is executed in a sandbox environment through the Ethereum Virtual Machine (EVM) [38], in which it is possible to execute arbitrary and Turing-complete code ((*i.e.*, allowing for the execution of loops) directly on-chain. An EVM defines an environment isolated from the host itself, being precisely the same for all Ethereum nodes (called "Ethereum Clients") in the BC network. A client software (*e.g.*, Geth and Parity) is used for external communications and interactions with the operating system of the host node.

Although many different BCs provide support for the execution of SCs, the majority follow the model determined by Ethereum. A sandboxed environment ensures that the execution of the SCs is precisely the same across all nodes of the network. While the SC is defined in a high-level language (*e.g.*, Solidy or Liquidity), it is transformed and interpreted in bytecode until it is propagated onto the BC network according to the consensus algorithm configured in the EVM. The EVM operates on the respective operating system and runs the Ethereum protocol. Thus, the client communicates with the host's operating system to broadcast the transaction containing the bytecode corresponding to the SC, which is crafted into different IP packets and sent to the BC network. The role of the EVM (*i.e.*, the BC's "virtual machine") is crucial, since code must be identical across all Ethereum nodes in the BC network and must comply with well-defined interfaces. Therefore, it is possible to enable flexible support for different clients, which, in turn, can provide different abstraction levels for the development of applications.

```
pragma solidity ^0.4.10;
contract HelloContract {
      string helloWorld;
      function getHello() public {
           helloWorld = "Hello World";
      }
}
```

Listing 2.1: Example of Smart Contract for "Hello World" in Solidity [205]

Listing 2.1 shows a simple example of SC code, implemented using the Solidity programming language, that returns the text *hello world* whenever it is called. Therefore, Ethereum provides direct support for its high-level language "Solidity", with a syntax based on JavaScript. However, support for different languages that developers are familiar with exists if that language is compiled into EVM opcodes, which can be interpreted and executed by the EVM.

Regardless of the high-level language of an SC, the EVM interprets and executes EVM opcodes based on an incentive scheme, which is paid in form of *Gas*. Gas defines the internal pricing to run a transaction or a contract in the Ethereum blockchain, which is efficient for measuring the computational usage in terms of monetary costs (*e.g.*, Gas per USD or Swiss Franc) [91]. Thus, the higher the complexity of an SC is, the higher will be the cost for its deployment and operation, demanding a higher amount of *Gas* for its execution. It is important to note that such an incentive scheme is required for BCs due to the permissionless of BCs. Thus, a mechanism is needed to prevent the BC from DoS attacks (*i.e.*, an endless loop within an SC), either maliciously or just by accident. In contrast, incentives may not be necessary for Distributed Ledgers, especially those that support permissioned (*i.e.*, pre-selected users) deployments. Once a sufficient amount of *Gas* is provided for the SC's deployment, the EVM generates the bytecode, which is sent to the client.

2.5 Terminology of Business and Computer Science Fields

As this PhD thesis covers different aspects with a technological and business view, it needs to clarify the usage of different terminologies, especially those related to the contributions of this work, such as methodology, framework, and solutions.

In computer science, a methodology can be divided into five categories: *(i)* Formal, *(ii)* Experimental, *(iii)* Build, *(iv)* Process, and *(v)* Model [128]. A process methodology is used, for example, to understand and determine the processes needed to accomplish tasks in computer science [128]. This might include different methods, processes, and representations. Also, this methodology can be used to define structured processes involved for the success of a project (*e.g.*, a cybersecurity strategy). Thus, this PhD thesis focuses on the process methodology definition to provide a transparent step-by-step methodology that represents all relevant tasks decision-makers must consider when aiming for a better cybersecurity strategy.

However, in the business field, another concept could be wrongly interpreted in the context of the concept of process methodology from computer science. This concept is the framework. A framework can be described, according to the Project Management Institute (PMI), as a structured way to provide control, direction, and coordination through people, policies, and processes to meet organizational strategic and operational goals [185]. Thus, a framework harmoniously connects a set of ideas, principles, and rules to facilitate handling the situation. Table 2.3 summarizes different definitions of framework from the business field.

Table 2.3: Examples of Definition of the Framework Concept in Business-related Fields

Business Definition	This PhD Thesis
Framework is a structured way to provide control, direction, and coordination through people, policies, and processes to meet organizational strategic and operational goals [185]	Methodology
Framework is a process and fundamental base of what operating strategies guide an business or organization. The choice of a business framework depends on the business, the organizational structure, the strategic planning and systems [226]	Methodology
A **framework** generally describes the corporate organization or management structure or may generally outline company policies or an organization might develop a framework to achieve a particular goal [127]	Methodology
A **framework** is a system of rules that are used to govern a process or decision [186]	Methodology
A **framework** connects a set of ideas, principles and rules in a harmonious manner to facilitate handling of situations	Methodology

As can be seen, the concept of a framework from the business field has a similar meaning as what in this PhD thesis is referred to as a methodology. The decision for the usage of methodology is to maintain the coherence with computer science concepts, since this PhD thesis is focused more on this field. However, a reader with a business background can interpret the proposed methodology as a framework without any loss of generality of this PhD thesis.

This PhD thesis then uses the concept of a framework from computer science to describe the second contribution (*cf.* Figure 1.4). Therefore, a framework here is defined as a layered structure that indicates what kind of softwares can or should be built to satisfy a particular methodology. Also, the framework describes how these programs are interrelated. Examples of frameworks also include: *(i)* the NIST cybersecurity framework [167] that provides a high-level taxonomy of cybersecurity outcomes and a framework to assess and manage those outcomes, and *(ii)* the Mitre ATT&CK [224], which is the knowledge base of adversary tactics and techniques based on real-world observations. This framework is used as a foundation for developing tools and methodologies to document and track various techniques attackers use in the different stages of a cyberattack. Also, the Mitre ATT&CK framework can be used to identify risks and the capacity of a company to handle these risks.

Finally, different solutions are developed to satisfy different components mapped in the proposed framework. Examples of solutions include pieces of code, interfaces, and APIs. These solutions can be developed as independent algorithms, tools, or even entire platforms integrating different function-

alities. Each proposed and developed solution in this PhD thesis has specific architectures according to the technology stack and components required during the development. All of these contributions and artifacts are presented and discussed in dedicated sections within Chapter 4.

Knowledge emerges only through invention and re-invention, through the restless, impatient, continuing, hopeful inquiry human beings pursue in the world, with the world, and with each other.

Paulo Freire

3

Literature Review on Cybersecurity Planning

THIS chapter provides an overview of the state-of-the-art of cybersecurity planning and investment, also focusing on the cybersecurity economics pillars. First, the most general regulations and well-known organizational guidelines are covered. Next, a review of the current work on methodologies and frameworks for cybersecurity planning and investment is provided. Then, specific models and techniques proposed within this context are discussed. Finally, this chapter summarizes novel solutions (*e.g.*, platforms, tools, and Web-based applications) proposed by academia and industry to simplify the process of investing in cybersecurity and defining cybersecurity strategies.

3.1 Regulations and Organizational Guidelines

The European Union (EU) Cybersecurity Act came into force in 2019 to strengthen the EU Agency for Cybersecurity (ENISA) and also establish a cybersecurity certification scheme for products and services [61]. This introduces a scheme that contains a set of rules, technical requirements, and standards that helps to evaluate the level of cybersecurity risk of a product (*e.g.*, basic, substantial, or high). This certification is to be recognized in all 27 EU Member States to make it easier for businesses to prove they encompass a certain level of cybersecurity.

As the certification process is a very complex environment, the European Watch on Cybersecurity & Privacy started to provide guidance to help SMEs understand where to start implementing required standards and technical specifications. An SME, if satisfying all requirements, can receive a Cybersecurity Label as a low-cost solution that assesses and showcases its cybersecurity posture [74]. The requirements include eight domains, such as requirements for software, services, and critical business products. Besides the self-assessment provided by the European Watch, it is also important to have solutions at hand that help SMEs achieve the different requirements.

Another important regulation in Europe that went into force in 2018 is the GDPR. The GDPR is a law for privacy and security that defines rules for every company that processes the personal data of EU citizens or residents, including companies that offer goods or services for such people. Therefore, the GDPR applies even to companies not located in the EU but that offer services there. The fines for violating the GDPR are substantial, with a maximum of € 20 million or 4% of a company's global revenue (the higher value of those is considered) [46]. Although the GDPR does not focus directly on planning and investment issues discussed in this PhD thesis, it is clear that a lack of capacity of SMEs to achieve GDPR compliance [101] might result in negative economic and technical impacts. Therefore, the challenges of this kind of compliance (*e.g.*, data management and protection, information audit, and data protection officer) also have to be considered when planning and investing in cybersecurity.

Besides regulations, there are also well-known approaches from standardization institutes. For example, the National Institute of Standards and Technology (NIST) of the United States of America (USA) defined, with its latest version released in April 2018, a framework to guide cybersecurity activities as part of the organization's risk management processes [167]. This framework is composed of three parts: *(i)* a core that provides a set of activities to achieve better cybersecurity outcomes in companies, *(ii)* the implementation tiers, which provide mechanisms to understand how companies are managing cybersecurity risks, and *(iii)* the cybersecurity profiles to help companies to align and prioritize its cybersecurity activities. The NIST CSF's core comprises five key cybersecurity outcomes identified by stakeholders when managing cybersecurity risk: Identity, Protect, Detect, Respond, and Recover. Thus, the main goal of this framework is to reduce and better manage cybersecurity risks.

The framework also highlights the importance of prioritizing investments to maximize the impact of each amount spent. Thus, the NIST CSF can be used to complement existing processes within the business to improve cybersecurity operations. However, although the framework provides a complete guide to cybersecurity, it is unclear how companies can apply this knowledge to achieve a better investment and cybersecurity, such as which models and tools must be in place for efficient planning

and investment. In order to simplify the understanding of the framework, the NIST also published a version to support small businesses [169], which is a summarized version of the framework that helps companies to understand the key activities to conduct.

The European Union Agency for Cybersecurity (ENISA) has also dedicated many efforts in the last years to develop new frameworks, standardization, and guidelines for building a solid cybersecurity ecosystem for Europe. These initiatives resulted in relevant outcomes for the industry, society, and academia, such as a threat modeling and landscape [63], risk management frameworks [170], and strategies for national cybersecurity [69]. Furthermore, ad-hoc working groups have been created by the ENISA and supported by other European projects focused on different perspectives of cybersecurity, such as skills and education [68, 96], SMEs challenges and guidelines [71], and cybersecurity investment [72, 166].

Also, the European Telecommunications Standards Institute (ETSI) published a technical report in May 2021, named ETSI TR 103 787-1, which focuses on the cybersecurity standardization essentials for SMEs [62]. This report discussed and compared seventeen different cybersecurity standards and frameworks (*e.g.*, ISO 27033, ISO 27036, ISO 27002, and NIST for Small Businesses) to create a quick unified reference for SMEs to implement cybersecurity processes. It shows that the European agencies and institutes know the key role of cybersecurity for today and the future, focusing on promoting an extensive adoption of cybersecurity by businesses of all sizes. Although many solid technical frameworks are available, many efforts are still required to organize and simplify the information for extensive adoption of best practices and efficient cybersecurity strategies.

Another example of frameworks provided by organizations is the one provided by the Armed Forces Communications & Electronics Association (AFCEA). AFCEA is a non-profit US-based organization serving the military, government, industry, and academia. In [223], AFCEA presented a discussion on cybersecurity economics in a practical framework. The framework guides private organizations and the US government highlighting principles to guide investments in mapping risks and their associated economic impacts. Threats are categorized according to their complexity and their mission criticality (*e.g.*, defining how specific vulnerability could impair a service/process).

Also, the ISO 27001 [234] defines requirements for establishing, implementing, and maintaining information management systems. A set of risk management and security best practices is provided, too. The ISO 27001 is an auditable standard that allows for a well-recognized certification throughout the industry. Organizationally mature organizations are more usually to take this certification due to its associated complexities, costs, and certification process.

From a different perspective, the Information Technology Infrastructure Library (ITIL) framework [45] is designed to standardize the overall lifecycle of IT services within a business. Therefore,

ITIL provides best practices that explore the role of information security management systems to align IT resources and offerings to businesses. ITIL security management is based on the ISO 27001 standard; however, it does not focus on providing guidelines, specifications, and implementation for cybersecurity strategies.

Concerning mapping risks and threats (without a direct analysis of economic impacts), the NIST developed a model for guiding the investment in cybersecurity countermeasures. Specifically, NIST's Special Publication 800-37 [166], and 800-53 [170] are part of the Cybersecurity Risk Management Framework (RMF), including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks and the AFCEA mapping of risks allows for establishing economic models based on threats. Although NIST 800-37 and NIST 800-53 do not present an analysis directly related to economic aspects, the NIST Cybersecurity Framework (CSF) [168] (as well as the AFCEA) allows for the classification of risks, for example, to establish economic models based on threats.

Also, specific models have been proposed over the years for different scenarios and applications. For example, while NIST guidelines focus on the overall risks of an organization, STRIDE [246], LINDDUN [245], and DREAD [213] map each specific type of threat as well as their mitigation actions. For instance, STRIDE stands for Spoofing, Tampering, Repudiation, Information, Denial-of-Service, and Elevation of Privilege. It is an industrial-level methodology that comes bundled with a catalog of security threat tree patterns that can be readily instantiated [246]. DREAD is a mnemonic for Damage potential, Reproducibility, Exploitability, Affected Users, and Discoverability. This, although similar to STRIDE, represents a different approach for assessing threats [213]. LINDDUN is built upon STRIDE to provide a comprehensive privacy threat modeling [245].

Table 3.1 provides an overview of relevant regulations, organizational guidelines, and threat modeling initiatives. In summary, there are a lot of interests and initiatives from governments, industry, and academia regarding the future of cybersecurity. This goes toward the standardization of cybersecurity, new regulations, and different frameworks from the organizational to the technical level proposed and promoted by institutions with a worldwide and national scope. These initiatives are highly relevant and support the level of cybersecurity as we know of today. However, no easy-to-follow guidelines fit all businesses; neither *de jure* nor *de facto* standards for cybersecurity planning and investment are placed. Thus, cybersecurity still has to advance in different dimensions, not only with better standardization and regulations but also with more tangible and accessible solutions for SMEs and stakeholders.

Table 3.1: Examples of Relevant Regulations, Organizational Guidelines, and Threat Modeling Initiatives

Work	Type	Main Stakeholders	Characteristics
Cybersecurity Act [61]	Regulation	ENISA and EU Companies	Regulation that strengthen the power of ENISA and established an EU-wide framework for cybersecurity certification
Cybersecurity Label [74]	Guidelines	EU SMEs and Start-ups	Provides a concise manner to assess and showcase that an SME understands the landscape and key cybersecurity elements needed for a good cybersecurity posture
GDPR [101]	Regulation	All EU Member States	Defines the rules for the processing of personal data and offering of digital products in Europe
NIST CSF [168]	Guidelines	Companies	A guide for cybersecurity activities in businesses, considering risks as part of the organization's risk management processes
ETSI TR 103 787-1 [62]	Guidelines	SMEs	A where-to-start guideline for cybersecurity concepts, processes, standards, and frameworks for SMEs
AFCEA Framework [223]	Guidelines	Military, Companies, and US government	A roadmap for incremental investments in cybersecurity
ISO 27001 [234]	Guidelines and Certification	Companies	Comprises best practices and controls to ensure information covering people and processes are secure within companies
OWASP Foundation [175]	Guidelines	Developers and Companies	Nonprofit foundation that works to improve the security of software
ITIL [45]	Guidelines	Companies	Standardization for the overall lifecycle of IT services within a business, including information security best practices
STRIDE [246]	Threat Modeling	Companies	Model of threats used by Microsoft to help reason and find threats to a system
DREAD [213]	Threat Modeling	Companies	Provides a mnemonic for risk rating security threats using different categories, previously used at Microsoft
LINDDUN [245]	Threat Modeling	Companies	Systematic elicitation and mitigation of privacy threats in software systems

The following literature analysis focuses on the research developed in academia and industry to highlight the current trends toward better cybersecurity planning and investment. This analysis is

conducted from an economic lens ever more than possible, which means that the ultimate goal is to highlight how the current and novel solutions can contribute to cost-efficient cybersecurity strategies.

3.2 Methodologies and Frameworks

Besides the fact that well-known methodologies and frameworks are placed, like those discussed in the section before, there are research efforts to understand cybersecurity nuances to develop and promote novel approaches that help during cybersecurity's planning and decision process. This section explores the knowledge and challenges of different fields and sectors to build a foundation (*i.e.*, methodologies and frameworks) for efficient cybersecurity planning and investment.

Inspired by the Project Management field, the work proposed in [222] modeled an easy-to-use cybersecurity canvas to address the problem of SMEs having a lack of knowledge to handle cybersecurity. The proposed framework is based on modular building blocks that can be individually or together according to the demands of an SME. This work uses a top-down approach divided into five layers: *(i)* Preparation and Assessment, *(ii)* Management Level, *(iii)* Technical Level, *(iv)* Attacks Management, and *(v)* Implementation and Improvement. The framework defines eleven obligatory tasks (*e.g.*, objectives of security and budget, definition of critical systems, and employee awareness-raising) for all organizations, ten strongly recommended but not mandatory, and four recommended but optional. This helps companies use the framework as an initial self-assessment to think about processes and complexities to determine or improve a cybersecurity strategy. However, although the steps are well-defined and the framework easy to use, it does not indicate which kind of information an organization has to collect nor which kind of techniques and tools are needed for a successful assessment. Also, the outputs of the framework are hard to measure, since there is no indication of what is a success/failure for each layer.

In another work, [31] provided a framework to improve the way how to think about cyber risk. This framework relies on the knowledge of different fields (*e.g.*, computer and network engineering, economics, and actuarial sciences) to investigate and shed light on the nature of cyber risks. This framework categorizes the risk factors into five sequential classes: threats, vulnerabilities, controls, assets, and impacts. According to the framework definition, not every threat realize a risk, and neither does every pair of threats and vulnerabilities lead to a successful attack. The interaction between threats, vulnerabilities, and controls determines the success of attacks. The value and importance of an affected asset define the impact of an attack. The key outcomes of the work include *(i)* a differentiated view on cyber versus conventional risk by separating the nature of risk arrival from the target exposed to risk, *(ii)* the conclusion that economic impacts are characterized by incomplete informa-

tion, externalities, and wrong correlation caused by risk factors, and *(iii)* quantification of cyber risks suffers from a lack of relevant data, information sharing, and knowledge about threats and vulnerabilities. Based on that, although the work discussed in-depth relevant challenges for cybersecurity, one of the most relevant key messages is that relevant data will never become available unless policies are written and regulations adopted (as discussed in Section 3.1 above).

[179] introduced an approach to identify cybersecurity challenges and opportunities, thus, helping to the development of new risk assessment and management frameworks. The work investigated the most well-known risk assessment methodologies and frameworks (*e.g.*, ISO 31000, TOGAF Security Guide, MEHARI, and MAGERIT), thus, mapping how they fit specific requirements. The analysis of existing frameworks identified that current risk assessment frameworks do not consider relations between sectors and cannot address multi-sector and transversal issues. Based on this analysis, the authors proposed a conceptual framework called E-MAF to evaluate cybersecurity risks in trans- and multi-sectoral contexts. This framework is composed of *(i)* the Transversal Foundation Tier, which guides the organizations to manage and reduce their cybersecurity costs in a way that complements an already placed processes for cybersecurity and risk management, *(ii)* the Multi-Sector Implementation Tier, where all multi- and inter-sector aspects are managed, such as supporting the understanding of specific views and priorities of organizations, and finally, *(iii)* the Security Alignment Tier, which implements all security controls. Based on that, it is possible to argue that [179] defines an interesting new approach that can be used for cybersecurity risk assessment and management in multi-sector and transversal scenarios. However, although it looks to be a promising approach for companies, it still lacks better comparisons and evaluations with the current frameworks.

Other frameworks are available for specific sectors or technologies, such as the one proposed by [229]. It provides a valuable tool for senior management to understand security problems and organize security processes in the construction industry and civil engineering-related tasks, thus, handling specific issues related to this sector's supply chain and activities. Another example is the methodology developed in [217] for the assessment of cybersecurity in healthcare scenarios based on IoT. Besides these examples, many works have explored well-known frameworks to validate and adapt for specific scenarios, such as for campus IoT collaborative defense using NIST CSF [243], and the analysis of blockchain cybersecurity [108].

There are also different methodologies and frameworks focusing on investments in cybersecurity. Most of them rely on the foundations provided by the well-established metrics discussed in Sections 2.2.2 and 2.2.3: the Return On Security Investment (ROSI) and the Gordon-Loeb (GL) model. For example, in [106], the authors proposed the usage of the GL model as a logical approach when considering the cost-benefit aspects of cybersecurity investment based on the implementation of the

NIST CSF. This allows for an integrated framework that addresses economic and technical aspects of cybersecurity. This kind of work might be used as motivation for a path to follow. As companies and research results become mature, it is expected that best practices and solutions emerge to address cybersecurity planning and investments using - at best - a common language and background.

The work conducted in [248] provided a comprehensive framework to measure the effectiveness of the ROSI metric. The framework was validated and, based on an experimental analysis using the Common Vulnerability Security System (CVSS) attack dataset, shown that it is possible to reduce 75% of annual loss due to cybersecurity by following the proposed systematic framework to determine the ROSI. Thus, it suggests that organizations can save resources (*e.g.*, time, money, and personnel) by following proper approaches and metrics during the investment in cybersecurity. In a previous work [99], a family of analytical frameworks was proposed to assess and measure the effectiveness of cybersecurity and the economic benefit of investments. This work helped to understand the complexities and different ways to think when analyzing the economic-benefit returns of cybersecurity investments. Therefore, even with the excellent results of different frameworks placed, planning and investments in cybersecurity cannot be based only on rigid model structures or static steps but requires a combination and selection of frameworks, models, and solutions.

3.3 Models and Techniques

Aiming at the evaluation of economic risks, [6] proposes a model based on Routine Activity Theory (RAT) to study the attacker's goals by using the information about the attack reported in news articles. It shows how RAT may explain DDoS attack trends in educational institutions. The work conducted argues that DDoS attacks are not random phenomena, but attackers are instigated by their circumstances. Therefore, it was observed that measuring the actual economic impact of DDoS attacks is a very complex task and requires, as a first step, understanding the context of a specific attack. From an economic and societal perspective, these arguments and the model itself can be used to understand different attacks, such as the current ransomware trend and phishing attacks.

In another work, [142] proposed a Deep Learning (DL) model to assess economic risks in virtual power plants. The authors explored two techniques called Naive Bayes and the J49 bagging tree model. The initial results suggested an exciting path for artificial intelligence as an ally for measuring and understanding economic impacts during cybersecurity planning. However, challenges have to be addressed in this field, such as the lack of explainability of DL algorithms [119] and insufficient cybersecurity information sharing for training these kinds of algorithms [203]. Also, researchers from the NIST proposed a model to assess cybersecurity risks to support investment strategies in network

security [155]. This work highlights how ML can be used as a foundation for cybersecurity investments in different scenarios, *e.g.*, those that use remote work tools, IoT devices, and mobile elements.

The work conducted in [133] proposed a model to measure data breach risk's probability, thus, identifying the maximum loss due to a cyberattack. The authors used an alternative approach to estimating the potential loss degree of an extreme event with one of the largest private databases for data breach risk. The statistical estimation process for the data breach loss maxima comprises data analysis, time-series analysis, extreme value analysis, and prediction techniques. Although existing models empower organizations to compute optimal cybersecurity investments (*e.g.*, GL and ROSI), some uncertainties must be considered. For that, in [77], the authors proposed a game-theoretic model that shows how uncertainties (*e.g.*, possible new vulnerabilities after investments and mistaken values assigned for the risk assessment parameters) regarding the cybersecurity risk assessment and planning might affect the efficiency of cybersecurity investments. The authors explored game-theoretic concepts and combinatorial optimization techniques, such as a single-objective multiple-choice knapsack-based strategy. The work argues that uncertainty is naturally a challenge that all cybersecurity managers face when making decisions. The work also highlights that it is possible to mitigate most damage by selecting proper cybersecurity measures even with some uncertainty during the cybersecurity planning and assessment.

In [194], a novel model called Cybersecurity Economics and Analysis (CEA) is proposed to increase the harmonization of European cybersecurity initiatives and synchronizing practices of cybersecurity solutions. This model is based on strategic and long-term thinking to incorporate economics in the decision-making for cybersecurity. Thus, a holistic approach is used to propose a model that considers technical perspectives of organizations' security and institutional, economic, governance, and human dimensions of cybersecurity. The CEA model was also a try to provide a benchmark for the economic assessment of cybersecurity at a national and international level. However, it still lacks evaluations to assess the effectiveness of the model and the economic impacts of cybersecurity.

Finally, an extension of the GL model is proposed in [52] to consider multi-period and relaxing assumption of a continuous security breach probability function (*cf.* Section 2.2.2). This allows capturing dynamic aspects of cybersecurity investment, such as in scenarios that are impacted by disruptive technologies and constantly evolving. The extension was demonstrated by conducting a case study for critical infrastructure protection. This case study and discussions show evidence that the extended ENBIS function (*i.e.*, the difference between benefits and cost) and security breach probability function allows the GL model to capture the financial consequences on the optimal investment level due to the advent of new and disruptive technologies. As a limitation, the authors highlighted that simulations and empirical tests are still required to validate the approach, since it requires the

specification of productivity parameters α and β, which are not trivial to measure these parameters, even though it is possible to derive by using specific GL model equations. In another work also based on the GL model, the framework proposed in [146] illustrates a continuous improvement of cybersecurity performance and investment cost analysis in a real-world cybersecurity scenario.

3.4 Solutions

The solutions considered for this PhD thesis are tools, systems, or software that implement methodologies or techniques to allow users to handle cybersecurity demands. All of these solutions discussed in this section provide at least *(i)* a backend that implements a set of features for cybersecurity planning and investment and *(ii)* a frontend that allows users to interact with the solution to access the features. Therefore, solutions like those discussed below are essential for cybersecurity planning and investment, especially for SMEs that need intuitive and simplified ways to handle their cybersecurity.

The Cybersecurity Osservatorio offers a set of cybersecurity services to raise SMEs' awareness of the importance of cybersecurity. One of these services is composed of a cybersecurity self-assessment tool [48]. The main goal of the tool is to provide a quick and straightforward tool for cyber risk self-assessment. The tool requires two types of input: information about security measures and information about key assets of the enterprise. When all inputs are provided, the tool estimates the expected annual losses for every relevant threat and a total one. The output is to be available when the input information is correctly provided.

Also, a radar chart, as shown in Figure 3.1, provides the average values of compliance for each category (*e.g.*, access control, communications security, and security policies) for the companies that used the self-assessment questionnaire. Also relying on questionnaires, the work developed in [28] presents an SME cybersecurity evaluation tool based on the NIST Cybersecurity Framework (CSF). By selecting and improving a set of the controls defined by the NIST CSF, the tool makes it easier for SMEs to complete a cybersecurity risk assessment. Also, the tool aims to provide best practices and specific recommendations on how to improve security in an organization.

[123] developed a tool named SERViz to support the risk assessment and economic analysis of cybersecurity. By using the tool, decision-makers can configure different parameters related to their business (*e.g.*, business sector, operation systems, and most common attacks), analyze the risks, obtain insights about direct and indirect costs (*e.g.*, due to business's downtime and reputation loss), and receive recommendations of cost-efficient countermeasures. The tool also relies on ROSI to highlight, besides technical aspects, the better from the economic perspective. However, the tool is still

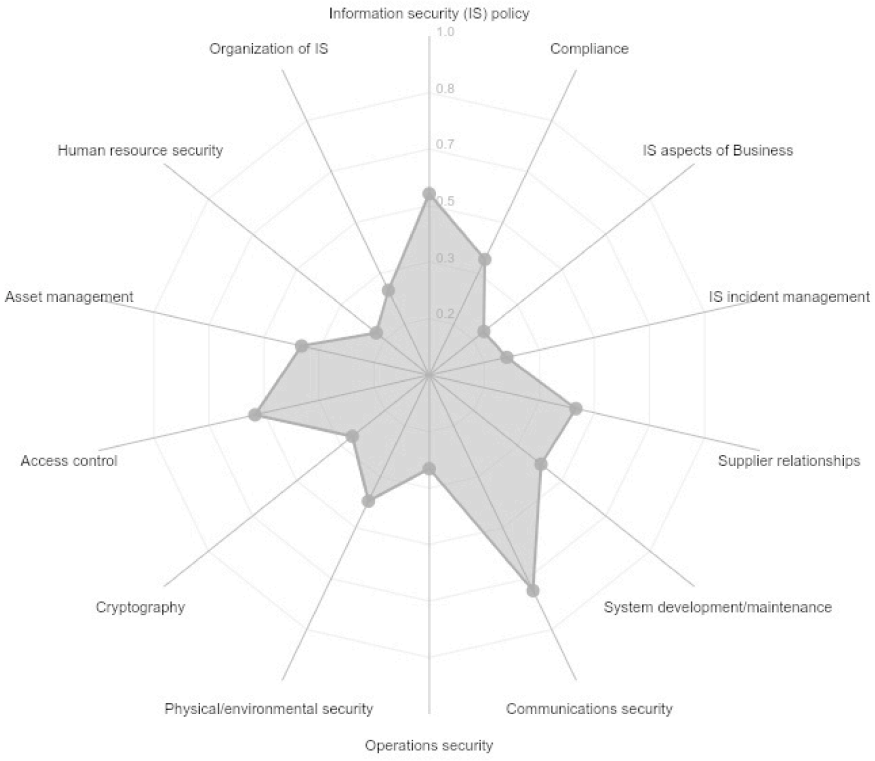


Figure 3.1: Summary of Compliance for Each Category in the Self-Assessment Questionnaire, as presented in [48]

a conceptual prototype, requiring more investigation related to available cybersecurity economics metrics, validation with industry partners, and populated with relevant cybersecurity information to become used in production.

[120] proposed a recommender system that tracks and recommends protection against vulnerabilities. The work uses a pipeline composed of Natural Language Processing (NLP), fuzzy matching, and ML. The automation provided by the solution allows a cybersecurity analyst to obtain a list of vulnerabilities that match their software or hardware inventories. The recommender system was tested and compared against a human analyst. During the evaluation, 50 software and 50 hardware inventories with commonly used software, network, and computer hardware components were considered. As a result, for these given datasets, the recommender system saved over 7 hours of work while also providing more accurate results than vulnerability analysis conducted by humans. Although other recommender systems are available in the literature, this is, according to the authors, the first work to address, in an automated way, the problem of the matching of vulnerabilities in private inventories of software and hardware.

A recommender system for data protection was introduced by [147], which simulates protection options and provides insights into aggregated plans. The system recommends protections for a given data group to achieve a higher risk deduction with a given budget. Also, related risk factors can be visualized in the user interface, allowing for interactions and recommendations according to the user's demands. This kind of system can reduce security analysts' cognitive load and improve the performance of tasks required for efficient data protection decisions. Even though this work can serve as the first step toward data-centric security application, the authors emphasize that evaluations with larger samples are still needed to validate and improve the proposed system.

In another work based on NIST CSF, the authors proposed a user-interactive cybersecurity tool to simplify and automate the NIST-compliance of companies [118]. This work developed a front-end and back-end to provide a robust and user-friendly NIST-compliance guideline tool. For that, features were developed, such as the questionnaires generators based on NIST CSF according to the company being analyzed, a heat map generator to visualize the CIA score, and a database editor for information management. Also, APIs were developed to allow the interaction between the different components and features of the work. The work was validated in a scenario considering e-commerce risk management. However, even simplifying the process by providing Web-based interfaces and other features, applying the NIST CSF remains a challenge for SMEs, since it requires an understanding of cybersecurity-related information, concepts, and interactions.

[195] proposed a new solution for the analysis and risk management. The solution novelty relies on the correlation between vulnerabilities and assets available in the company. It is possible to understand the potential impacts on the assets if a given vulnerability is exploited or an incident happens. The authors argued a gap in the literature that concerns technical and economic impacts, since most of the solutions available for risk management focus on the threats only without understanding the assets and their possible economic impacts.

A tool named ReCIs was introduced in [114]. The tool applies the Return on Cybersecurity Investment (ROCI) model, also proposed by the authors of the work, to quantify the effect of cybersecurity investment on critical infrastructure. In the ROCI model, the ultimate return value to determine if protection is cost-efficient is calculated as the annual difference between costs associated with cyber-attacks minus the costs of those same attacks, now mitigated by a cybersecurity solution. This metric looks very similar to the ROSI, one of the metrics covered by this PhD thesis. By using the ROCI model and recommender systems, the ReCIs tool can provide financial cost overviews. Also, it helps during the decision process of selecting a cybersecurity solution for critical infrastructure. This work was one of the first cybersecurity investment approaches to quantify a return on investment for the critical infrastructure sector.

As an example of effort from the industry, there are dedicated efforts to developing a tool for real-time risk assessment called CERCA [152]. The tool receives input data from various sources that can inform about changes in the target system (*e.g.*, new threats, new target nodes, new vulnerabilities, alarms from Security Information and Event Management, and Intrusion Detection System tools). Input data can also come from historical events or questionnaires (filled by end-users). However, the strength is the usage of real-time indicators, such as security events/alarms, configuration changes, vulnerabilities (detected by monitoring tools), and potential threats/attack patterns (predicted by AI-based tools or provided by threat intelligence sharing). These efforts show the potential and interest of the industry in the market of cybersecurity and its potential economic impacts. At the time of this PhD thesis, the CERCA solution was still under development [214].

An overview and comparison of different solutions discussed within this section are shown in Table 3.2. These solutions are classified according to their categories (*e.g.*, risk assessment or cybersecurity investment) and whether they are commercial products or research prototypes. Also, the availability of important features to support cybersecurity planning and investment are analyzed, including the *(i)* availability of intuitive and user-friendly interfaces to users access the features provided by the solutions, *(ii)* technical dimensions of cybersecurity, such as analysis of vulnerabilities, identification of violations of CIA triad, and integration with robust monitoring solutions, and *(iii)* coverage and analysis of economic aspects of cybersecurity, such as considering financial loss due to cyberattacks and cost-effective decisions for better cybersecurity.

3.5 Key Observations

This chapter provided an analysis of the state-of-the-art of cybersecurity planning and investments. This analysis was conducted during this PhD thesis's development and was fundamental to identifying and validating research gaps, opportunities, and challenges for the field. This PhD thesis covers different aspects of cybersecurity, from the planning and risk assessment to the investment and deployment of cybersecurity strategies. Therefore, the related work also has to investigate different domains while maintaining the focus and scope relevant to pave the path and contributions of this PhD thesis, *i.e.*, methodologies, frameworks, and solutions.

Different organizational guidelines and standardization approaches were mapped to highlight the efforts toward better cybersecurity. It is possible to observe that the most well-known and accepted initiatives (*e.g.*, NIST CSF, ENISA, and STRIDE) have been placed there for many years. However, there are still many complexities (from the technical, legal, and economic perspective) involved in

Table 3.2: Overview and Comparison of Solutions for Cybersecurity Planning and/or Investment

Solution	Category	Type	User-Friendly Interface	Technical Aspects	Economic Aspects	Characteristics
Cybersecurity Osservatorio Questionnaire [48]	Risk Assessment	Product	Yes	Partially	Yes	Provides report on expected annual losses.
Rea-Guaman et al. [195]	Risk Assessment	Research and Prototype	Yes	Partially	Partially	Correlation between Vulnerabilities and Assets.
CERCA [152]	Risk Assessment	Product	Yes	Yes	Yes	Real-time Assessment and SIEM integration.
Tracking Vulnerabilities [120]	Recommender System and Risk Assessment	Research and Prototype	No	Yes	No	NLP and ML techniques is applied to list vulnerabilities in a software inventory.
ReCIst [114]	Cybersecurity Investment	Research and Prototype	Yes	Partially	Yes	Quantifies the effects of cybersecurity investment in critical infrastructures.
CET [28]	Risk Management	Research and Prototype	No	Yes	Partially	Questionnaire-based tool with 35 questions based on NIST CSF.
SERViz [123]	Cybersecurity Planning	Research and Prototype	Yes	Partially	Partially	Protection measures and ROSI integration.
CSAT [118]	Risk Management	Research and Prototype	Yes	Yes	No	Visual tool that simplifies and automates the application of NIST CSF in companies.
Li et al. [147]	Recommender System and Cybersecurity Planning	Research and Prototype	Yes	Yes	Yes	Provides recommendation for data protections based on risk factors and a given budget.

following cybersecurity guidelines and achieving compliance with regulations in the short term, especially if considering the reality of SMEs. Therefore, the cybersecurity culture might need to be promoted by state-sponsored actions, while approaches that simplify the adoption of cybersecurity become more accessible for any interested stakeholder.

These investigations conducted observed that the methodologies being researched for investment in cybersecurity are based on three fundamental areas for building cybersecurity strategies: People, Processes, and Technology. The methodologies address the open challenges considering different views and dimensions. For example, approaches had been undertaken to improve cybersecurity planning by exploring project management concepts to support how companies plan and implement cybersecurity strategies [150]. Also, there are different approaches exploring cybersecurity economics

metrics (*e.g.*, GL and ROSI) together with risk assessment methods to build frameworks that allow for the analysis of cybersecurity from an economic perspective, thus, helping to better plan how and where to invest in cybersecurity to reduce the financial losses due to cyberattacks with the minimal possible investment. Nevertheless, there is still a need for validation and better evaluation of the potential benefits, in real-world scenarios, of most of the methodologies and frameworks proposed, since they are addressing a field that has many uncertainties and lack of information, especially due to the information asymmetry that makes it hard to build an approach that fits all scenarios.

As can be seen by looking at related work regarding models and techniques, there are efforts and open challenges to propose efficient models to understand and evaluate economic risks. Many of these models are inspired by the models proposed at the beginning of the century. However, these models have used many extensions to achieve better and more reliable performances. It is still an open field regarding techniques being used, which requires exploratory research in the sense that different techniques can be used together with a theoretical foundation to evolve these models [203].

The analyzed solutions are helping the adoption of cybersecurity by companies from different sectors. For that, most of the solutions are implementing user-friendly Web-based applications to simplify the interaction of stakeholders with novel algorithms, models, and techniques. These solutions are evolving with different workflows and integration proposed by the research conducted in the field and industry efforts to address cybersecurity challenges, especially for SMEs in a market that still needs more popular and cost-effective solutions. However, these solutions are still limited by the amount of information needed to plan and invest. This limitation can be described as a paradox, since new solutions are needed to understand cybersecurity planning and investment information. At the same time, these solutions also need specific information for cybersecurity planning and investment. Hence, research in the field is crucial to develop solutions that can correlate information and also provide insights to decision-makers based on the information they have at hand.

In conclusion, the cybersecurity field is receiving much attention on different fronts, from the mitigation of cyberattacks to the planning and investment for defining cybersecurity strategies. This PhD thesis will focus on the open gaps of the last one in order to shed light on challenges and opportunities in this direction. These gaps and opportunities identified will be analyzed and addressed with the technical view that is required for a complex field like cybersecurity but also with an economic bias, since economic aspects (*e.g.*, financial losses due to cyberattacks, lack of budget to invest in cybersecurity, and profits made by attackers) are highly relevant when discussing and planning cybersecurity strategies for all involved stakeholders

If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

Richard Clarke

4

The CyberTEA Approach

DETERMINING stakeholders and its economic dimension concerning costs of different systems and processes is one important pillar for efficient cybersecurity planning. Besides, there are different steps to be followed to plan and deploy an effective cybersecurity strategy not only from a technical perspective but also considering economic aspects (*e.g.*, cyberattack costs vs. protection costs). For that, the Cybersecurity Technical and Economic Approach (CyberTEA) focuses on three main contributions: *(i)* a methodology that maps key elements and guides business in the initial and critical steps, when planning a cybersecurity strategy, *(ii)* a framework that defines the components required to be implemented by solutions that aim to cover the important steps of cybersecurity planning, and *(iii)* a set of solutions that implements different features to support the planning, investments, and deployment of cybersecurity. These solutions satisfy one or more components determined by the framework proposed as well as can be mapped within the methodology defined by the *CyberTEA* approach.

Therefore, this chapter is organized as follows. First, the methodology is introduced, including all phases. Next, the framework is presented, and each component required is discussed. Finally, novel designed and developed solutions are introduced, providing proofs-of-concept that implement features and components. All of the implemented solutions covered at least one phase of the method-

ology while also implementing one or more components of the defined framework. Also, APIs are implemented for each solution to enable the exchange of information. Therefore, the solutions can be placed as a stand-alone solution or as part of the same ecosystem to address the demands for an efficient cybersecurity strategy.

4.1 Methodology for Cybersecurity Planning and Investment

The proposed methodology comprises five phases representing sequential tasks decision-makers must consider, when planning a new (or updating an already placed) cybersecurity strategy [93]. Figure 4.1 shows the methodology, including all phases (from A to E) and examples of critical steps that must be performed in each one of these phases. This methodology was defined based on an in-depth literature review, interviews with cybersecurity experts and decision-makers from industry, SMEs, and academia, and based on all knowledge obtained and discussions conducted. It is important to mention that the steps highlighted for each phase are examples of general steps common for most companies, but not exhaustive. The methodology can be extended and adapted to fit the specific demands of a particular company or sector.

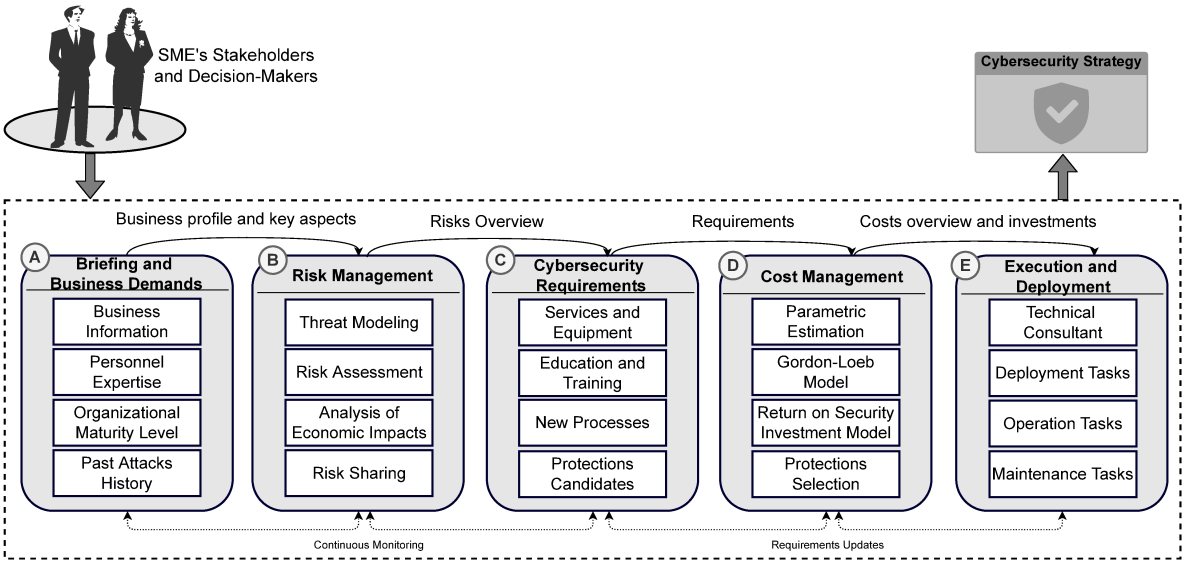


Figure 4.1: The Methodology for Cybersecurity Planning and Investment with the 5 Phases Mapped by the *CyberTEA* Approach

The methodology starts in **Phase A** (*i.e.*, Briefing and Business Demands), where all information related to the business have to be collected and a briefing conducted with the stakeholders involved.

An example of the relationships of stakeholders in the financial sector is provided in the Appendix C. For this phase, information regarding the business is the key, such as company sector, technologies being used, number of employees, revenue, and portfolio. Next, the personnel expertise is an important indicator of understanding possible challenges or technical weaknesses to be considered during the planning of a cybersecurity strategy. If the company does not have a high level of education in cybersecurity, it can become a vector for many attacks (*e.g.*, phishing and ransomware). Also, an important point to consider is if the company has a dedicated security team or a person to handle security-related issues. Understanding the maturity level of the business and its processes is also relevant for this initial step, since it shows the capacity of the company to adopt new processes during the planning of a cybersecurity strategy.

For the final step of this phase, the history of past attacks on the company has to be collected. Examples of this information can be the frequency of attacks in the last years (*e.g.*, last three years, a company has a yearly average of seven phishing attacks), the success rate of these attacks, and their impacts (*e.g.*, business disruption during 8 hours). This is an important metric that can help, combined with other statistics and security trends for the sectors (*e.g.*, Healthcare, Telecom, and Finance sectors), to plan the initial cybersecurity requirements for business.

This kind of information can trigger alerts that have to be considered by the company. For example, even if a company did not face any critical impact due to cyberattacks, a high rate of attacks in the sector and also a high success rate of other attacks in the company might lead to the conclusion that the company has to conduct the risk assessment for this kind of attack carefully. Therefore, the company should not rely only on the idea of no critical impacts due to cyberattacks but read the success rate of these attacks in the business as an indicator of possible problems in the future. For example, a phishing attack that does not look so dangerous for the company can be used to infect the whole company infrastructure with a ransomware attack, which can cause business disruption, leak of data, and, consequently, high financial losses.

In the **Phase B** (*i.e.*, Risk Management), the focus is on the security analysis and threat modeling of the company. For that, state-of-the-art tools and solutions can be considered for the risk assessment, including well-known and commercially established tools in the market to analyze security-relevant data and conduct penetration tests (*e.g.*, Nmap, Metasploit, Elastic Stack (ELK), and Splunk). Also, during this phase, the threat modeling can be conducted by using specific models, such as the STRIDE threat model and MITRE ATT&CK framework, as discussed in Chapter 3. Besides that, an analysis of the economic impacts is also a highly relevant step, since the difference between investments in cybersecurity and the costs of cyberattacks have to be positive. An analysis has to be conducted to determine how valuable each asset is for the business operation (*e.g.*, segments of information within

the business, marketplace, and underlying infrastructure) and the likelihood of these assets being attacked. Also, besides understanding the risks and costs of an attack individually, it is crucial to understand the interdependence between systems/subsystems, which can trigger cascade failures.

Information sharing is also essential, when conducting risk management, since companies can define a consortium of trusted partners sharing information regarding technical and economic impacts within companies with similar characteristics (*e.g.*, same sectors and attack vectors). Furthermore, to avoid reducing substantial economic impacts in case of a cyberattack or failure, it is possible to share the risks with third-parties companies, such as contracting a cyber insurance company to cover unexpected costs due to cyberattacks. Cyber insurance is a growing market in which companies pay premiums to have coverage that alleviates the costs of cyber incidents. Without cyber insurance, many companies (especially SMEs) might not even continue with their business after a cyberattack due to the direct and indirect costs.

After having defined the business profile and understanding the risks, the **Phase C** (*i.e.*, Cybersecurity Requirements) can start. This phase consists of defining cybersecurity requirements to achieve a sufficient level of protection, mapping processes that must be modified or created within the company, and defining activities required to implement, deploy and operate the cybersecurity strategy. After the information is mapped and all relevant cybersecurity requirements are defined (*e.g.*, the main goal, acceptable level of protection, and which risks can be assumed), it is possible to map possible protection candidates. For example, the company can decide that a new solution against DDoS and phishing attacks must be placed. Therefore, a list has to be determined with possible solutions or providers that offer a proper level of protection against DDoS and phishing while also addressing the company's requirements. After all cybersecurity requirements are defined, the costs must be investigated and determined.

In the **Phase D** (*i.e.*, Cost Management), the costs of implementing the cybersecurity strategy have to be estimated and adapted. As an initial step, a parametric estimation can be conducted to determine the costs of time and resources required to implement the cybersecurity strategy. This step might use the company's historical data and successfully implement cybersecurity strategies in companies with a similar environment. It helps to estimate, with a certain level of granularity, the resources and time required for that. As SMEs do not have extensive experience with cybersecurity, it is possible to use both *(i)* information from other companies and partners with similar characteristics and sectors and *(ii)* expertise in other IT projects that shows the costs to deploy, train, and operate new solutions. This, together with other models, can be very useful to be used as an estimating tool with a reasonable level of accuracy. Examples of aspects to be considered for the parametric estimation (*i.e.*, for the estimation of costs and time) include:

- Historic and market data on the cost and time requirements to implement similar protections and training;
- Determine the maturity of the team to lead and implement the project;
- Determine the steps that are critical for the success of the project, which cannot be excluded from the budget available;
- The number of solutions to be deployed and how large is the infrastructure to be protected (*e.g.*, number of endpoints, computers, and network devices).

This list of aspects cannot be considered complete for all scenarios but highlights important aspects as an example of which kind of information to focus on. Considering this information and metrics, it is possible to apply the parametric estimating formula for each relevant metric to view the project's cost estimation, which can be correlated with the optimum investment and ROSI. Still, it is important to determine the maximum amount to invest in cybersecurity based on its value and data in the Cost Management phase. For example, it is more adequate to assume risks than invest a large amount of money in protecting not critical systems in some instances. In order to obtain the optimal investment amount, the *CyberTEA* explores the GL model, one of the most well-accept models for cybersecurity investments (*cf.* Chapter 2, Section 2.2.2). As one of the assumptions for optimal calculations, GL determines that the investment in security must not exceed 37% of the potential loss (d). It relates to how much the system is valued (λ), how much the data/system is at risk (t), and the probability that an attack on the data/system is going to be successful (v).

After obtaining the optimum amount of investment in cybersecurity (*i.e.*, the GL calculation), the next step consists of, based on the budget available, determining which of the candidate solutions and strategies will be selected to be implanted, as mapped in the previous phases of the methodology (*i.e.*, Step C - Cybersecurity Requirements). For that, recommender systems (*cf.* Section 4.7) can be used together with other methodologies based on the company's technical know-how. After the solutions are mapped, the ROSI model (*cf.* Chapter 2, Section 2.2.3) can be calculated for each one of the solutions and strategies mapped to be implanted. This includes, for example, the calculation of ROSI for investment in solutions (*e.g.*, firewalls, antivirus, and cloud-based services) and other tasks (*e.g.*, training and backups). The ROSI is considered satisfactory (*i.e.*, the investment is recommended compared to the potential loss) if it results in a number higher than one.

The ROSI considers the ALE, the mitigation rate, and the investment cost to assess if a solution is worth the investment or not. For that, the SLE and the ARO have to be considered, which describe the estimated cost of a security incident (*e.g.*, a data breach or a DDoS attack in the company) and the

estimated annual rate of an incident occurrence (*i.e.*, based on the historical data and threat modeling, which are the probability of being attacked). This information has to be investigated in Phases A, B, and C of the methodology. Furthermore, the cost of the investment and the possible proactive mitigation (*i.e.*, how much of the attacks can be avoided or mitigated by implementing the solution) have to be mapped during Phases C and D.

Finally, an overview of all costs, optimal investments, and understanding of investments versus economic impacts in case of no mitigation can be used to deploy the cybersecurity strategy. It might also be possible to return to one phase if the costs are high and new requirements have to be defined. In the last phase of the methodology (**Phase E**), the company already knows different artifacts and information provided by early phases to manage the execution and deployment of the cybersecurity strategy with a clear view of its risks, costs, goals, and success rate. In the light of this information, the company can define requirements for an external technical consultant or schedule different technical tasks required for the effective deployment and configuration of the new cybersecurity strategy adopted by the company. Also, operation and maintenance tasks have to be mapped within this last step in order to reach not only a proper protection level but also an efficient plan to manage and operate the entire set of countermeasures, which might require additional training, employees, and equipment that fits the budget as previously defined in the cost of the cybersecurity strategy.

This methodology shows a path for companies to start planning and investing in cybersecurity. However, many of these steps are not trivial, since most SMEs do not have this amount of information or solutions to support them in all of these steps. In order to address this issue, a framework architecture has been proposed to describe the main different layers and components required to be implemented by solutions that want to support these relevant steps in an integrated, simplified, and effective way.

4.2 Framework Architecture

The framework is an important contribution provided by the *CyberTEA* approach to help decision-makers and software developers understand the requirements, information, and relationships between components, when developing cybersecurity planning and investment solutions. Also, the framework maps essential components analyzed, designed, and implemented by the *CyberTEA* to provide data, information, and elements that enable companies to perform all steps defined in the methodology explained above (*cf.* Figure 4.1). It is worth mentioning that the framework is not exhaustive and is defined to be modular. This modular architecture allows for integrating solutions already placed in the real-world and those under research once a company or a specific model can

require additional steps or information. Therefore, the framework maps and implements all methodology phases into layers and components while also providing a concise path for novel solutions to emerge to support cybersecurity planning and investments.

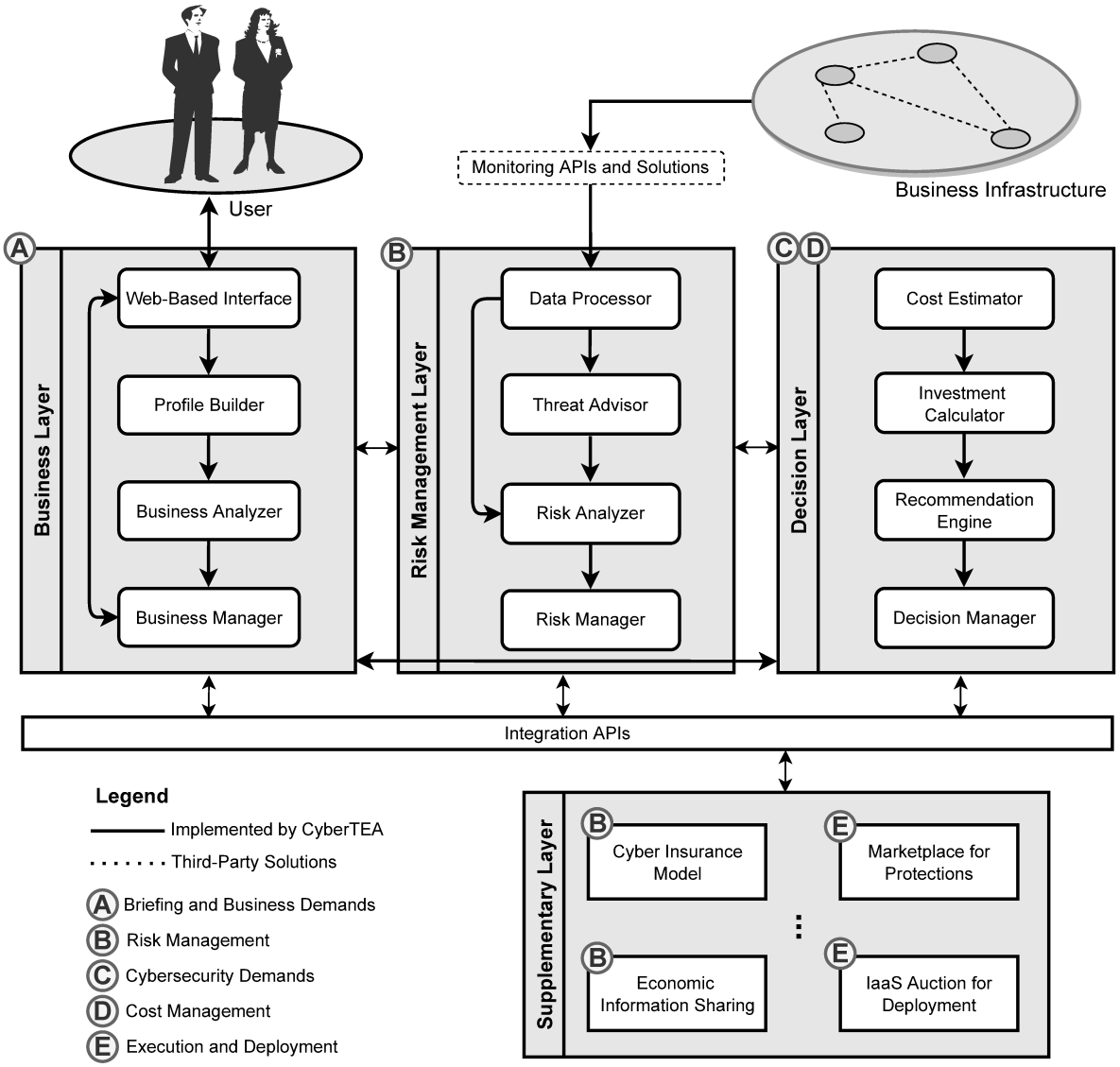


Figure 4.2: The Architecture of the Framework Defined by the *CyberTEA* Approach

The framework, proposed as part of the *CyberTEA* approach, is divided into four layers, as shown in Figure 4.2. The **Business Layer (BL)** represents the interface between the user and the different components, also being in charge of receiving inputs regarding the business information to be used by the other layers and components. Next, the **Risk Management Layer (RML)** focuses on the

steps required for understanding and analysis of threats and risks. For that, the RML is in charge of obtaining data from monitors and inputs from the business (*e.g.*, from CISO or external advisors) to perform different tasks required to understand better and quantify the risks. Finally, the **Decision Layer (DL)** focuses on the overall cost management and selection of adequate protection. Furthermore, a **Supplementary Layer (SL)** allows for the implementation of external solutions that can support specific tasks performed by each layer or provide additional features, *e.g.*, when cyber insurance models can be considered after analyzing risks and marketplace for protections can be used to find protections. The communication between the BL, RML, and DL layers happens, respectively, via the Business Manager, Risk Manager, and Decision Manager. For the SL, integration APIs are exposed to establish the communication, in a standardized way (*e.g.*, based on RESTful APIs and JSON syntax), between external solutions and the framework components.

Databases are not explicitly highlighted in the framework due to decisions regarding the visual representation of the framework. However, the Business, Risk, and Decision Manager components might implement their own databases, whenever needed, to store and retrieve data/information.

4.2.1 Business Layer (BL)

The BL comprises steps mapped in Phase A (*i.e.*, Business and Demands) of the methodology proposed. Therefore, this layer is in charge of handling business information to understand better the different characteristics that define the business. For that, a *Web-based Interface* is available, where users can interact with a solution. A *Profile Builder* also has to be provided in this layer in order to collect data from the user/company (*e.g.*, revenue, sector, infrastructure, technologies being used, organization of the company, and the number of employees), store this data in a structured way, and feed the other components and layer whenever required. The *Profile Builder* can be extended according to the demands, thus, being possible to add new fields in the *Web-based Interface* to user's fill regarding the business or implement automated algorithms for collecting the required data.

Next, the *Business Analyzer* is in charge of processing the data available, refining, and obtaining insightful knowledge regarding the business. For example, based on the sector, business processes, technologies being used, protections available, and level of training of employees in a company, the *Business Analyzer* can infer the maturity of the business, understanding of past attacks history, and also classify the personnel expertise. The other layers can then use this information, especially during risk management. Finally, the *Business Manager* stores and manage all data and information available, answering requests from other layers with adequate information. Thus, the *Business Manager* works as a data manager and also an interface for communication between layers via other managers (*i.e.*, Risk Manager, Decision Manager, and Integration APIs).

4.2.2 Risk Management Layer (RML)

The RML implements the components used to understand and analyze risks, thus, processing data, modeling threats, and analyzing the likelihood of threats. This layer is related to Phase B of the methodology, where the steps related to the threat modeling, analysis of risks, measure of impacts, and risk-sharing are placed.

The RML has a *Data Processor* that receives data from different sources (*e.g.*, Security Information and Event Management (SIEM) systems, network monitors, and manual inputs from human operators) in order to organize that for further analysis of risks. Thus, with this data at hand, the *Risk Analyzer* applies different techniques, models, and solutions to identify, estimate, and evaluate the risk of cyberattacks and their impacts (*e.g.*, business disruption and potential economic losses). The *Threat Advisor* allows for the discovery and mapping of threats within the company, which can be done by using data coming from the *Data Processor* or the BS via *Business Manager*.

The *Risk Manager* then is in charge of handling the threat models defined and the different information related to risks, such as the likelihood of an attack happening, the successful rate of attacks, and the potential of damages. The other layers can have access to this information if requested, especially during the DL, since the risks are critical for defining the cybersecurity strategy. Also, supplementary services can use the information provided by this layer for solutions that provide, for example, cyber insurance models and information sharing approaches.

4.2.3 Decision Layer (DL)

This layer implements the components required to execute tasks that are part of the Phases C and D of the proposed methodology. Therefore, the DL has to perform tasks to support the definition of the requirements for a cybersecurity strategy, the costs, and the most appropriate protections.

As a first step, the *Cost Estimator* has to allow for the estimation of the costs to implement a given cybersecurity strategy, taking into account the business profile, risks, and potential impacts of cyberattacks. Next, the *Investment Calculator* is placed to determine which is the optimal investment and how to address all requirements with the optimal investment. This optimal investment can be calculated to achieve the best combination of the costs of investing in protections and the loss if not investments in protections are not placed. Also, the price of protection, mitigation rates, and business profile has to be considered for mapping protection candidates.

Finally, the *Recommendation Engine* recommends, from a list of protection candidates, which fits better to the cybersecurity requirements and business profile. This is performed considering the budget available (*i.e.*, optimal investment) as well as the protection candidates received from the *Invest-*

ment Calculator. The *Decision Manager* is responsible for storing and managing the decisions and also sending/receiving information to/from the other layers.

4.2.4 Supplementary Layer (SL)

The Supplementary Layer is defined to map supplementary solutions that do not fit in one of the above layers but offer features and information that are highly relevant for cybersecurity planning and investment tasks. These solutions can support any of the phases described by the methodology.

For instance, cyber insurance models have a key role in risk-sharing, as mapped in Phase B of the methodology. Cyber insurance can be considered for a company that understands or even assumes risks but wants coverage to receive a certain amount of money from cyber insurance companies whenever a cyberattack happens. This helps to amortize the economic impacts by paying a yearly premium for the cyber insurers' companies. Also, information sharing is crucial for the excellent planning of cybersecurity, which can also be achieved by sharing with partners data from monitors and information regarding (economic) impacts of past cyberattacks.

Also, solutions available on the SL can be used to support different tasks of the Phase E (*i.e.*, Execution and Deployment) of the methodology. Examples of these solutions can be a marketplace that allows users to compare and acquire protections. Also, these marketplaces can automate the deployment of the contracted solutions and monitor key performance metrics a contracted protection (*e.g.*, mitigation rate and Service Level Agreement (SLA) monitoring).

Furthermore, solutions that offer Infrastructure-as-a-Service (IaaS) can also be an ally to companies that do not have the on-premises infrastructure to run the required protections, thus, needing to find an adequate provider that provides required sources at the best price. Many additional solutions can be placed in this layer. These examples show how cybersecurity planning and investment are complex tasks that can evolve in different ways, supported by various solutions.

4.3 Empowering ML for Risk Assessment in Businesses

Besides understanding the threat landscape and the different types of attacks affecting companies, it is important to understand the likelihood of these threats and their possible impacts. Despite the several risk assessment standards and approaches available (*e.g.*, ISO 27005, NIST SP 800-30, TOGAF Security Guide, and SEConomy), organizations still find this activity challenging and are often confronted with a massive volume of unstructured data, which hinders the identification of risks. In this case, traditional techniques may not provide valuable insights and cannot perform an adequate risk assessment due to the amount of data to be processed.

Studies on possible applications of ML algorithms [119, 211] have highlighted their ability to process large amounts of structured/unstructured data, extract valuable patterns, learn from historically collected records, and make accurate predictions. Given the characteristics of learning and identifying patterns, ML-based solutions can be an ally for the qualitative analysis of potential risks and threats within a company, thus, helping in risk assessment and planning of cybersecurity. For example, ML algorithms can be used to correlate specific characteristics and information (*e.g.*, number of employees, sector, cybersecurity strategies, and underlying infrastructure) of a company to associate it with a higher or lower risk to have a breach in its cybersecurity. In the field of cybersecurity, research has tended to focus mainly on leveraging ML to detect various types of cyberattacks and recognize breaches [211]. However, there are still opportunities for ML-based cybersecurity risk assessment and prediction solutions based on business demands and characteristics, especially for early stages assessment before cybersecurity planning.

The **SecRiskAI** solution [92] was designed and developed to address the lack of solutions for risk assessment and predicting threats in a straightforward and simplified way. SecRiskAI implements four ML algorithms for risk assessment and builds models to predict general and specific threats (*e.g.*, the risk of a successful DDoS or phishing attack). Relevant information and features for the ML-based risk assessment are also presented and described. A Web-based user interface is also part of SecRiskAI to simplify understanding the business risks in a user-friendly and more intuitive way. Therefore, the SecRiskAI implements components that fit the BL (*e.g.*, Web-based Interface, Profile Builder, and Business Analyzer) and the RML (*i.e.*, Risk Analyzer).

The SecRiskAI solution focuses on predicting the risks of companies to support the planning and deployment of effective cybersecurity strategies, which can avoid technical problems and reduce potential financial losses resulting from cyberattacks. For a qualitative cybersecurity risk assessment and understanding of the likelihood of attacks in companies, SecRiskAI provides an approach based on three main steps: *(i)* datasets definition and data generation due to the lack of real data available, *(ii)* ML model creation, and *(iii)* the risk prediction. Different data sources and features are determined, and ML algorithms are employed in different situations and constraints (*e.g.*, limited amount of information and size of datasets available). Also, it is critical for companies, especially those without in-house expertise (*e.g.*, SMEs and micro enterprises), to have a straightforward approach. Therefore, SecRiskAI integrates the entire risk prediction process in a user-friendly and intuitive Web-based Interface. The source code of SecRiskAI and a fully operational prototype is publicly available at [56], including all components, training datasets, and models.

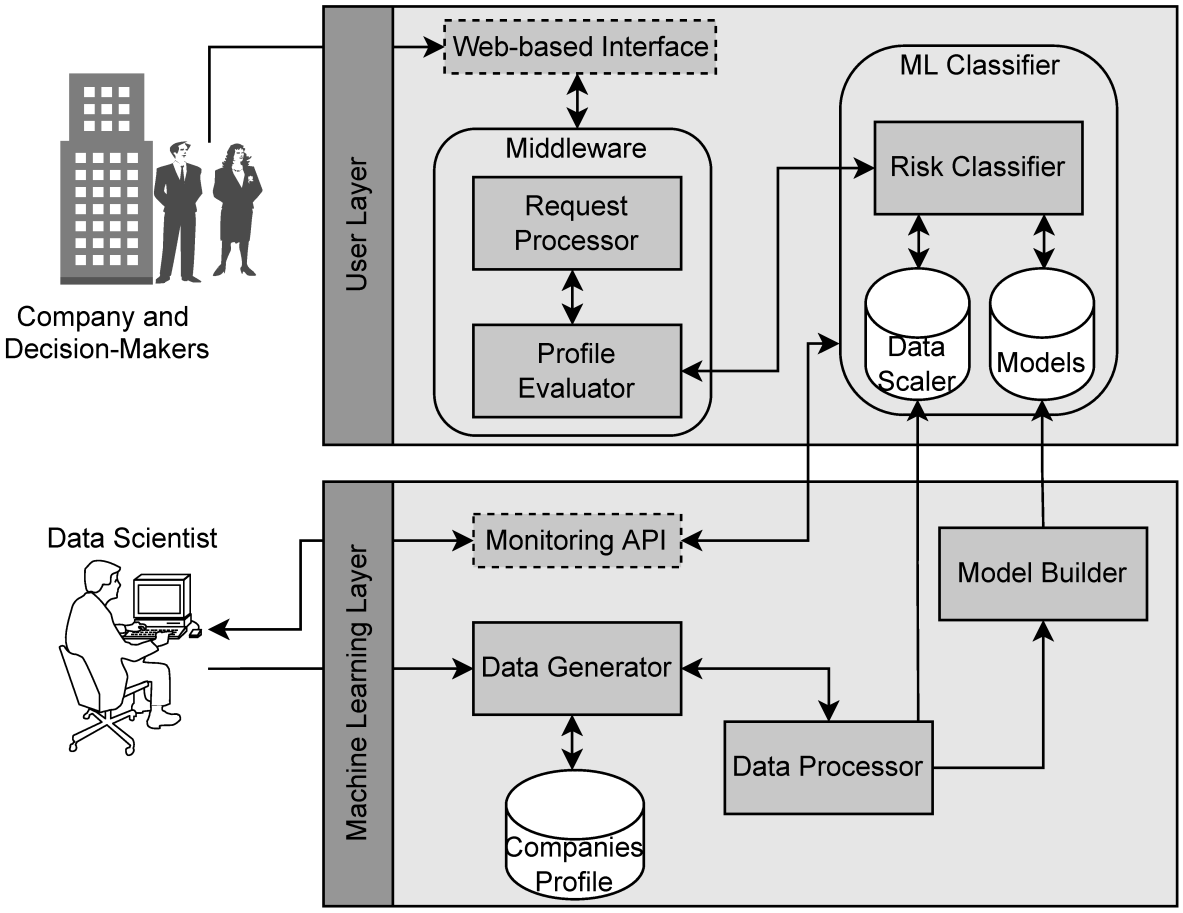


Figure 4.3: SecRiskAI's Architecture Overview

Figure 4.3 introduces the SecRiskAI architecture and stakeholders. First, the user (*i.e.*, companies and decision-makers) accesses the dashboard. The Web-based interface is designed to provide visibility of business-related risk indicators and, at the same time, increase productivity and better forecasting of important aspects related to business security. Moreover, the user can change contextual information through the Web-based interface, such as business value, operational region, number of employees, level of employee training, and cybersecurity budget.

The Middleware module performs the task of using the data provided by the user (*i.e.*, business profile and characteristics) to make risk predictions. As soon as the request sent by the Web-based Interface is received, the *Request Processor* handles it and forwards the information to the *Profile Evaluator*, which is in charge of contacting the ML models and evaluating the prediction response. The risk prediction starts with a request to the *Risk Classifier*, which is a prediction service included in the ML Classifier module and is essentially used to expose the trained ML models through an Application Programming Interface (API). Additionally, the ML Classifier module also stores the trained

ML models, as well as the *Data Scalers*, used to normalize the input data and increase prediction accuracy.

The process of training and validating the ML models occurs in the Machine Learning (ML) Layer and is usually carried out by data scientists/experts knowing about the business and respective sector. This can also be part of consultancy services provided by third parties. The *Data Generator* component is used to initialize the synthetic data generation process. This data generation is a Python script implemented to generate synthetic labeled datasets based on characteristics of businesses (*cf.* Table 4.1), according to the requirements of the ML algorithms. Next, the data is processed (*i.e.*, Data Processor) and used by the *Model Builder* for training, validating, testing, and building the models. Lastly, a Monitoring API is available to check the status of the deployed models, retrieve model-specific metadata (*e.g.*, version, creation time, accuracy), and other metrics about the prediction service (*e.g.*, request duration in seconds and status).

Once the opportunities of applying ML to cybersecurity risk assessment are defined and well-understood, the process of designing and developing an ML workflow starts. The most critical stage is data collection/gathering. Usually, data is collected from sensors or other sources and stored for further processing in this phase. However, in the field of cybersecurity risk assessment, companies either do not disclose any information at all or, in some cases, publish various reports that are often incomplete and difficult to extract meaningful results from. A synthetic data generator approach was designed and implemented to overcome this limitation and feed SecRiskAI with data for the algorithms' training process.

An exploratory analysis was conducted to determine relevant parameters that can increase or decrease the risk of a company. This analysis consists of three main sources: *(i)* public reports from different agencies and companies, such as those from ENISA and European Digital SME Alliance, *(ii)* scientific works indexed by well-known digital repositories (*e.g.*, IEEEXplore, ACM Digital Library, and Google Scholar) that covers the likelihood, severity, and effects of cybersecurity issues in SMEs mostly, and *(iii)* interviews with cybersecurity experts and SMEs owners to understand their reality and information asymmetry challenges. It is important to note that this is not an exhaustive analysis but gives indications of the most common characteristics of companies that can be related to the risks of being affected by a cyberattack. Also, the cyberattacks investigated are restricted to phishing, ransomware, and DDoS attacks. After such an exploratory analysis of different cyberattacks and corresponding companies' contextual information, the following parameters to be used as a basis for this work were identified:

- **Revenue.** Referred to the income generated from normal business activities and operations, and in most cases, is also used to classify businesses by providing a scale for determining their sizes.

- **Cybersecurity Investments.** Normally, businesses already have cybersecurity investment strategies in place to ensure a proper level of defense. This kind of information needs to be taken into consideration during the cybersecurity risk assessment, as it may impact the likelihood of being targeted by a cyberattack.

- **Number of Employees and Training Level.** Similar to the revenue, information regarding the actual number of employees in a company as well as the corresponding cybersecurity training level (*e.g.*, cybersecurity basic knowledge and phishing training) represent essential contextual information required for assessing possible cyber-risks. The employee training level is measured as *Low*, *Medium* and
textitHigh.

- **Successful/Failed Cyberattacks.** This parameter indicates the number of cyberattacks that the company has already experienced. This includes different attacks (*e.g.*, DDoS and phishing) that have targeted the organization's infrastructure and resulted in either a financial loss or reputation damage. Failed attempts are also taken into consideration.

- **Known Vulnerabilities.** For an effective and comprehensive risk assessment, it is essential to report any known vulnerabilities of the infrastructure. Vulnerability management is usually a key responsibility of the company's IT security team. This phase usually involves assessing and reporting any security vulnerability present in the organization's systems. There are a variety of comprehensive tools used for vulnerability scanning, such as `nmap`, Metasploit, and OWASP. The total number of known vulnerabilities is currently defined during the synthetic generation process.

- **External Cybersecurity Advisor.** In order to further strengthen their cyber resilience (*i.e.*, the ability to prepare for, respond to, and recover from cyberattacks), businesses are encouraged to hire an external Cybersecurity Advisor (CSA). Furthermore, CSAs provide various services, such as cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, incident coordination, and support. During the synthetic data generation phase, a binary value will be generated (either *Yes* or *No*).

- **Risk.** The last parameter represents the value of the qualitative risk assessment based on the previously generated parameters. Since the synthetic data generation process is designed to generate historical records of companies operating in comparable industries, the value of the risk column may be derived from past formal or tailored qualitative risk assessment techniques. The generated risk can assume one of the following values: *Low*, *Medium* and *High*.

The information mentioned above was generated based on some assumptions made. First, upper/lower boundaries for each column were specified so that each generated value would effectively lie in the defined range. Table 4.1 provides an overview of the determined boundaries as well as examples of values for each generated information. These attributes are also used as input to map the risks according to what is proposed by SecRiskAI in Equation 4.1.

Not all of this information must be available within the company, especially considering SMEs that do not have in-house expertise. This is highlighted in the last column of Table 4.1. Therefore, the Failed Attacks and Known Vulnerabilities are optional for the SecRiskAI. Although it is essential to know these metrics for an accurate risk assessment, it is possible to address the lack of this information by understanding the correlation between successful attacks and other statistics available (*e.g.*, economic losses, number of attacks per sector, and trends) from companies from the same sector. This can be adjusted by adding, in the training dataset, labeled data that represents this behavior or trend.

$$
\begin{aligned}
i_r &= \frac{invested\_amount}{business\_value} \\
e &= \frac{nr\_employees}{tot\_empl} * map(employees\_training) \\
att_r &= \frac{succ\_attacks}{max\_attacks} \\
v_r &= \frac{known\_vuln}{max\_known\_vuln} \\
adv_i &= map(external\_adv) \\
map(x) &= \begin{cases} 0, & \text{if } x = Low \\ 1, & \text{if } x = Medium \\ 2, & \text{if } x = High \end{cases}
\end{aligned}
\tag{4.1}
$$

$$
computed\_risk = i_r + e + adv_i - att_r - v_r \tag{4.2}
$$

The risk is computed based on the generated attributes shown in Table 4.1 using the generalized Equation 4.2. For the supervised learning process, the dataset must be labeled. As a result, the *computed_risk* output is mapped to either a Low, Medium, or High class. A manual labeling process would be too expensive, since the generated dataset would include thousands of records. Therefore, based on the numeric value of *computed_risk*, a mapping range is defined. This means that each *computed_risk* value is labeled using the range as specified at the end of Equation 4.1.

Table 4.1: Overview of the Generated Dataset Attributes

Information	ID	Range	Priority
Revenue	`business_value`	0 to 5,000,000	Required
Cybersecurity Investment	`invested_amount`	0-30% * Revenue	Required
Successful Attacks	`succ_attack`	0 to 50	Required
Failed Attacks	`fail_attack`	0 to 50	Optional
Number of Employees	`nr_employees`	30 to 10,000	Required
Employee Training	`employees_training`	Low, Medium, or High	Required
Known Vulnerabilities	`known_vuln`	0 to 10	Optional
External Cybersecurity Advisor	`external_adv`	Yes or No	Required
Risk	`risk`	Low, Medium, or High	-

Figure 4.4 summarizes the ML workflow implemented by SecRiskAI. Once a sufficient amount of data has been successfully generated, the processing phase starts. The ML algorithms require an initial processing step as they cannot work with raw data. In the first step, any categorical variable present in the dataset is handled. Precisely, variables such as employee training level and external cybersecurity advisor are mapped into numerical values using the one-hot technique, which is easier for the ML process.

A further normalization may be necessary, depending on the selected ML algorithm. Normalization is the process of scaling data into a range of $[0, 1]$. Some ML algorithms are susceptible to features with varying degrees of magnitude, range, and units. The dataset generated for SecRiskAI includes different features, such as revenue and the number of employees with different ranges. Training sensitive models on unscaled data may lead to lower performance and accuracy. Therefore, a normalization technique known as Min-Max scaling is used as defined by Equation 4.3. The Min-Max normalization technique is applied to the entire dataset but only to features (*i.e.*, every column except the risk), which contains the three output classes based on which future predictions will be made.

$$x_{scaled} = \frac{x - min(x)}{max(x) - min(x)} \tag{4.3}$$

The processing phase then involves splitting the dataset into a training, validation, and test set. After successful training and validation, the final model is subjected to extensive testing. During this phase, the final model is usually evaluated using previously unseen data (*i.e.*, test set generated using the implemented synthetic data generator), also called the holdout set. The size of each dataset

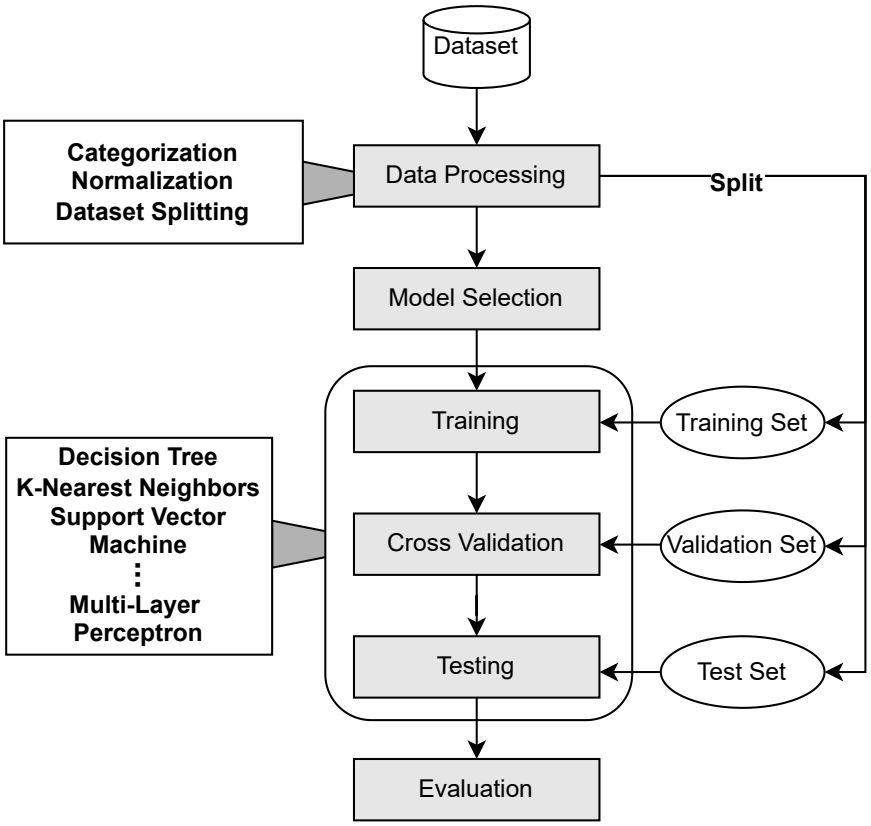


Figure 4.4: ML Workflow Implemented by SecRiskAI

used for training and testing is in the range of 5,000 to 50,000 entries. The nuances of the different algorithms implemented by SecRiskAI are described below.

4.3.1 Multi-Class Classification Algorithms

In ML, Multi-Class Classification algorithms (MCC) are developed to solve the problems of classifying instances into one of three or more output classes. Popular MCC algorithms are chosen for qualitative cybersecurity risk assessments in the model selection phase. The main goal is to design and develop ML models that, based on contextual information, can make accurate qualitative risk assessment predictions and further monitor the organization's infrastructure by providing continuous assessment based on input data.

Decison Tree (DT) Algorithm

DT is a Supervised Learning (SuL) algorithm for the classification used in the proposed solution. This technique essentially looks at the feature values of the input dataset and categorizes them according

to a specific parameter, also known as information gain. Algorithm 1 shows the pseudo-code of the procedure for implementing the decision tree algorithm.

Algorithm 1: Decision Tree (DT)

input: D, dataset containing organization's contextual information
  Tree = {}
  for all attributes $\in D$ **do**
    Find the attribute which best divides D using information gain
    $X_{best} \leftarrow$ feature column with the highest information gain
  end for
  $Tree \leftarrow$ Create a Decision Node that divides the dataset on X_{best}
  $D_{sub} \leftarrow$ sub-datasets from D splitted on X_{best}
  for all D_{sub} **do**
    $Tree_{sub} \leftarrow \text{DTree}(D_{sub})$
    Add $Tree_{sub}$ to the corresponding branch of the tree
  end for
  return Tree

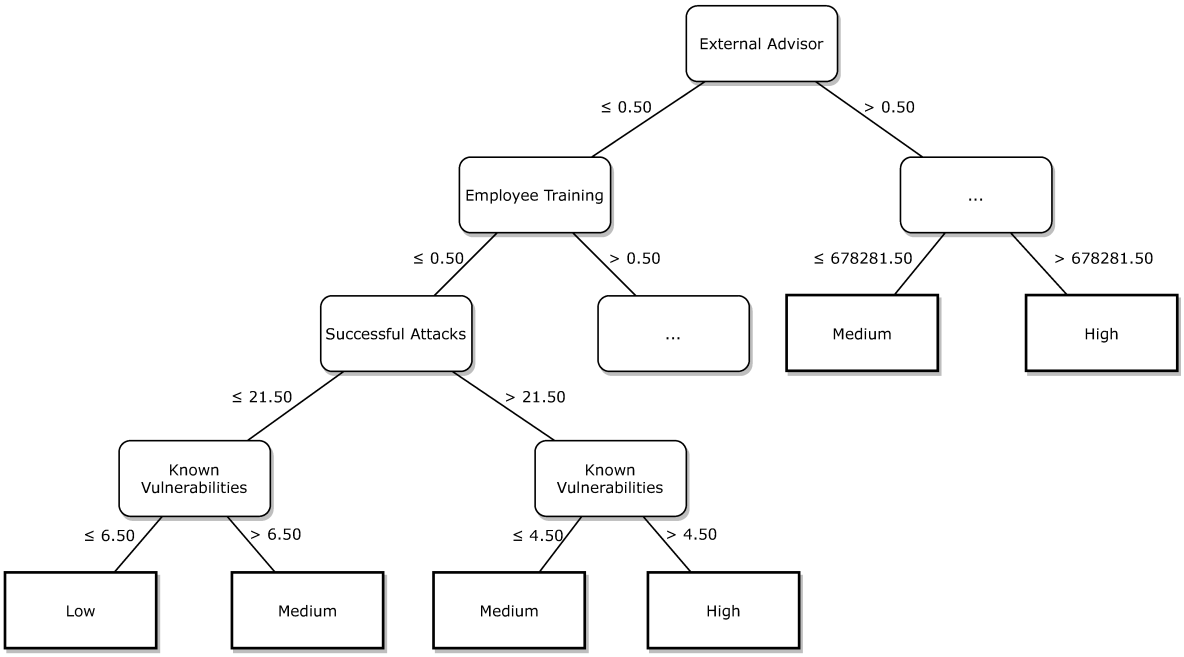


Figure 4.5: DT Trained using the Data Generated by the SecRiskAI

The goal is to find, in a given dataset D, the feature having the highest information gain, which will, in turn, serve as a decision node of the tree. Next, the algorithm splits the dataset on the identified

decision node and searches the sub-datasets. A tree structure is then constructed, with each node representing a feature column and the leaves indicating the output class.

Besides being an easy-to-use and straightforward classification technique, this algorithm can be trained on historical data without requiring extensive data pre-processing. Compared to other classification algorithms used in this approach, the decision tree requires less effort for data preparation, and the normalization step is not required. The resulting model is therefore easy to understand for both technical and non-technical stakeholders. Figure 4.5 shows the DT algorithm trained with the datasets generated by SecRiskAi. In order to make a prediction using the DT, a new sample i would traverse the tree based on each feature value, and the resulting leaf value would be the output class.

K-Nearest Neighbors (KNN) Algorithm

KNN is usually referred to as an instance-based classifier as the main idea behind this technique is to memorize the input dataset to make future predictions. As shown in the Algorithm 2, KNN requires three input parameters: a dataset D containing the historical information is given, a chosen number of neighbors k and x, a sample that is to be classified. The algorithm then proceeds to compute the distance between x and every record contained in D. Next, the computed distances are sorted in ascending order and k closest samples, also known as *neighbors*, to x are selected. Finally, the predicted class of x ($Class_x$) is based on the similarity with the neighbors, meaning that x is labeled following a majority voting of classes among the neighbors.

Algorithm 2: K-Nearest Neighbors (KNN)

input: D, dataset containing organization's contextual information
k, number of nearest neighbors
x, unclassified sample
for all $r \in D$ **do**
Compute distance between r and x
end for
Neighbors $\leftarrow$ Sort computed distances and select k closest samples to x
$Class_x \leftarrow$ majority output class based on *Neighbors*
return $Class_x$

In essence, KNN calculates the probability of a sample x belonging to a specific class based on neighbors' observations. Compared to the DT, KNN requires more data pre-processing. On the other hand, the training phase is faster, and new training data can be seamlessly added without reconstructing the model. Suppose that the representation of the KNN classification with k equal to

seven and x being a new sample to classify. In this example, only two dimensions are considered (*i.e.*, cybersecurity investment(s) and a specific number of employees). Figure 4.6 shows a visual representation of the implemented KNN. Once the k closest neighbors to x are identified, the predicted class of x is Low if the majority of the neighbors belong to the Low class.

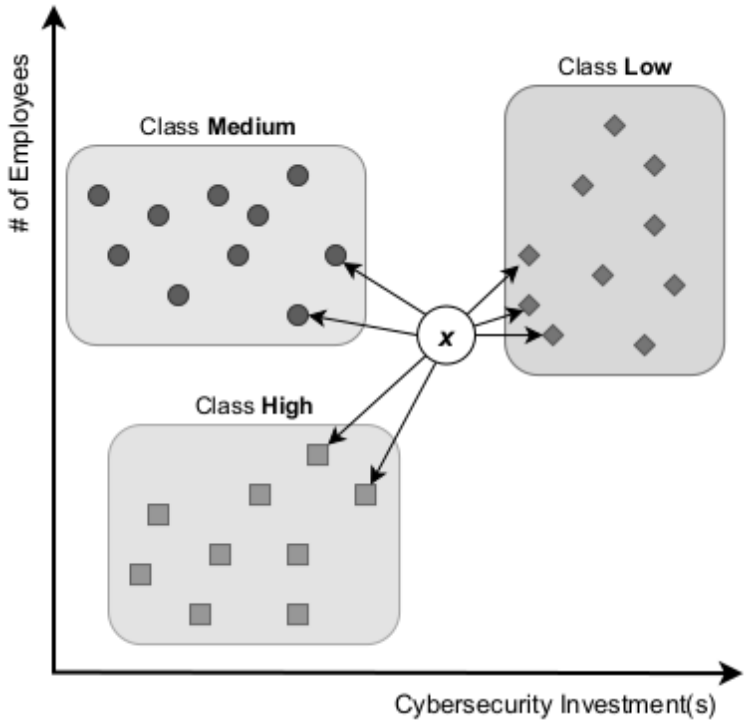


Figure 4.6: KNN Visualization, where $k = 7$

Support Vector Machine (SVM) Algorithm

The SVM is the third SuL classification algorithm implemented in SecRiskAI. In contrast with DT and KNN, SVM uses a line or hyperplane to separate input data into classes. Moreover, SVM is computationally less expensive than KNN but does not natively support MCC algorithms. To achieve that, a *One-vs-Rest* strategy is followed. First, the multi-class dataset is broken down into multiple binary classification problems as highlighted in Figure 4.7. In this case, the following classification problems are identified:

- High vs {Low, Medium} (Figure 4.7 - Step 1)

- Medium vs {Low, High} (Figure 4.7 - Step 2)
- Low vs {Medium, High} (Figure 4.7 - Step 3)

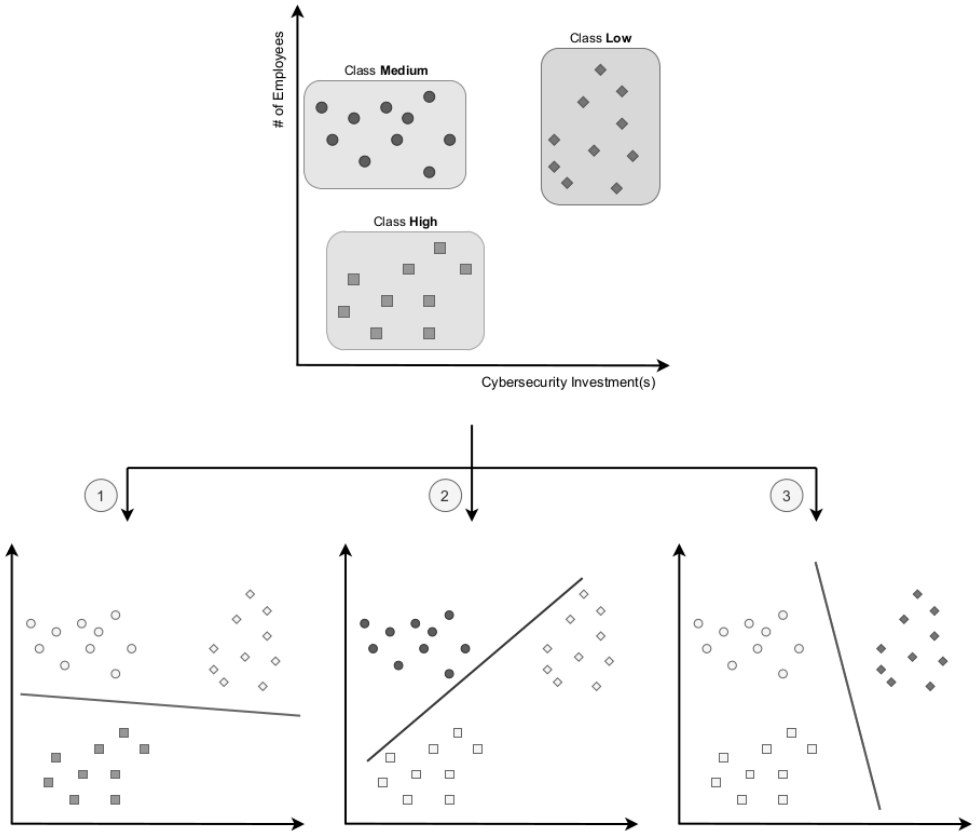


Figure 4.7: SVM Visualization

Next, a binary classifier is trained on each binary classification problem. It can predict a class probability (P_{class}), *i.e.*, the probability of an object belonging to a specific class. After the training phase, the binary classifiers return the probability of a sample being labeled as Low (P_{Low}), Medium (P_{Medium}), and High (P_{High}). Finally, the model that can predict the class of an unclassified sample x with the highest confidence is chosen and is represented in Equation 4.4:

$$Class_x = argmax(P_{Low}, P_{Medium}, P_{High}) \tag{4.4}$$

When dealing with larger datasets and n output classes, SVM would require the creation of n binary classifiers for each class, resulting in high computational costs. SVM also suffers from performance

issues, when confronted with overlapping classes, *i.e.*, data points are not well separated. On the other hand, SVM is a very flexible algorithm and allows the specification of a kernel function that can be linear (*cf.* Figure 4.7) but can also be of different types, such as non-linear, polynomial, radial basis function, and sigmoid to solve many non-linear problems.

Multi-Layer Perceptron (MLP) Algorithm

MPL using the backpropagation algorithm is also explored in SecRiskAI. More specifically, MLP is a class of feed-forward ANN. Figure 4.8 gives a visual representation of the MLP model implemented for SecRiskAI. Each node in the input layer corresponds to a specific feature of the generated dataset. Moreover, the MLP model has a total number of two hidden layers having five neurons each. Choosing the best parameters for an ANN is a very challenging task, as there are no clear rules, and it depends on the complexity of the underlying problem. The decision was based on the general guidelines available in the literature and extensive exploratory research and testing. On the other hand, the output layer was defined based on the output classes of the model (*i.e.*, Low, Medium, and High). Therefore, it consists of three neurons representing each possible classification state.

During the training phase, the MLP uses a technique called *backpropagation*. An ANN propagates the input data forward through the neurons towards the output layer, where the prediction occurs. The backpropagation algorithm refers to propagating the information about the prediction error backward from the output layer throughout the entire network, intending to adjust the weights and improve accuracy. Figure 4.8 also gives an example of a backpropagation mechanism initiated as soon as the original label (Medium) and predicted class (Low) differ. The computed error/loss is calculated, and lastly is used to adjust the weights in the hidden layers.

Once the dataset is generated and the required ML algorithms are chosen, the training phase is initiated. Examples of the training datasets and overall process are available at [56]. First, the dataset is split following the 80-20 train-test strategy. Next, the process of choosing a set of optimal hyperparameters, also called hyperparameter optimization, takes place. The main idea is to use grid search to test every combination from a pre-defined list of parameter values (*cf.* Table 4.1) required by the ML algorithm to build the model. Subsequently, the performance of each model is evaluated with the help of a 5-fold Cross-Validation strategy. The model with the highest accuracy is selected and tested with unseen data (*i.e.*, the test set). Lastly, the entire process is applied to each ML algorithm.

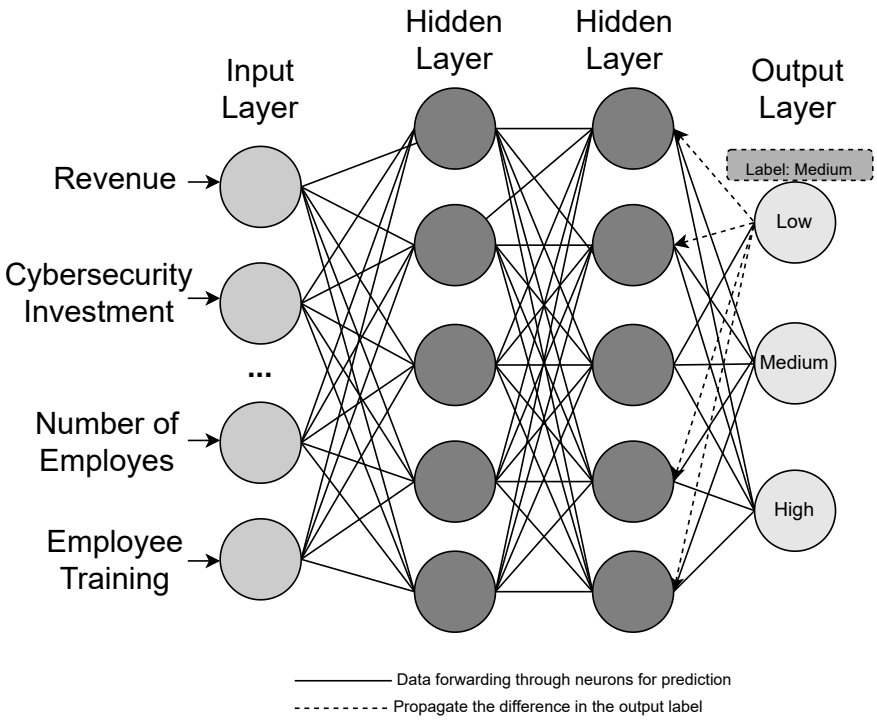


Figure 4.8: Examples of a Visual Representation of the MLP Implemented by SecRiskAI

4.3.2 SecRiskAI's Implementation

All of the ML algorithms (*i.e.*, ML Classifier) explained above were implemented using the *BentoML*, a flexible, high-performance framework written in Python for serving, managing, and deploying ML models. In the SecRiskAI, the ML Classifier makes use of the full potential of BentoML for deploying and serving trained ML models efficiently and effectively. The frontend of the SecRiskAI is implemented using ReactJS, a popular and widely adopted JavaScript library for building user-friendly interfaces. For this particular prototype, *TypeScript*, a well-known typed super-set of JavaScript, was used. This decision was based on the benefits that TypeScript offers over plain JavaScript, such as static typing, readability, and improved maintainability. Finally, the backend (*i.e.*, Middleware) was developed using *Nest.js*, a progressive framework for building efficient, reliable, and scalable server-side applications.

Figure 4.9 shows the main page of the SecRiskAI, with all of the information regarding the company and the risk assessment placed, including the integration of a recommender of protections called MENTOR (*cf.* Section 4.7). In the first row, the Web-based interface contains multiple tabs, including contextual information, such as business value, employees, successful/failed past cyber-attacks,

and known vulnerabilities. Additionally, the second row gives an overview of general information (*e.g.*, company name, industry, and operational region), the cybersecurity risk assessment predictions, and the desired protection services parameters used for the recommendation process.

As soon as the user accesses the interface, the cybersecurity risk predictions are retrieved through a POST request sent to the Middleware. SecRiskAI then provides an overall cyberattack risk prediction, where the different ML model prediction outcomes are compared and predictions for specific cyberattacks. It is important to note that, SecRiskAI is designed to be extensible. Therefore, additional ML models can be easily integrated with the current ML Classifier to cover specific cyberattacks. The prediction result is shown in the *Attack Risk Prediction* tab.

This prototype also implements a table containing the recommended list of protection services most suitable for the specified profile. Each row gives an overview of protections with a short description for each. The Middleware retrieved this list directly from MENTOR via Restful API. Moreover, updating the service-specific parameters can trigger a new recommendation process if the user is not satisfied with the recommended services. These parameters can also be configured by clicking on the *Configure* button.

4.4 Conversational Agents to Support Risk Management

As discussed in Chapter 2, from a human-centric perspective, simplifying the cybersecurity decision-making process requires clear and straightforward approaches. It is essential to promote novel approaches that present cybersecurity technical information in an intuitive and user-friendly way, allowing less-skilled personnel to make informed decisions while maintaining a proper level of protection for their businesses. SMEs can benefit from adopting faster and cheaper cybersecurity strategies, *e.g.*, by minimizing human experts' needs while reducing costs by efficiently investing protections.

Conversational agents (*i.e.*, chatbots) [191] have been recently highlighted as an ally to enhance business' cybersecurity adoption by sharing network and security information with non-technical staff [51] [25]. Advances in NLP [134] — driven by novel ML techniques [198] — led to conversational interfaces capable of extracting meaningful information and simplifying interactions between humans and machines. Compared to command-lines and technical dashboards, chatbots *(i)* provide a more direct interaction using natural language, *(ii)* enable faster decision-making, and *(iii)* speed-up complex processes. However, even with those benefits, the employment of chatbots in SME cybersecurity is still scarce and limited to particular scenarios. Hence, the current state-of-the-art neither

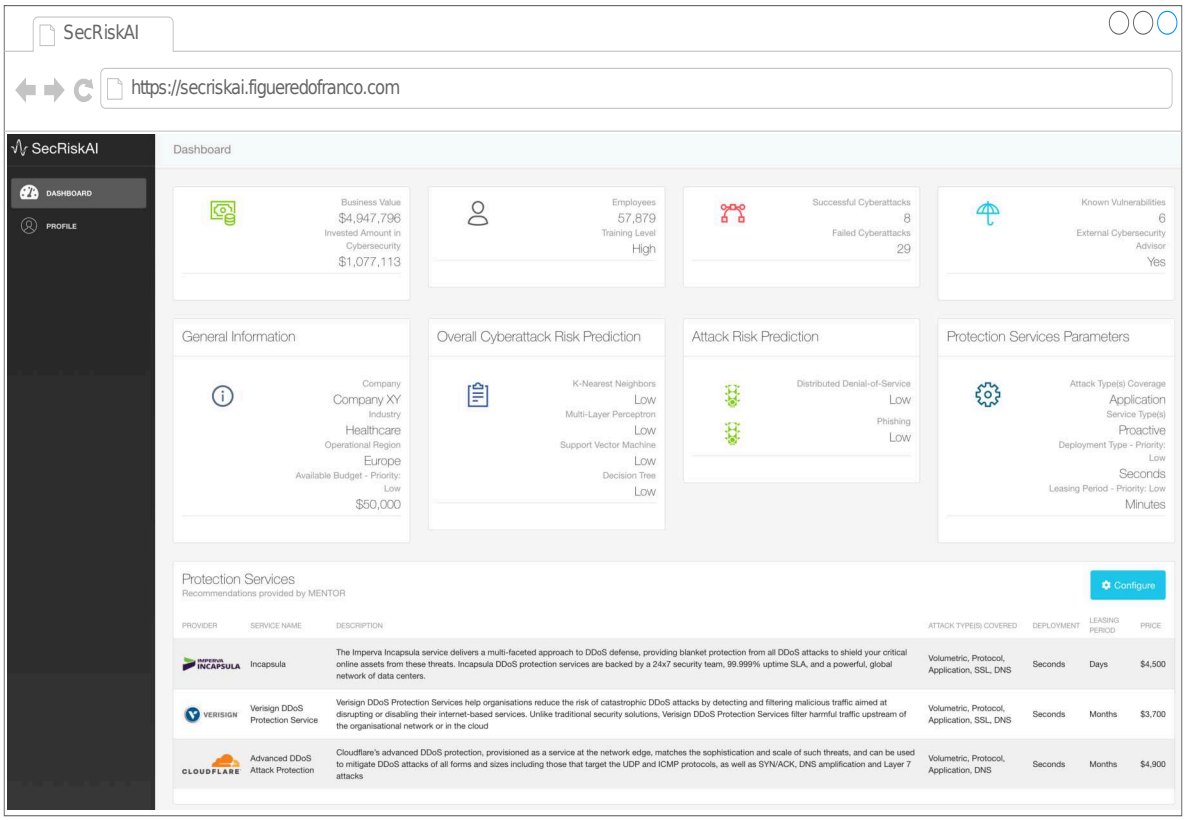


Figure 4.9: Main Screen of the SecRiskAI

fully covers the demands of SMEs nor considers barriers to cybersecurity adoption in SMEs (*e.g.*, awareness of standards, limited internal knowledge, and lack of clear implementation guidelines).

To address this lack of solutions and shed light on opportunities in this field, it was designed and implemented the **SecBot** solution [86]. SecBot is a cybersecurity-driven conversational agent designed to interact with non-experts to extract information on cybersecurity demands and business requirements. Thus, the solution can *(i)* understand symptoms and business risks to correlate with potential cyberattacks, helping users comprehend incidents and their impacts, *(ii)* provide recommendations for actions in different levels of abstraction, such as which efforts are required to avoid or to mitigate problems, and *(iii)* support the configuration (*e.g.*, in-house firewall) or acquisition of protections, preparing actions (*e.g.*, command-lines or configuration files) required to configure or deploy a solution. SecBot then can be placed as an ally for risk management and decisions on SMEs, thus, implementing all components from the *Business Layer* of the proposed framework and allowing for the integration with implementations of all of the components mapped in the other layers. It is worth mentioning that SecBot was highlighted as one exciting application of chatbots by the Rasa

Reading Group [221], one project funded by the Rasa community to analyze systems built using the Rasa framework [193].

Two fundamental concepts are required for conversational agents: *Intents* and *Entities*. These concepts determine the basis for describing information and flow supported by SecBot. *Intents* refer to user's intentions, when interacting with the chatbot, and *Entities* are defined to extract specific terms or values. Extracting entities and intent classification typically involves an ML architecture. While non-ML approaches do exist [134], they are normally outperformed by supervised learning algorithms [251], which can generalize the information extraction process by understanding the context of input phrases. In the case of SecBot, a Dual Intent and Entity Transformer (DIET) [37] architecture is used for intent classification and entity extraction, implemented by the Rasa framework [193]. The DIET classifier relies on a transformer neural network to encode input text with context, Conditional Random Fields (CRF) [145] to identify and extract entities from text encoded, and dot-product similarity [237] to classify the input intent.

While *Intents* identify users that want to find protection according to the budget available or want to ask for help to configure efficient protection, *Entities* are used to extract specific terms or values from the user intent to provide a correct response. To reach accurate responses, all entities are connected to knowledge databases, which describe values accepted for each of the specific entities. About 150 entries are defined for *Entities* of SecBot. New entries for these *Entities* as well as new *Intents* can be added, such that the SecBot can cover different scenarios and demands. Table 4.2 provides examples of intents implemented in SecBot.

Table 4.3 lists examples of entities supported as input by the SecBot. After identifying the user's intent and extracting entities from the input text, SecBot needs to decide which action to best help the user. To that end, another important concept for conversational agents needs to be defined: *Stories*. A single *Story* defines those steps SecBot can take in response to a user's input, resulting in multiple possible conversation flows. For example, after recognizing the intent *attack_notification* and if the next one is the Intent *attack_details*, a message is sent asking for the budget available to invest in protection before issuing a recommendation. However, if the next intent recognized is *problem_desc*, a different action will be executed to identify the type of attack. Thus, the definition of *Stories* is critical, given that it is used to train the solution to recognize the context of a conversation and to select the following actions or flows.

SecBot supports functions that can be run as an action in response to users' inputs, according to an identified *Intent*, such as providing feedback messages, running arbitrary code (*i.e.*, custom actions), or listening for new inputs. Based on that, SecBot implements different custom actions that

Table 4.2: Examples of Intents Implemented by the SecBot

Intent	Example	Associated Entities
attack_notification	My Windows systems are under a ransomware attack	@target, @attack_name
attack_details	It is a WannaCry attack	@attack_type
target	The target is my database	@target
problem_desc	My server is receiving a lot of requests from different IPs	@symptom, @target
solution_config	I want to block an SYN flood using my IPTables	@solution, @technology, @target, @attack_name, @action
solution_support	How can I block a specific port using UFW?	@operator, @object, @solution
rosi_calc	Should I invest in backups against ransomware impacts?	@attack_name
critical_data	I have almost 10 TB of critical data	@cardinal

run actions according to different scenario flows. These custom actions involve *(i)* finding the best solution for a request, *(ii)* identifying the type of attack based on symptoms, *(iii)* helping during the configurations of in-house protections, and *(iv)* calculating metrics related to the economic impacts of different cyberattacks.

During the training phase of the SecBot, besides database entries and *Intents*, different *Stories* have to be defined for the supervised learning to allow the implemented Rasa neural network algorithm to obtain sufficient knowledge to extract and process information. Thus, it is possible to determine which action to take during a conversation correctly. These *Stories* were defined to cover SecBot scenarios, being able to predict a correct flow based on an identified *Intent*.

4.4.1 Proactive and Reactive Scenarios

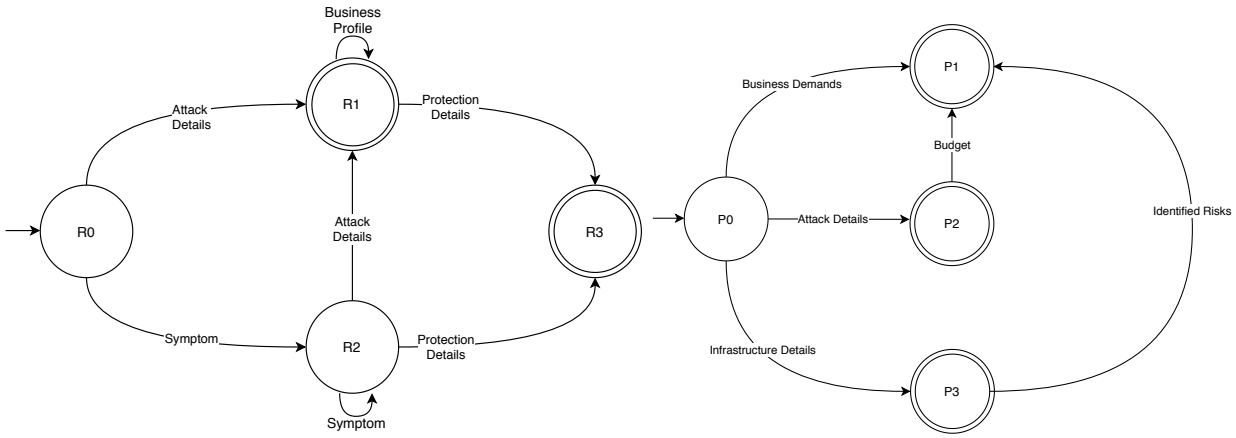
Two possible approaches are defined to describe different scenarios and to guide users during the interaction with the SecBot: the Reactive R and the Proactive P approaches. This definition can be viewed as complete, since it comprises the only two possible ways to behave in cybersecurity, *i.e.*, situations where the user wants to react to protect against an imminent attack (reactive) or a user who wants to operate a better plan defining the business cybersecurity strategy (proactive). These two approaches are divided into six different flows that can be combined to provide a more accurate and complete answer to the user.

Table 4.3: Examples of Entities Supported by the SecBot

Entity	Description	Input's Example
@attack_name	Name of the attack	I am being target of a @DDoS Attack.
@attack_type	Type of attack	It looks like a @SYN flood.
@target	Target of the attack or the component with symptoms	The target is my @Windows systems. It is my @database server.
@symptom	Describe specific problems or symptoms	My server is receiving @a lot of requests.
@budget	Amount and currency available to invest	My budget is @5000 EUR.
@solution, @technology	Describe in-house solutions	I have an @IPtables running on @Linux.
@operator	Describes the users' required action	I want help to @block an IP traffic using the UFW firewall.
@object	Explicitly describes an element to apply the operator	I want to block the @Port 22 using IPtables.

Figure 4.10 (a) describes the finite automaton for **reactive** scenarios. R_1 represents a conversation where the user knows technical details of the attack (*e.g.*, type of attack or log files) and wants to know which solution matches his/her budget and demands. R_2 focuses on understanding symptoms associated with cyberattacks and problems, thus, helping users find a suitable solution. Lastly, the flow resulting in the final state R_3 covers users that have already deployed protection solutions but need help to configure these.

The finite automaton for **proactive** scenarios is presented in Figure 4.10 (b). P_1 assumes users who want to reduce the economic impacts of threats in their business. Different metrics can be employed to provide useful information, directly helping, when deciding how investing in cybersecurity. *e.g.*, , the ROSI metric is calculated using the user's inputs and business requirements to provide insights about whether to contract a solution, assume risks, or even acquire cybersecurity insurance coverage. Furthermore, based on its knowledge database, the agent can suggest actions to reduce costs and avoid a financial loss for specific business sectors. Scenario P_2 covers the conversation flow in which users want to proactively protect their systems against specific cyberattacks (*e.g.*, WannaCry ransomware or Mirai Botnet). Recommendations for updates, configurations, or solutions to be ac-



(a) Reactive (R) Flow **(b)** Proactive (P) Flow

Figure 4.10: Finite Automaton for the SecBot Scenarios

quired can be provided. Finally, P_3 considers requests about the most common risks and vulnerabilities according to the business configuration, sector, and information provided.

Users can configure a business profile descriptor to provide the SecBot with a detailed view of their business. This information is used for the recommendation process and steps requiring specific information on the business organization (*e.g.*, number of employees, regulations, sector, or underlying security configurations/demands). To choose the best solution from a list of possible protections, the SecBot is integrated with MENTOR (*cf.* Section 4.7), the recommender system for protections.

Different custom actions are presented next to handle information obtained during the conversation, providing accurate answers for specific cases where algorithms and calculations are required to process the output, such as those specific reactive and proactive flows described. Custom actions are provided to SecBot to *(a)* identify a cyberattack based on a list of presented problems or symptoms, *(b)* provide configurations for protections according to requests, and *(c)* conduct an economic analysis based on user's requests to support the decision-making.

Attack Identification

The symptoms or problems extracted from the conversation can be used to identify the attack described by the user. A decision-tree containing the relationship between known attacks and associated symptoms is proposed as a custom action, which receives a list of symptoms and returns the related attack for the user. This action is directly related to the intent named as *problem_desc* (*cf.* Ta-

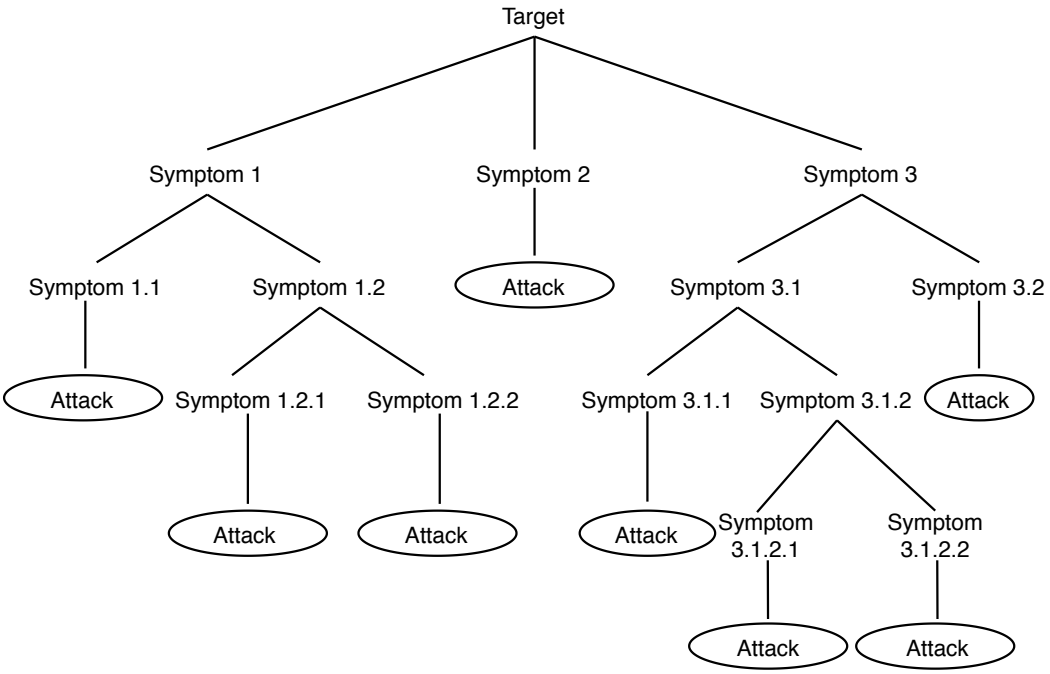


Figure 4.11: Symptoms' Tree Structure to Search for an Attack

ble 4.2), which is recognized when the user describes problems without a technical understanding of what is happening.

Figure 4.11 shows an example of the attack tree structure. The SecBot starts with an initial tree containing examples of well-known attacks (*e.g.*, DDoS and ransomware) relationships and their symptoms. Thus, the user's described symptoms are checked in the attack tree. If the resulting path ends in a leaf, it means that the attack was identified. Thus, using a *Server* as a target, the symptoms *"receiving many requests"* and *"many of them are SYN packets"* can result in the identification of an SYN flood attack. The same approach can be applied for different attacks in which previously known symptoms can be used to create the attack decision-tree. If the path cannot achieve a leaf, it means that the attack cannot be identified, resulting in negative feedback sent to the user.

Protection Configuration

The SecBot also interprets requests for help to configure protection already available in-house. Hence, entities are extracted to understand *(i)* the user's intent, which includes the name of the solution available, *(ii)* the operator (*e.g.*, block, allow, or protect), and *(iii)* the attack type for which the user wants a specific configuration. Based on these entities, SecBot can determine the associated configuration or provide the syntax for the user to create his/her configuration. For that, descriptors are defined to

store the relevant information about each configuration available. This information can be manually added or automatically generated by scripts that can extract and process public information available by solutions, such as using the Linux manual pages (man page) database.

```
<input>: "I have an IPtables installed and I want to protect my network against ICMP
    flood"
Entities_Extraction {
    "intent": solution_configuration
    "solution": IPtables
    "operator": protect
    "target": network
    "attack_name": ICMP flood
}
<custom_action>: find_configuration(solution, action, target, attack_name)
<output>: "The command for your configuration request is: iptables -t mangle -A
    PREROUTING -p icmp -j DROP"
```

Listing 4.1: Example of SecBot Processing and Output Based on a User's Input

Listing 4.1 presents the input and output for scenarios where users want to protect the network from an imminent attack (*i.e.*, reactive) or anticipate (*i.e.*, proactive) this type of attack to avoid damages. *E.g.*, the request *"I have an IPtables installed and want to protect my network against ICMP flood"* results in a message containing a configuration for *protection* against *ICMP flood* tailored for the IPTables packet filtering solution. This configuration is provided as a JSON structure stored by the SecBot, which maps different solutions, configurations, and commands.

```
{
  "iptables": {
    "version": "1.4.21",
    "OS": "Linux",
  "support":{
    "block": {
  "ports": "iptables -A INPUT -p <protocol> --destination-port <port number> -j DROP",
  "ip traffic": "iptables -A INPUT -s <ip> -j DROP"
    }
  },
  "protection_config": {
    "syn flood": "iptables -t raw -A PREROUTING -p tcp -m tcp --syn -j CT --notrack |
        iptables -A INPUT -p tcp -m tcp -m conntrack --ctstate INVALID,UNTRACKED -j
        SYNPROXY --sack-perm --timestamp --wscale 7 --mss 1460 | iptables -A INPUT -m
        conntrack --ctstate INVALID -j DROP",
    "icmp flood": "iptables -t mangle -A PREROUTING -p icmp -j DROP",
    "port scanning": "iptables -N port-scanning | iptables -A port-scanning -p tcp --tcp-
        flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN |
        iptables -A port-scanning -j DROP"
  }
 }
}
```

Listing 4.2: Example of a JSON File Describing a Protection Configuration

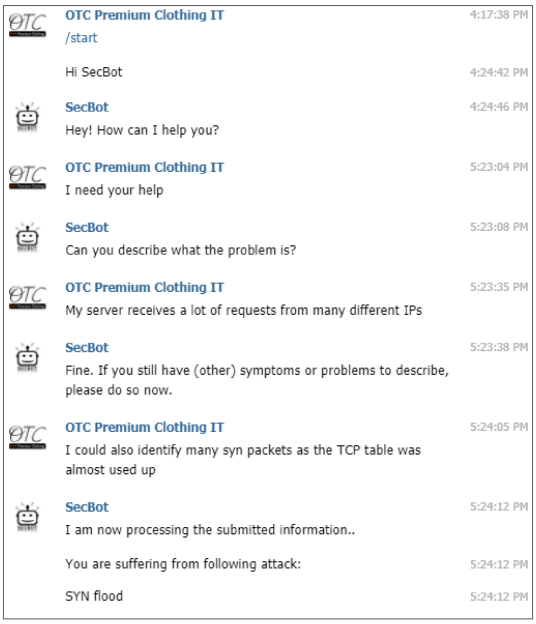
Listing 4.2 provides an example of this data structure describing a specific solution. In this example, a structure for an IPtables 1.4.21 running on Linux is defined, which supports requests to describe different actions, such as how to block Ports/IP traffic, and also allows for the configuration of IPtables to block different types of attacks (*e.g.*, SYN flood, SSH Bruteforce, and Port Scanning [131]). The OS being used by the business is taken into consideration to provide the correct configuration. This information can be described in the business profile or during the conversation.

4.4.2 SecBot's Implementation

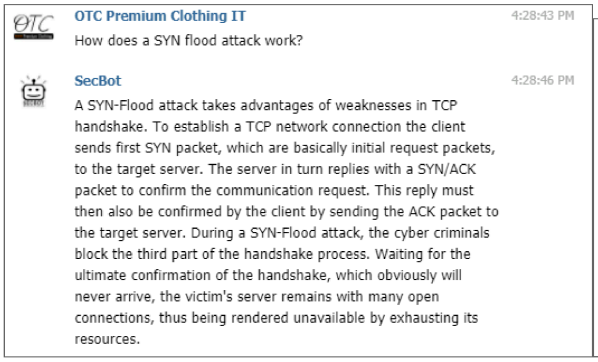
A proof-of-concept of SecBot was developed using Rasa 2.2.2 [193], an open-source machine learning framework to build contextual AI agents and chatbots. SecBot's code and training data set are publicly available [151]. The implemented solution relies on the Rasa framework abstractions of the underlying NLP and ML algorithms to simplify the design and handling of Entities and Intents. Custom actions were developed using Python 3.8.3, while the knowledge databases are described as plain text or JSON files. In its current version (as of March 2022), SecBot is composed of 61 stories (conversation flows), 37 intents (action conveyed in the sentences and all its participating parts), and 32 rules (short pieces of conversation that follow the same structure). Also, hundreds of entities values for targets, attack names, attack types, symptoms, and solutions are listed in lookup files.

Also, SecBot was integrated with the Telegram messenger application. For that, Telegram's BotFather was used, and an *access_token* was generated. A Ngrok tunnel was configured to make the chatbot reachable at localhost and the Internet. The Ngrok tunnel automatically creates both an HTTP and an HTTPS endpoint, which are then forwarded to the *localhost 5005*. The newly created HTTPS connection can then be assigned to an *webhook_url*. Figure 4.12 shows a simple interaction between a company (*i.e.*, OTC Premium Clothing IT) and SecBot via Telegram chat.

In Figure 4.12 (a), the company interacts with SecBot by providing some description of the symptoms being perceived. SecBot then collects her/his information and classifies it as an SYN flood. In Figure 4.12 (b), the company asks for SecBot what is this kind of attack. SecBot answers with a definition based on its database. Then, in Figure 4.12 (c), the company asks what is the impacts of this kind of attack, thus, receiving a brief description and a suggestion of PDF with more information about that. This shows the potential of supporting users not only with detailed information but also with supplementary material (*e.g.*, guidelines, configurations, and scripts).



(a) Attack Identification



(b) User Asking for Details About an Specific Cyberattack

(c) User Asking for Details About Possible Impacts of an Specific Cyberattack

Figure 4.12: Example of Interactions with SecBot using the Telegram Messenger App

4.5 Visualizations and ML for Threat Analysis and Identification of Cyberattacks

Network traffic analysis has been used for different purposes, such as monitoring and executing performance, accountability, and security tasks. For that, popular tools [230] can capture and analyze network traces (*e.g.*, Packet Capture (PCAP) files and Netflow records). This can be useful for both real-time and also postmortem analysis of attacks. In the cybersecurity field, a postmortem analysis (*i.e.*, after the attack occurred) reads traffic log files in order to extract characteristics of the attack,

identify damages, and acquire sufficient knowledge to mitigate new attacks [98]. However, there is still a certain lack of visualization approaches to explain cyberattacks and support cybersecurity planning. Also, ML-based systems can benefit from insightful visualizations to represent data in an accessible manner for different stakeholders without prior knowledge within such a field. Thus, these approaches can be used during the process of taking action against further attacks, such as those related to DDoS attacks and malware infection.

The **SecGrid** platform [90] was designed and developed as an open-source solution for post-mortem analysis, classification, and visualization of cyberattacks. SecGrid addresses the lack of integrated approaches for processing, analyzing, and visualizing complex datasets of cyberattacks by implementing an extensible set of miners to process information from network traces (*i.e.*, PCAP) and providing visualizations for the analysis of cyberattacks. According to demands, both miners and visualizations are extensible to address different scenarios and requirements. SecGrid is based on an ML-based approach to automatically classify traffic given according to its type (*e.g.*, SYN flood and Ping of Death) or as regular traffic. SecGrid defines for the *CyberTEA* framework the part of the RL, thus, implementing the *Data Processor*, *Threat Advisor*, and *Risk Analyzer*. Also, it provides a *Web-based Interface* for user interactions.

Three main dimensions are defined to represent the requirements of the SecGrid: *(i)* Automation, *(ii)* Usability, and *(iii)* Scalability and Extensibility. A fully integrated and automated process is provided to process and store information from PCAP files containing traffic originating from cyberattacks. Different abstractions are provided during the analysis and comparison of attacks, which simplifies identifying characteristics related to a cyberattack for improved cybersecurity planning and enhanced detection of attacks. Also, a supervised ML approach is used during the analysis and classification of cyberattacks. Finally, SecGrid's components are designed to be extensible, which means that both the extracted information and the visualizations can be rendered according to user-specific demands. Examples of work that use and extend SecGrid include economic information sharing [76], DNS Sinkhole [121], Real-time Netflow analysis [177], and Collaborative Mining [54].

SecGrid consists of *(i)* miners, which can decode PCAP files and extract features from different protocols (*e.g.*, Ethernet, IP, TCP, and HTTP), *(ii)* a Web-based Interface that allows users to interact with the platform and access overview statistics, *(iii)* an ML model to classify different attacks traffic automatically, and *(iv)* visualizations that give insights regarding the datasets under investigation. Besides, a Web-based user interface is provided, where users can share their insights and datasets with interested users, taking into account privacy concerns (*i.e.*, data anonymization).

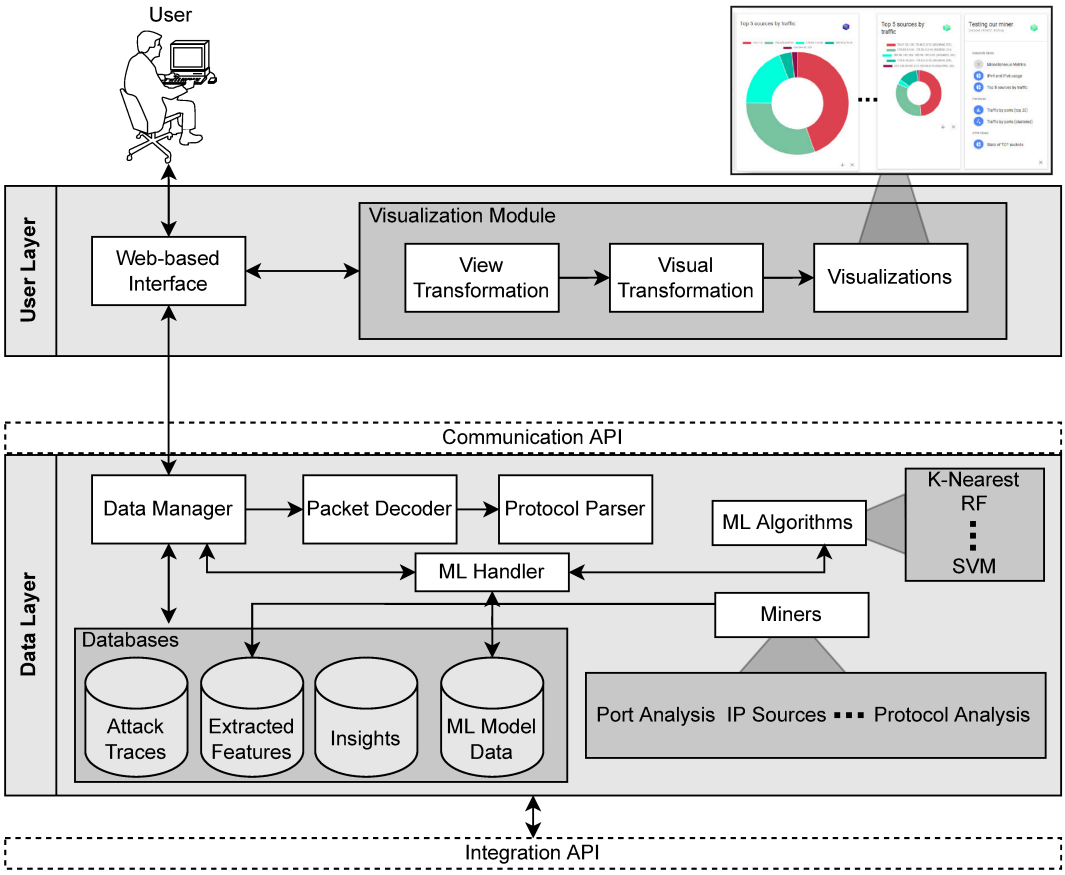


Figure 4.13: Architecture of the SecGrid Platform

The architecture of SecGrid is shown in Figure 4.13. The user accesses the Web-based Interface to analyze a dataset available (*i.e.*, PCAP file) or upload a new one. The *Data Manager* is in charge of handling user requests to store and access data related to a cyberattack. After the user uploads a new dataset, it is forwarded to the components of the *Data Layer*, which perform data extraction and processing of all relevant features of the cyberattack. Finally, these features are available in a well-defined data structure for the *Visualization Module* to build different visualizations according to user interactions. The *Data Layer* and the *User Layer* communicate through the *Communication API*. An *Integration API* allows for external solutions to request information and reuse available miners, which provides also integration options with external solutions.

In the User Layer, the *Visualization Module* renders the diagrams based on the result produced by the *Data Layer modules*. This module contains three components that work together and can be implemented as one integrated module. First, the *View Transformation* component receives the results of the mining process through the *Communication API*. It then transforms the properties of the data

structures into fitting visualizations, such as by mapping the number of packets contained in a result to the values for a *y*-axis of a bar chart.

These data structure properties can then be further adapted by the *Visual Transformation*, which can change the way how these properties are shown. *E.g.,* given that a user wants to zoom out, it aggregates specific data points on the *y*-axis of a bar chart. Finally, with this configuration, visualization components can plot the data using different visualization techniques. For example, a set of TCP ports and their number of occurrences could be plotted using different charts (*e.g.*, line, bar, histograms, pie). Therefore, the *Visualization Module* contains the required components that allow SecGrid to build interactive visualizations. Each visualization is described as a template, which can be fed with different information, thus, allowing the reuse of the same features to visualize different behaviors (*e.g.*, malware in its infection phase or a DDoS attack on the application layer). New visualization templates can be added to enrich the capacity of SecGrid to plot the information available.

Figure 4.14 provides an overview of the SecGrid Web-based Interface. In this view, the opened dataset (*i.e.*, Dataset 1) can be seen on the top left. In the *Metrics Tab*, a summary of all extracted information from this dataset is available (*e.g.*, number of packets, attack size, and the number of different sources IPs). All of the visualizations are accessible via the *Visualizations Tab*, separated based on the OSI layer model (*e.g.*, visualizations considering the application, transport, network, and physical layers). After clicking on one visualization, a new window is added to the dashboard grid, allowing for simultaneously analyzing different information and even datasets. For example, these opened visualizations can indicate a possible SYN Flooding attack leading to port 80 with a specific origin (*e.g.*, IP addresses and country).

The Data Layer contains the *Packet Decoder* module, which reads a PCAP file provided by the *Data Manager* and parses packets using the *Protocol Parser*, which is in charge of identifying the type of packets and separating them for further analysis. Then, the *Miners* extract specific information from the decoded packets, thus, making the extracted features available to users in different ways (*e.g.*, as a statistical report or in a set of insightful visualizations). These modules allow independent miners to analyze some protocols' packets without fetching packets that they do not need or without being affected by other miners. The protocols decoded and processed today by SecGrid include: Ethernet, ARP, IPv4 and v6, ICMP, TCP, UDP, and HTTP.

This set of miners, as summarized in Table 4.4, can access packets of a particular protocol or abstraction. Thus, it allows independent feature extractors to produce a visualization result for one or more attack types. For example, one implements an autonomous miner to visualize a possible SYN flood attack and an additional miner for a DNS amplification attack.

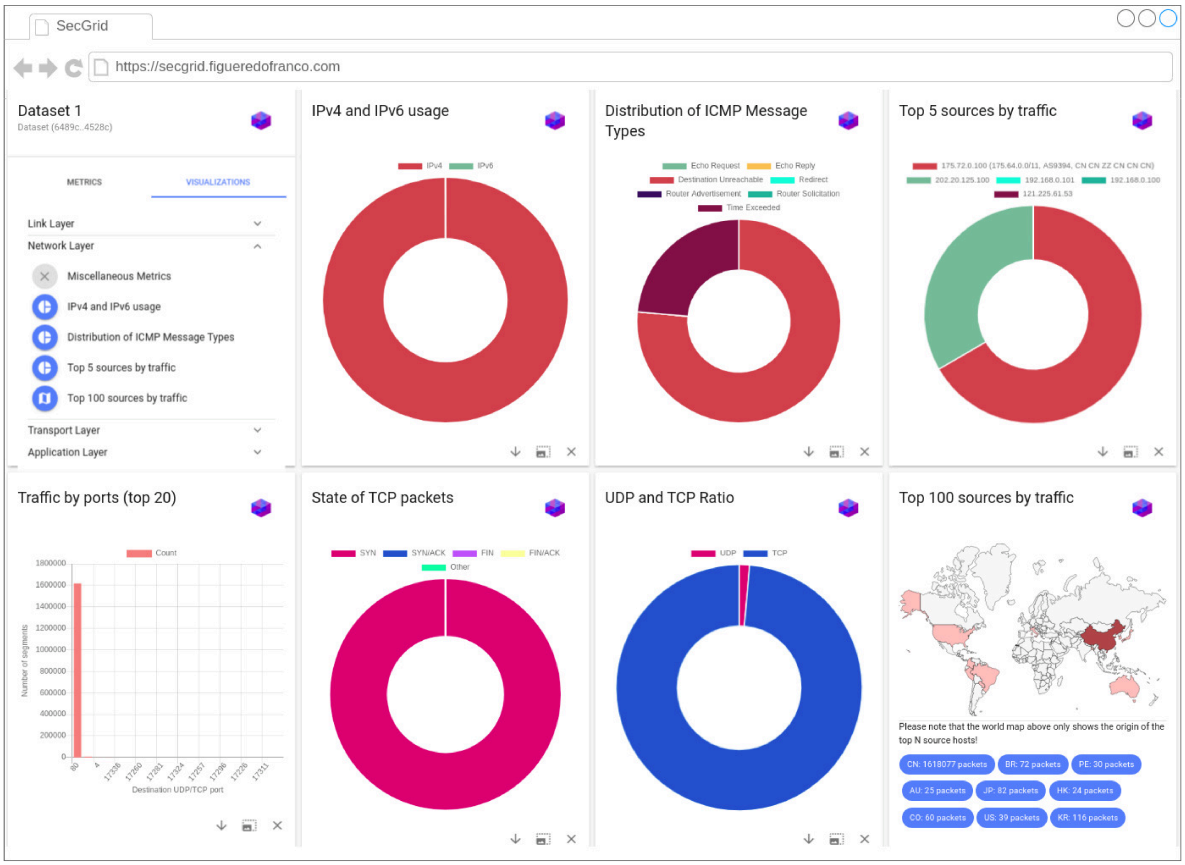


Figure 4.14: Example of a Dataset Opened in the SecGrid's Web-based Interface

The first miner observes packets emitted in TCP protocol, and the latter observes an application layer protocol. Then, they extract relevant features from the packets and store them for analysis. For example, a TCP States miner analyzes the TCP flags that indicate the connection states, highlighting the distribution of connection states of the overall observed packets. The miners then make available the results in a structured way to visualize such characteristics. It is important to note that although a set of miners are provided, it can be extended by implementing new miners (*e.g.*, JavaScript or Python-based) and linking them with the *Packet Decoder*. Thus, SecGrid's extensibility allows for further analysis and insights about different types of cyberattacks and behaviors, such as traffic related to WannaCry (ransomware), Mirai (Botnet) [97], or even a simple port scanning.

Table 4.4 lists examples of miners implemented by SecGrid. These miners can be applied separately or combined to extract meaningful information about the traffic available in a PCAP file. This information can then be combined to generate different reports and visualizations. For example, the combination of the TCP States Analyzer, Device Analyzer, and Port Analyzer can be used to identify

Table 4.4: Examples of the Miners Implemented for SecGrid

Miner	Target Data	Outcome
Metrics Analyzer	Attack duration, number of packets, IPs and ports	Overview of metrics associated to a cyberattack log file
IEEE 802.1Q Tagging	Frame tags	Overview over the VLAN membership of link-layer frames
IP Protocol Analyzer	IPv4, IPv6 packets	Analysis of the packets according to the IP protocol versions being used
Port Analyzer	UDP and TCP ports	Overview of the most used UDP/TCP ports by number of segments
Top Source Hosts Extractor	Source address	Overview of the hosts sending more traffic and requests
TCP States Analyzer	TCP flags	Analysis of the frequency of TCP flags in the packets, such as ACK, SYN, and FIN
Device Analyzer	HTTP User Agent	Identifies which type of device is being used for the request
Browser and OS Analyzer	HTTP User Agent	Identifies the browser and operation system being used for the request
HTTP Analyzer	HTTP Verbs and End-points	Analysis the most used HTTP requests (*i.e.*, GET and POST) as well as the end-points accessed via HTTP protocol
ML-Feature	Events emitted by the Protocol Parser	Listens to all events emitted by the protocol parser and process the information required for the attack classification ML model

Command and Control (C/C) traffic between IoT devices of a botnet. This traffic usually shows activity in port 23 (*i.e.*, Telnet), with most of the packets being SYN packets, and occasionally keep-alive packets (*e.g.*, PSH and ACK) can be observed [2].

For the classification of given attack traffic, the *ML Handler* acts as a gateway for the SecGrid and the ML algorithms (*e.g.*, K-Nearest Neighbour, Random Forest, or Neural Networks). Thus, when traffic data has to be classified, the *Data Manager* sends a request to the *ML Handler*, which will be in charge of preparing the data to be used as input for the implementation of classification ML algo-

rithms. Also, the *ML Handler* manages the *ML Model Data*, training and adding new data from the ML-Feature miner. Details on the implementation and the ML models being used are presented in the following sections.

4.5.1 SecGrid's Implementation

All of SecGrid's components and its *Web-based interface* were developed using *Javascript* (mostly Node.js and Vue.js). An instance of a running prototype and its source code is publicly available at [153]. Integration with the European DDoS Clearing House pilot is placed [82] to support better the analysis of one of the most prominent cyberattacks: DDoS attacks, thus, allowing for the exchange of information and features between SecGrid and the DDoSDB. Thus, SecGrid and the DDoSDB can communicate via APIs provided by both solutions. The need for the development of new miners is because extensibility and control of the different levels of granularity possible are important, when extracting information to provide insights, novel visualizations, and features for today and the next generation of cyberattacks.

One of the most important decisions, when implementing the packet parser of SecGrid, is which library to use for network capture decoding. The final decision for a library based on Node.js was taken because of different reasons, such as *(i)* technical aspects related to the capacity to handle capture files that are multiple gigabytes large and *(ii)* scalability aspects, which require well-defined structures to allow all miners to be easily extendable and optimized. Besides that, to support the implementation of the different miners, a list of protocol parsers was initially developed for the SecGrid. Table 4.5 lists protocols that are decoded by platform's *Protocol Parser*. Besides those protocols listed, other protocols and packet types are already decoded and emitted to miners (*e.g.*, 802.11, IGMP, SSL, and Websocket). Thus, it is possible to implement miners to extract features from them according to the demands of the different scenarios.

Multiple miners implemented by SecGrid provide specific features for analyzing and understating cyberattack traffic. Also, they allow for a straightforward extension of metrics and scenarios to be considered, which is helpful for different purposes, such as research experiments, cybersecurity education, and companies with specific analysis demands. However, as an alternative for SecGrid miners, well-known network tools like *tcpdump* and *SmartSniff* can use SecGrid as a more intuitive visualization and reporting platform. Thus, these powerful tools can be integrated into the SecGrid dashboard, enabling opportunities for SecGrid real-time analysis by using tools already tested and validated by the cybersecurity market.

Table 4.5: Decoded Protocols by SecGrid's Protocol Parser

Protocol	Description	Decoding support
Ethernet	This network access layer protocol was observed most frequently during the initial investigations	Fully decoded packets can be obtained and respective properties, including 802.1Q tags, can be conveniently accessed
ARP	The address resolution protocol provides resolution services to the internet layer	Decoding fully supported
IPv4	Version four of The internet-layer IP protocol	Full access to all properties in the IPv4 header
IPv6	Version six of the Internet-layer IP protocol	Limited decoding support. Only the fixed frame header is decoded with limited support for extension headers
ICMP	The control protocol used along IPv4	Decoding fully supported
TCP	Widely used connection-oriented transport-level protocol	Decoding fully supported
UDP	Widely used connectionless transport-level protocol	Decoding fully supported
HTTP	Application-level protocol	Parsers for certain attributes have been implemented, *e.g.*, User-Agent strings
BGP	Exchange routing protocol used by autonomous systems on Internet	Parsers for BGP messages

Although miners as implemented (*cf.* Table 4.4) provide information for the analysis of attacks, it is still required to process this data in order to be used to build the ML training model. Therefore, a miner *ML-Feature* was designed to extract data available by other miners and transform them to build the ML training model, such as transforming respective source IP addresses and ports into unique counters, obtaining the percentages of packet types from packets extracted, and calculating the inter-packet interval from the array containing all arrival times of packets.

The special *ML-Feature* miner listens to all possible events emitted by the package parser and processes all information of a time window to provide all relevant features for the attack classification.

Thus, the *ML-Feature* miner is used to process the PCAP files in order to generate the required information to be used in the training phase of SecGrid's algorithms and also during the classification of attacks. The training dataset created and to be used by SecGrid consists of 55,349 records extracted from different DDoS attack datasets, publicly available at [90]. Thus, as a proof-of-concept, the implementation and training dataset is provided to classify seven different behaviors within SecGrid: Regular traffic, SYN Flood, ICMP Flood, UDP Flood, IP Sweep, Ping-of-Death, and Port Sweep.

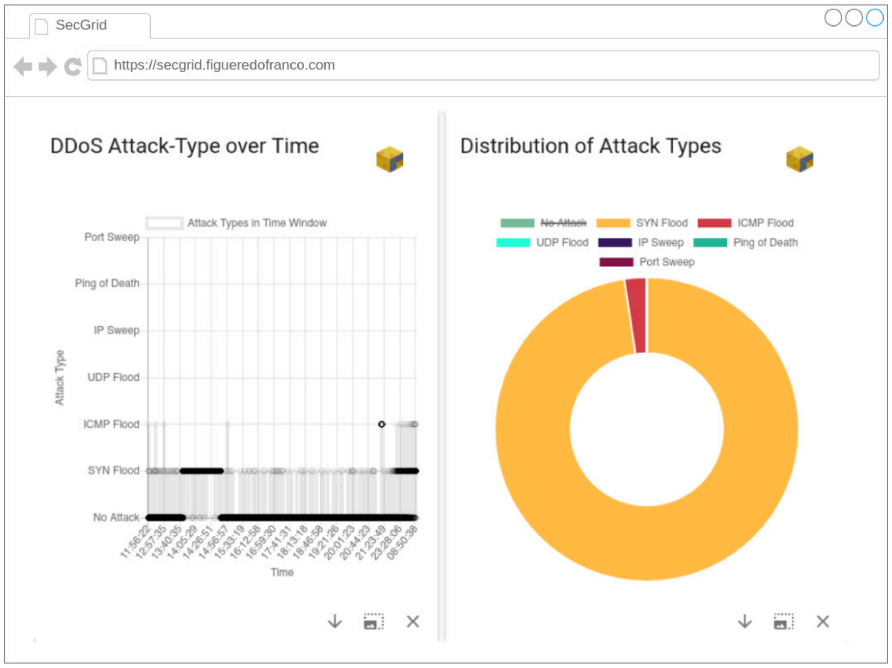


Figure 4.15: Visualization of ML-based Classification of DDoS Attacks Along the Time

Two ML algorithms implemented in the SecGrid platform were the Random Forest (RF) and KNN. The Scikit-learn classifiers were used to implement these algorithms, allowing for customization options and parameter tweaks. The RF classifier used ten estimators; thus, ten sets of random decision trees were created and compared. After classifying these different attacks identified in a single or multiple PCAP files, SecGrid provides a visualization in which the user observes along time, when regular traffic or specific attack occurred. This visualization shows the duration and behavior of attacks identified.

Figure 4.15 shows on the left the total distribution of the attack classified in the given time. The darker the lines, the heavier the classified traffic is. Therefore, solid black lines highlight intensive traffic (in terms of packets per second), while gray lines show less expressive traffic. In addition, on the right side, a pie chart summarizes the percentage of packets representing each attack classified.

4.6 Determining Optimal Investments in Cybersecurity

Another relevant challenge for cybersecurity, as discussed in the previous chapters, is how companies should invest their money. Currently, companies invest in cybersecurity solutions (and response teams) to ensure availability and protect critical services and infrastructure. The cybersecurity market is worth billions of dollars and steadily rising investments. However, achieving perfect security is essentially an impossible task from a technical perspective. If an attack happens, prevention is cheaper than reaction after an attack has already surpassed the infrastructure.

Suppose the companies do not invest correctly in cybersecurity. In that case, the security of its operation depends on luck. The impacts of attacks can be devastating, which is not acceptable for one with a reputation to maintain. Thus, it is important to understand risks and mitigate them to reduce possible losses due to cyberattacks. One fact is that the more valuable an information or service, the greater the amount of effort and money an attacker would spend to obtain or negatively impact that (*cf.* Chapter 2). Therefore, the value of the different business assets should be carefully analyzed during the different steps required to determine the economic impacts of a cyberattack and, consequently, achieve better investments in cybersecurity.

In cybersecurity economics, the GL model (as discussed in Section 2.2.2), is the most well-accepted analytical model to determine the optimal investment level in cybersecurity. The model considers *(i)* how much the data or service is valued, *(ii)* how much the data is at risk (*e.g.*, attack probability-based historical data), and *(iii)* the probability that an attack is going to be successful, which can be defined based on the threat modeling and risk analysis. Also, extensions to the GL model have been proposed over the years.

The idea of information segmentation was also introduced as a key element for investments in cybersecurity. The information segmentation argues that the amount invested in cybersecurity, when calculated using the GL model, should be considered in terms of specific information segment and their potential benefits (*i.e.*, invest more to protect information that can cause more losses). However, this kind of model is not trivial to be applied by companies, nor is it well-known by non-technical users. Therefore, solutions that help and simplify the application of GL and other economic metrics to cybersecurity are very welcome for companies' faster adoption, since economic motivation is one of the strongest ones to convince a company to invest in cybersecurity.

Based on that, **SECAdvisor**, a visual tool for calculating the optimal investment in cybersecurity is proposed. SECAdvisor allows to define information segments within a company and calculate the optimal investment for each segment, including potential losses with and without an optimal invest-

Table 4.6: Values Calculated and Provided by SECAdvisor based on the Gordon-Loeb Model

-	Customers	Internal Operations	External Operations	Total	Without Segmentation
Value of Information	120,000,000	60,000,000	20,000,000	200,000,000	200,000,000
Vulnerability	40%	20%	10%	-	31%
Expected Loss Before Additional Investments	48,000,000	12,000,000	2,000,000	62,000,000	62,000,000
Optimal Investment	2,280,000	788,528	180,000	3,248,528	3,321,363
Expected Loss with Optimal Investment	2,400,000	848,528	200,000	3,448,528	3,521,364
Total Cybersecurity Costs	4,680,000	1,637,056	380,000	6,697,056	6,842,727

ment in cybersecurity. This calculation uses the GL model and considers security-breach probability functions to estimate values accurately. After calculating an overview of the number of funds in cybersecurity, SECAdvisor can recommend protection measures using an external recommendation engine (*cf.* Section 4.7). Furthermore, the ROSI metric is calculated for each recommended solution to compare different protection alternatives in payback or cost-effectiveness. Table 4.6 overviews, as an example, relevant costs and investments calculated by SECAdvisor for three determined database segments (especially "Customer", "Internal Operations", and "External Operations"). These outcomes are based on the GL model [144] and are suggested to be used to guide precise investments in cybersecurity. The Appendix E shows examples of different values calculated in the background until achieving this optimal investment.

Figure 4.16 gives an overview of the three different application layers and their responsibilities. The flow starts with the decision-maker (*i.e.*, user) accessing the Web-based Interface of SECAdvisor and defining the business profile representing the company that he/she wants to conduct the calculations. To create such a profile, the user must submit key information about the company to the SECAdvisor, such as the revenue, sector, and the number of employees. Next, the Segment Layer is in charge of *(i)* managing the different segments within the company, *(ii)* estimating how valuable each segment is (*e.g.*, based on the critical data available and specific parameters for a given segment), and *(iii)* calculating the optimal investment per segment. Finally, the *Recommendation Layer* allows for the selection of specific threats and, based on the optimal calculation provided by the *Segment*

Layer, can determine which protections are suitable for the company in terms of fitting the optimal investment, budget available, and demands to mitigate/avoid a selected threat.

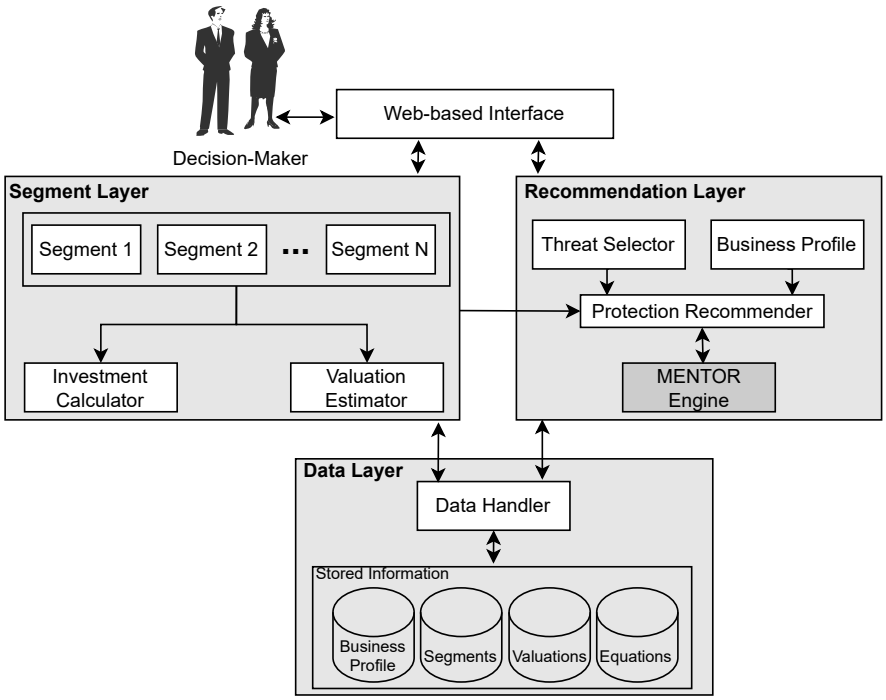


Figure 4.16: Architecture of the SECAdvisor

The *Recommendation Layer* prepares all information required and makes requests to the recommendation engine implemented by MENTOR, which is another solution developed and discussed in-depth in Section 4.7. After a list of protections is recommended for the company, the SECAdvisor also calculates the ROSI metric (as introduced in Section 2.2.3) for each protection, since it can support cost-efficient investments by comparing different recommended protections. The *Data Layer* is also implemented by SECAdvisor to store all relevant data (*e.g.*, information regarding the business, segments, and knowledge used for the segments estimations). Besides that, all configurations needed for the GL model (*e.g.*, security breach functions as discussed in Section 2.2.2) and for the customization of the SECAdvisor are stored in a database. Therefore, although predefined equations and configurations are placed, the SECAdvisor can be extended and adapted by changing key fields in the database.

4.6.1 Segments and Value Estimation

Determination of the segments and their values is critical for the optimal calculation of investments and the recommendation of protections according to specific demands. As already discussed in Section 2.2.2, a segment represents a technical business area of a company. The optimal investment amount should be calculated per segment, since a specific segment might be directly related to the potential benefits of cybersecurity investments. The following information is required to determine a new segment:

- **Segment Name:** The parameter represents the name of the segment, which can be freely chosen by the company (*i.e.*, user).
- **Segment Type:** The type of segment is used to suggest suitable cybersecurity threats and to simplify the monetary valuation of the segment. SECAdvisor allows for the selection of different pre-defined segments, such as *Web Server*, *Network*, or *Database* segments.
- **Value:** In order to calculate the optimal cybersecurity investment level, the monetary value (US$) of the segment is needed. Since it is often difficult to determine this value, the SECAdvisor provides assistance for the valuation of the segment based on publicly available reports and data.
- **Risk:** The *Risk* parameter describes the probability of a cyberattack. The user is allowed to specify a number between 0% and 100%. This parameter is needed to determine the optimal investment.
- **Vulnerability:** This parameter is also needed to calculate the optimal cybersecurity investment. It describes the probability that a cybersecurity attack on the segment will be successful. Values between 0% and 100% are allowed.

Next, the value of the segment must be estimated. However, it is not a trivial task for a user to determine the monetary value of the segment, such as how much a database is worthy for the business or networking infrastructure. Therefore, the SECAdvisor provides aid to facilitate this decision. The system allows the user to enter parameters tailored to the segment, which are evaluated based on previous knowledge populated in the database (*e.g.*, values based on estimations made by reports, research, or shared by partners). Thus, the user can receive a suggestion for the segment's value, which he/she can use as it is or adapt according to his/her view.

One example of this valuation is shown in Table 4.7, with the different parameters with their corresponding values for a database valuation. Based on data breach evaluations and reports, such as

the one yearly provided by the IBM Security about costs of data breaches [122], the application can determine the value of a segment. The user can specify how many records are stored in the database for different categories. The system multiplies the given number by the value of a record of this category. This allows the application to estimate the total value of the database based on the amount of sensitive data.

Table 4.7: Database Valuation based on the Average Cost per Type of Data Compromised According to the IBM Report for the Year of 2021 [122]

Parameter	Cost per Record Compromised
Number of Customer Data	US$ 180
Number of Anonymized Customer Data	US$ 157
Number of Employee Data	US$ 176
Number of Intellectual Property Data	US$ 169
Number of Other Corporate Data	US$ 165

4.6.2 Investment Calculation

The SECAdvisor calculates the optimal cybersecurity investment based on an extension of the GL model proposed by [144]. This extension combines the GL with the idea of information segmentation. Many concepts used for this calculation were discussed more in-depth in Chapter 2, precisely in Section 2.2.2. Therefore, it is recommended to check this section to understand GL model particularities better.

An important factor for the investment calculation is the breach probability function. It is denoted as *S(z,v)*, where z describes the monetary investment and v the vulnerability of the segment. The breach probability function describes the productivity of the investment, which first increases and then decreases after a certain point. Each additional investment is higher than the resulting benefit from this point on. The following steps and definitions, based on the work conducted in [144], are used to showcase the application of the GL model within SECAdvisor.

- L_i describes the value of the segment where L comprises the value of all segments. The breach probability function for a segment i (where $i = 1, 2, \ldots n$) is then expressed as follows:

$$S_i(z_i, v_i) = S(\frac{z_i}{L_i/L}, v_i)$$

- Each segment can minimize the segment's total cybersecurity costs:

$$\min_{z_i}[S(\frac{z_i}{L_i/L}, v_i)L_i + z_i]$$

- With the resulting z^*, the optimal investment can then be calculated:

$$S(\frac{z_i^*}{L_i/L}, v_i)L + 1 = 0$$

To calculate the optimal invest in cybersecurity, as the values shown in 4.6, the SECAdvisor uses the breach probability function defined in Equation 4.5. Thanks to this GL model extension, the SECAdvisor calculates the optimal investment level for each segment. In addition, the monetary advantage of information segmentation is also illustrated in the application. Note that these equations are fully extracted from the original work that extended the GL model to support information segmentation [144]. Therefore, it tries to generalize the security breach functions to cover hypothetical scenarios anchored by some assumptions related to the reality of cybersecurity today. However, this is not true for any company that wants to invest in cybersecurity. Thus, for an accurate optimal investment calculation, the security breach function has to be defined according to the reality and demands of a given company or sector.

$$S_i(z_i, v_i) = \frac{v_i}{1 + \frac{1}{L \times 0.001}\frac{z}{\frac{L_i}{L}}} \tag{4.5}$$

To determine the cost-effectiveness of a cybersecurity investment, the SECAdvisor then uses the ROSI metric. This metric is used because cybersecurity investments do not bring a direct profit but reduce potential damage. The ROSI calculation extends the Return On Investment (ROI) formula. The ROI calculation is shown in Equation 4.6.

$$ROI = \frac{\text{Gain from investment} - \text{Cost of investment}}{\text{Cost of investment}} \tag{4.6}$$

The ROI index makes statements about how effective the investment is compared to the return. The result is expressed as a percentage. The higher this number, the higher the effectiveness of the investment compared to the return. This index can be poorly applied to cybersecurity investments, as cybersecurity investments do not yield a monetary return. Instead, the ROSI metric is applied. During the evaluation of cybersecurity investments, the focus is on assessing how much potential

loss can be prevented by an investment. Therefore, the monetary value of the investment must be compared with the monetary value of the risk reduction. The ROSI's definitions and equations are discussed in detail and with examples of application in Section 2.2.3. The ROSI metric applied by the SECAdvisor is shown in Equation 4.7.

$$ROSI = \frac{(\text{ARO} \times \text{SLE} \times \text{mitigation\_rate}) - \text{Cost of the Solution}}{\text{Cost of the Solution}} \tag{4.7}$$

While *ARO* stands for the estimated annual rate of a cyberattack occurrence, the *SLE* represents the monetary damage caused by a successful cybersecurity attack. Using the *mitigation_rate*, which represents the percentage value of risk reduction from the cybersecurity investment, the ROSI metric can be calculated. Through the ROSI metric, the SECAdvisor provides the decision-maker with valuable information on how effective his/her cybersecurity investment is. This makes it easier for the user to select the appropriate cybersecurity solution for specific segments, such as selecting from a given list of antivirus solutions which one is better from an economic point of view.

The rest of this section highlights how these different equations and concepts were implemented and integrated into SECAdvisor to be used by companies during the decision process of investments in cybersecurity. All of the technical decisions and interaction flows are explained and described below.

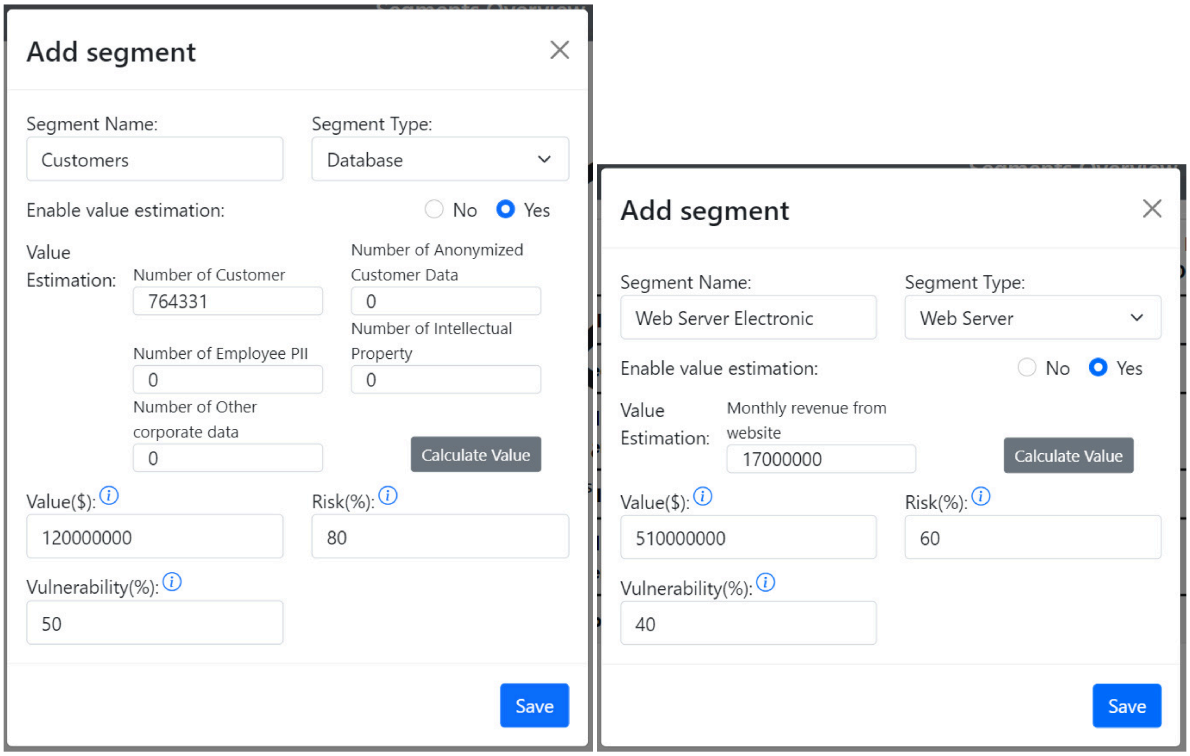
4.6.3 SECAdvisor's Implementation

The SECAdvisor was mainly implemented using *AngularJS* and *NestJS* frameworks. The database is the *MongoDB*, a document-oriented NoSQL database management system. The data used for the SECAdvisor prototype is stored on *MongoDB Atlas*, which is a flexible and scalable cloud database service. The database was connected using the *Mongoose*, an Object Data Modeling (ODM) library for Node.js. The calculation of the optimal investment level is a core competence of the application. For that, the library *nerdamer* was used to enable calculation operations that JavaScript does not provide by default. Finally, the integration with the recommender system so-called MENTOR (*cf.* Section 4.7) was performed by making calls for a RESTful API implemented by MENTOR. The source code and a full-fledged prototype of SECAdvisor are publicly available at [41].

In the first step, the user has to add his/her business profile and the segments that compose the business under analysis. The user can use the SECAdvisor interface to add each segment required for the optimal investment calculation. Figure 4.17 shows the interface for adding two different segments. In Figure 4.17 (a), a database segment (*i.e.*, segment type) is selected, which requires the user to fulfill the information regarding the records stored in such a database (*e.g.*, number of records

with sensitive and anonymized data). If this information is available, the value estimation can be performed automatically; otherwise, the value for the segment has to be defined manually. Also, the risk of an attack happening in this segment has to be defined together with the likelihood of a successful attack (*i.e.*, vulnerability).

Figure 4.17 (b) shows a different segment being added, which represents an Web Server. In this case, the fields required are different. If the user wants an automated estimation of the segment's value, the user has to provide the monthly revenue of the Web site running on the webserver. Based on that, the SECAdvisor can estimate how worthy this is as an asset for the company. Otherwise, the information has to be provided manually, as it is for the risk and vulnerability.

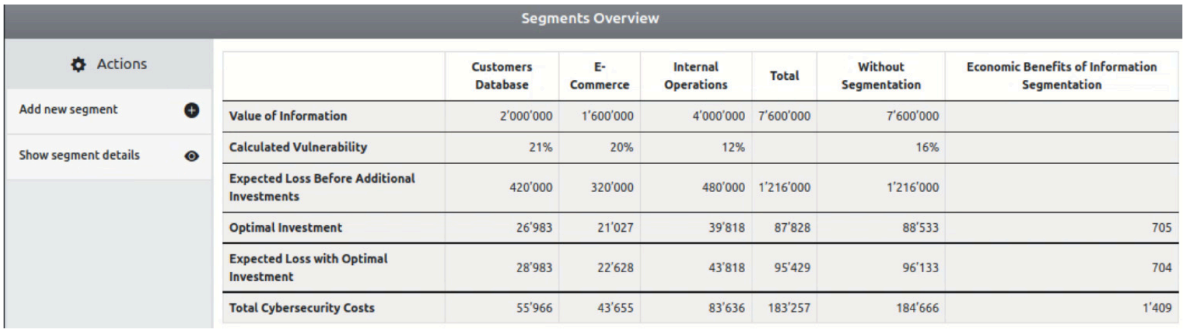


(a) Database Segment **(b)** Web Server Segment

Figure 4.17: Definition of Segments Using the SECAdvisor Interface

After having the segments determined (*i.e.*, value, risk, and vulnerability of a segment), optimal investments can be calculated by applying the GL model. The equations are used as defined by the database (*e.g.*, security breach function and additional calculations). Figure 4.18 shows the calculations made for each segment added to the SECAdvisor. In this example, three segments are available:

Customers Database, E-Commerce server, and Internal Operations. An overview of information is available in the table generated by SECAdvisor, and the optimal investment is defined.



	Customers Database	E-Commerce	Internal Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	2'000'000	1'600'000	4'000'000	7'600'000	7'600'000	
Calculated Vulnerability	21%	20%	12%		16%	
Expected Loss Before Additional Investments	420'000	320'000	480'000	1'216'000	1'216'000	
Optimal Investment	26'983	21'027	39'818	87'828	88'533	705
Expected Loss with Optimal Investment	28'983	22'628	43'818	95'429	96'133	704
Total Cybersecurity Costs	55'966	43'655	83'636	183'257	184'666	1'409

Figure 4.18: Overview of the Optimal Investments per Segment Calculated Using SECAdvisor

The user can use this information as input for the next steps of planning and investment, taking it as a reference value for each segment. For instance, this value can determine the maximum budget to spend with protections for a specific segment. By having this amount at hand, the user then can go for the *Recommendation tab*, which allows obtaining recommendation of protections based on the MENTOR engine (*cf.* Section 4.7). Besides providing the recommendation of protections that fit the budget (*i.e.*, optimal investment) and customized demands, the SECAdvisor also calculates the ROSI metric by just clicking right below one suggested protection. Figure 4.19 highlights these features by showing a list of recommended protections as well as the button to calculate the ROSI.

The ROSI calculation requires the user to provide the mitigation rate, the cost of the incident, and the annual rate of incidence for each protection. According to the segment definition, these values are already received from the MENTOR recommendation engine and provided by the SECAdvisor. However, this can be manually edited by the user if needed. After receiving the recommendation and the value for ROSI (*i.e.*, a ROSI higher than one means cost-efficient protection), the user can decide which protection to acquire to achieve sufficient protection while also investing only the optimal amount in cybersecurity.

4.7 Selection and Recommendation of Cybersecurity Protections

The cybersecurity market is worth billions of dollars [199] and investments are steadily rising. There are financial incentives for Security Providers (SP) to enter the market by offering protection services. At the same time, users can reduce protection costs (*e.g.*, related to the deployment, configuration, and operation of services) by leveraging a competitive cybersecurity market to meet their

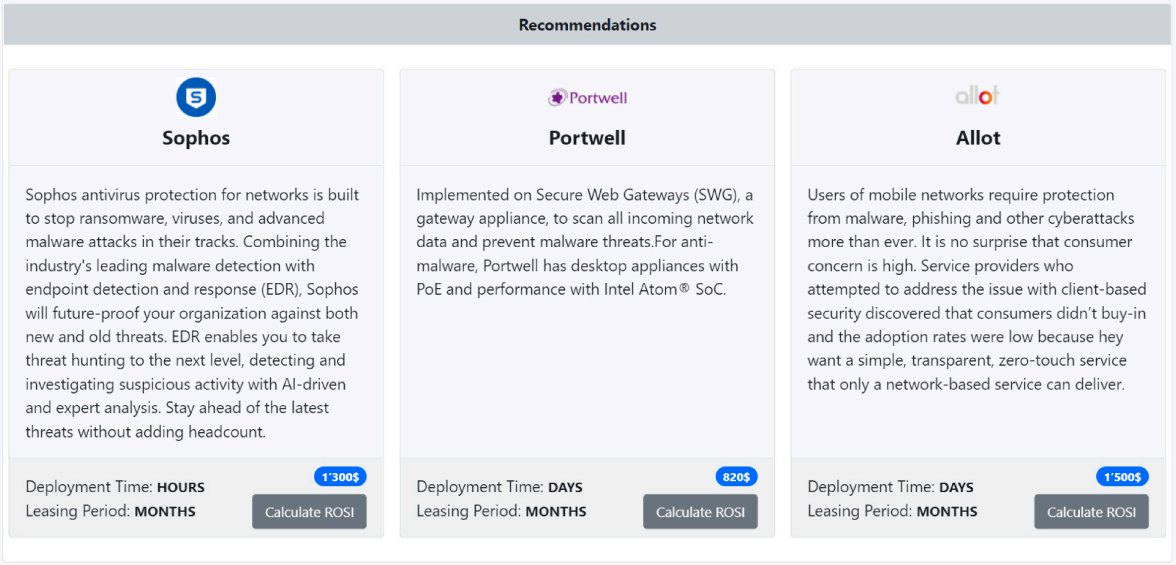


Figure 4.19: Recommendation of Protections and ROSI Calculation in SECAdvisor

specific demands. These protections may include acquiring physical appliances, software licenses, virtual network functions, and cloud-based protection. Thus, although traditional models will still meet specific demands, a notable amount of next-generation protection services – as an instance of cybersecurity planning – can adapt to flexible business models and provide a different level of protection on-demand.

Several on-demand protection services and marketplaces are available, which are not only offering protection services but also offer alternatives regarding the deployment and management aspects of such services [34] [204]. However, it is not a trivial task for users to select one of them. Decision-making is even more critical if the company's infrastructure is under attack. The decision to mitigate the attack should be based on information about the infrastructure, such as its economic aspects, demands, and characteristics of the attack. In this scenario, it is essential to observe not only how often attacks surpass the on-site infrastructure capacity but also which off-site services can provide the necessary protection, considering their different service flavors, such as the amount of traffic supported, the capacity to address particularities of a determined attack, and price conditions. In this sense, recommender systems [209] provide a valuable cybersecurity planning tool to support decisions during the detection and mitigation process.

Therefore, **MENTOR**, a recommender system for protection [88], is proposed in the context as a solution to support cybersecurity planning. The MENTOR solution assists companies in measures to protect critical infrastructure and assets during the decision process, thus, performing an important risk management task. The recommender engine indicates protection services available from

different SPs to prevent and mitigate threats. MENTOR considers different properties from available protection services, the customer profile (*e.g.*, budget available, region, and technical demands), and characteristics of the cyberattack to establish a fair recommender system, where one or more services from different SPs (*e.g.*, both small companies and global players) can be proposed to neutralize a threat efficiently while minimizing cost and reducing damage. By looking at the framework proposed by this thesis, MENTOR provides specifically the *Recommendation Engine*, one of the cores of the Decision Layer.

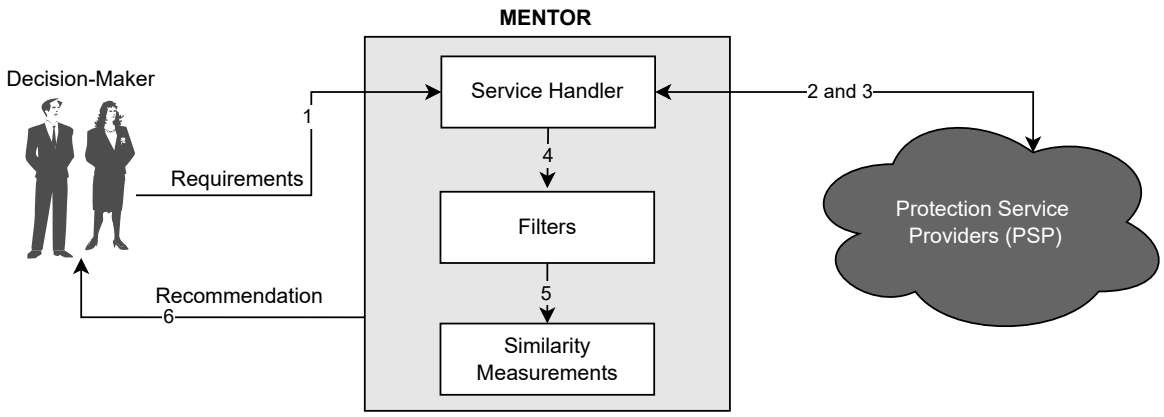


Figure 4.20: Recommendation Process Overview in MENTOR

The process overview of MENTOR is depicted in Figure 4.20. The user can describe his/her requirements (*e.g.*, budget, threat, and type of protection service) that can be used by the solution to filter the content of available services from different SPs. MENTOR can then determine which one is most suitable to support all requirements and demands described. For that, the recommendation engine applies different similarity algorithms to determine the most appropriate service.

4.7.1 Recommendation Process

Figure 4.21 shows the overall architecture of MENTOR, highlighting all components and steps related to the recommendation process. The recommendation flow is described as follows. First, in Step 1, the *Service Requestor* receives information related to the infrastructure under attack and the characteristics of the attack (*e.g.*, logs from monitors). Such information is transformed into an appropriate data structure and delivered to the *Extractor*, which initializes the recommendation process. Next, in the Extraction and Classification phases (Steps 2 and 3), the information is analyzed and correlated with the type of attack to identify those requirements which fend off the attack. In turn, a list of possible protection services is generated (Step 4) and forwarded (Step 5) to the recommendation engine.

Finally, in Step 6, the recommendation engine uses the customer profile input to define which service from the list of potential candidates is the optimal recommendation.

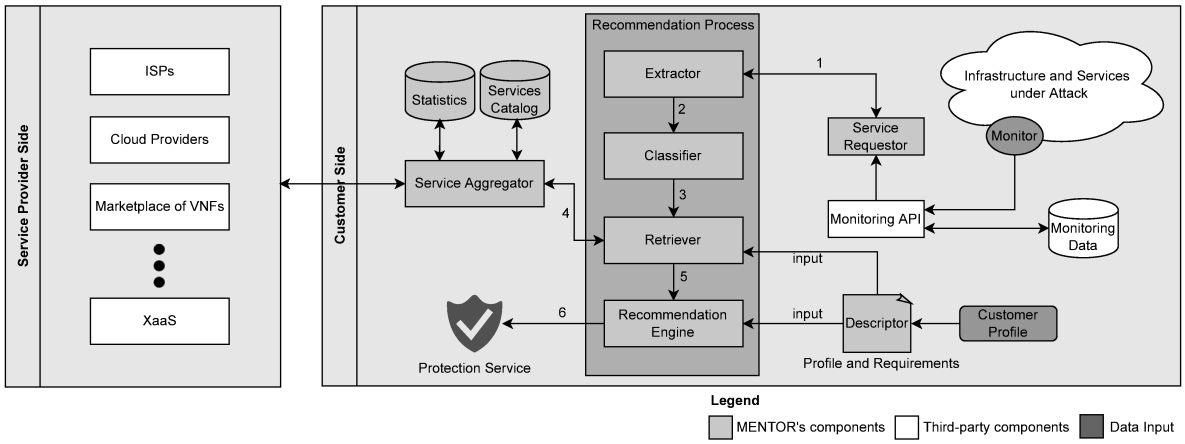


Figure 4.21: The MENTOR Architecture

In the first step, the *Service Requestor* receives data from monitors and stores relevant data in a database for future analysis. If a threat or an imminent attack is identified, the component sends the relevant information and meta-data to the *Extractor* component to start the recommendation process. Next, the *Extractor*, which is the first step of the recommendation process, is in charge of extracting relevant insights (*e.g.*, attackers, attack characteristics, and infrastructure impacts) from the data monitored. After the extraction, the information is forwarded to the data categorized into different attacks.

During the next step, the *Classifier* is responsible for classifying the extracted data according to the previously reported and identified attacks (*e.g.*, DDoS variations). To achieve this classification, techniques to identify attack patterns and also a database providing attacks fingerprints [189] are applied. After the classification, the *Service Aggregator* communicates with different SPs to obtain a list of available services available and relevant properties of each service (*e.g.*, price, type of service, and coverage area). Next, the database containing the services catalog is populated to supply customers. The list of SPs can be modified according to customer preferences. Then, the *Retriever* is in charge of querying the *Service Aggregator*, who can fully or partially address the demands of the user. Such services selected and returned can yield different solutions targeting the same problem but vary in performance, price, and technology.

The final step of the recommendation process is composed by the *Recommendation Engine*, which supports different algorithms to select the optimal service based on the list provided by the *Retriever*. Besides the input provided by the *Retriever*, a set of details is described by the customer to map the

user profile and requirements. Therefore, to support such a decision, different aspects have to be considered, such as budget constraints, service coverage, and the capacity to address the particularities of a cyberattack.

4.7.2 Recommendation Engine

The input data for the recommendation engine depicts a list of available protection services from SPs. This list comes from the MENTOR'S database previously populated manually or by automated systems that search for protections available on the market [227]. The database contains general information about the service (*e.g.*, price and type of service) as well as technical details regarding threats and attacks supported by each service. The data returned by each SPs should optimally be provided through an interface to communicate with MENTOR's *Service Aggregator* to be incorporated into the recommendation process. Thus, providing such an interface is in the interest of every SP.

Table 4.8 presents those parameters that define the requirements of the user running the recommender system. These parameters are to be defined inside a profile and requirements descriptor (*e.g.*, a JSON file), containing helpful information used during the filtering and recommendation steps conducted by the *Retriever* and the *Recommendation Engine*. One user, for instance, can use such descriptor to configure the recommender system to temporarily contract a reactive virtual protection service being remotely hosted in South America, with a deployment time of just a few seconds. The amount available to spend on such service will be defined as US$ 500. Also, if available, information about an imminent attack or threats possible to be exploited can be described. Thus, protection services that do not support all requirements will not be considered a viable option based on this information. The descriptor can also be extended to support new parameters and relevant information provided by the protection services available.

In order to evaluate the feasibility of the recommendation process, the MENTOR was assessed using four widely used similarity measures: *(i)* Euclidean distance, *(ii)* Manhattan distance, *(iii)* Cosine similarity, and *(iv)* Pearson correlation. These measures were selected because of their potential to quantify the similarity of two objects [209]. Thus, users' demands can be compared with protections available to decide which fits better for each specific case. MENTOR was designed to be generic and extensible to support other algorithms to recommend protection services. In this regard, service requirements from customers and offered protection services are mapped as vectors in space as depicted in Figure 4.22, *i.e.*, their set of attributes as well as magnitudes represents a direction in space, allowing a geometric evaluation of similarity.

Table 4.8: Customer Profile and Requirements

Parameter	Description	Value
Type of Service	Describes if there is a demand to protect the network from further threats (*i.e.*, proactive) or react in order to mitigate imminent attacks (*i.e.*, reactive)	Reactive or proactive
Type of Attack	Provides details of the attack which a protection is being required	*e.g.*, SYN Flood or a specific malware
Attack Details	Uploads log files or details about the attack	*e.g.*, DDoS fingerprints or behavior data of any attack
Region	Defines specific geolocalization that one protection service should be deployed or able to act	Continent, country, city, or any
Deployment Time	Describes the maximum time between the service being contracted until it be able to protect the customer	Seconds, minutes, hours, days, or any
Leasing Period	Defines the period for which the customer want to contract a protection service	Minutes, hours, days, weeks, months, or any
Budget	The amount (*e.g.*, in Euro or USD) available to spend with protection	Any

Equation 4.8 presents the Euclidean distance. The Euclidean distance is calculated by taking the square root of the sum of the squared pair-wise distances of every dimension. In terms of the recommendation process, a vector containing the parameters defined by the user (*cf.* Table 4.8) are described as a vector x_i, and each service available is transformed into a vector y_i in the same way. Then, the sum of differences of all individual squared pair-wise distances is squarely rooted. Thus, the Euclidean distance determines if a service is adequate for the request: *i.e.*, the optimal recommendation is the service with the lowest possible Euclidean distance.

$$euclidean(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{4.8}$$

In a similar approach, the Manhattan distance, introduced in Equation 4.9, calculates the distance (β) between two vectors by considering the difference in the absolute values of each vector. The vector x represents the protection service and y the user profile. The best service is the one with

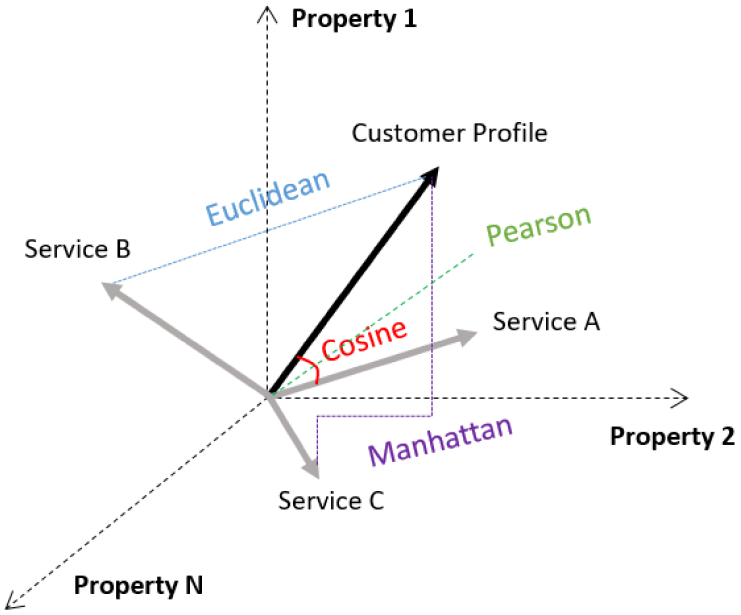


Figure 4.22: Protection Services Mapped into Vectors and Compared to Customer Profiles using Different Similarity Measures

the shortest diagonal path between the two vectors. Like the Euclidean distance, the best protection service with the lowest possible value is optimal.

$$manhattan(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{4.9}$$

Equation 4.10 shows the Cosine similarity calculation, which finds the normalized dot product of two attributes x and y. $\cos(x, y)$, where x is any dimension of the user request and y is a dimension of a protection service), is calculated between the two vectors to decide if one service fits the user request. If the angle is equal to 0 the value for the cosine will be 1 (best recommendation), and it is less than 1 (*i.e.*, it ranges from 0.99 to -1) for any other angle.

$$\cos(x, y) = \frac{\sum_{i=1}^{n}(X_i \cdot Y_i)}{\sqrt{\sum_{i=1}^{n} X_i} \cdot \sqrt{\sum_{i=1}^{n} Y_i}} \tag{4.10}$$

The fourth measure under investigation is the Pearson correlation (*cf.* Equation 4.11). The Pearson correlation determines linear relationships between two normalized distributed variables. This

correlation provides a value ranging from -1 to 1, representing the correlation between two vectors. Thus, the lower the value, the worse is a protection service x recommended for a demand y.

$$pearson(x, y) = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2(y_i - \overline{y})^2}} \tag{4.11}$$

The recommendation process works as follow. Initial preparation steps involve *(a)* receiving/preparing input data and *(b)* filtering unrelated services. The input *(a)* requires receiving protection services from the *Service Aggregator*, which for the purpose of evaluation were created randomly. Next, the customer profile is determined (*i.e.*, received from the front-end or to establish the comparison of those services offered for protection. Before calculating similarities, unrelated services are discarded in the filtering process. This involves eliminating services, whose binary properties do not match the customer's requirements, *e.g.*, type of service (reactive or proactive) or service region (Europe).

Step 1 involves the indexing of *(a)* service parameters required by the customer and *(b)* each service in order to build an integer array representing the service. These steps are necessary to map services and enable the application of similarity measures geometrically. Similarly, Step 2 is applied to each service to index its properties. Steps 3 and 4 involve the actual recommendation of services and storing the rating. In Step 3, the customer profile is mapped as a vector Y and each protection service as a vector X, provided as input to similarity algorithms. In Step 4, ratings are stored as a similarity dictionary with the service ID as a key, especially to later enable the export or plot of similarity data.

4.7.3 MENTOR's Implementation

A prototype of MENTOR was implemented to evaluate the feasibility of such a solution practically. The Web-based user interface was developed using ReactJS 16.8. The *Recommendation Engine* was implemented using Python 3.7.3. Flask 1.0.2 was used to implement REST APIs allowing the communication between components. The recommendation engine's code is available online at [149]. An additional instance of MENTOR called ProtectDDoS [89] was developed to provide a Web-based interface and refinements in the engine to make it optimized for the recommendation of protections against DDoS attacks. The source code is available at [55] and shows the first integration of MENTOR with an external solution via API. The API allows for easy integration with other solutions. Examples of this integration is mentioned also in Sections 4.3, 4.6, and 4.4 by showing, respectively, how SecRiskAI, SECAdvisor, and SecBot are integrated with MENTOR.

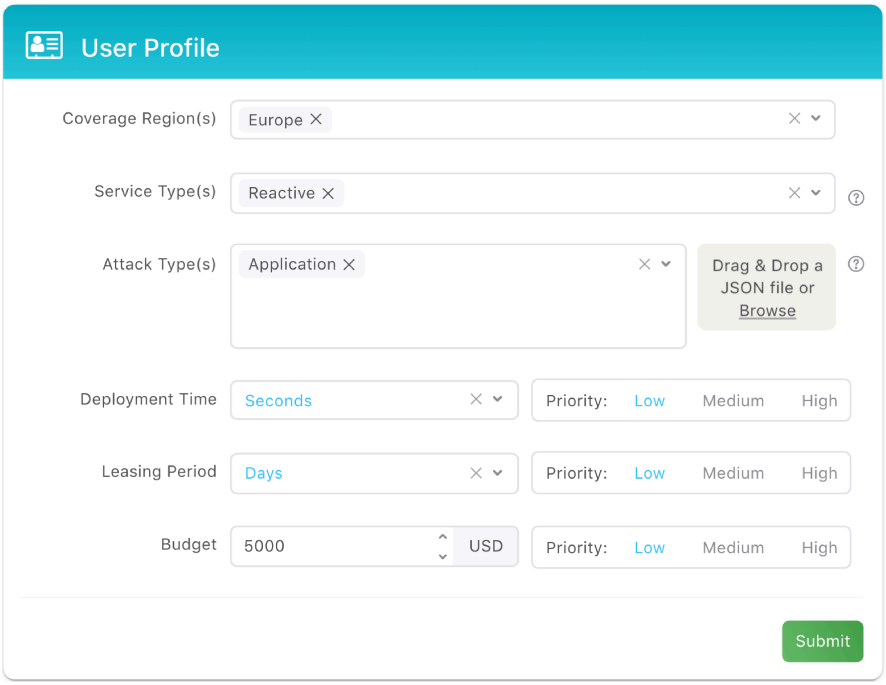


Figure 4.23: User Requirements Configuration using ProtectDDoS's Web-based Interface

Figure 4.23 shows the interface where users can access to configure their requirements (*i.e.*, customer profile) and prioritize each demand from *High* to *Low*. Defining priorities during the recommendation process, such as *High* priority for the price, will impact the recommendation and, thus, return the protection service with a lower price while neglecting others, less prioritized criteria. After that, a list of the most recommended protection services available is returned. Even though a dashboard was implemented, the recommendation engine is loosely coupled to the dashboard. It can be executed autonomously, without any interaction, only providing the adequate inputs (*e.g.*, attack's characteristics or specific demands) via MENTOR's API to automate the process. The possible automation favors further steps towards a real-time recommendation of protection services.

As the MENTOR offers support for different algorithms, the user can select the recommendation algorithm according to preference. In order to help in the decision process, different information is provided, representing how the algorithm classified each protection service. Thus, the user can visually process and understand the accuracy of a recommendation by comparing the vector describing the customer profile and the vector of each protection service.

The MENTOR not only optimizes the service selection for users but also encourages SPs to actively publish their prices, which in turn increases price competition and usually results in a decreased price for the user. New services can be automatically added using descriptors provided through the

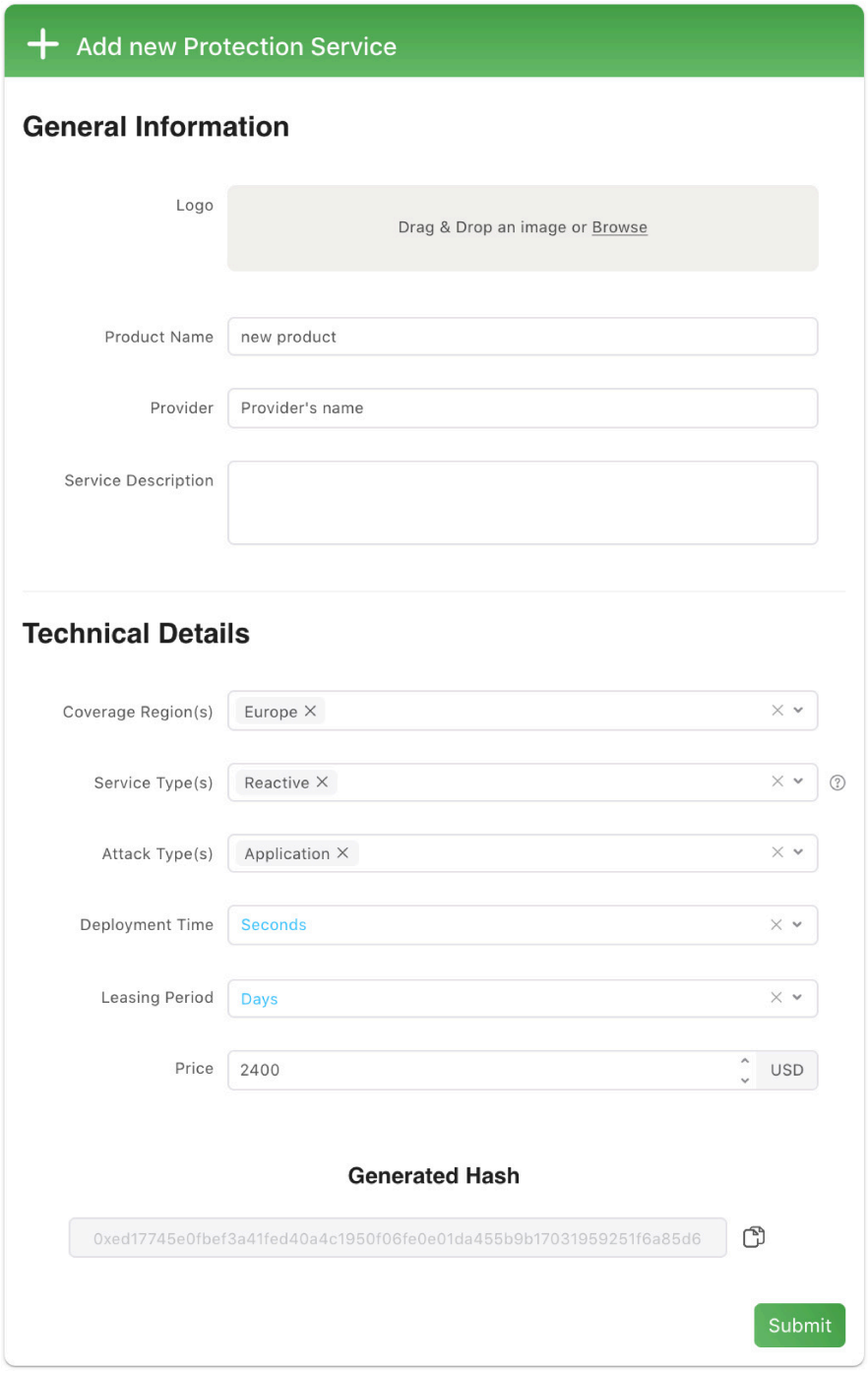


Figure 4.24: Upload of a New Protection via the Web-based Interface of ProtectDDoS

RESTful API running on the SPs side. For this, each SP that wants to announce its service needs to describe its services as a JSON file containing relevant information about the service and adhering to

the model provided in Table 4.8. This can be done automatically by using the Web-based Interface of MENTOR as shown in Figure 4.24. After that, MENTOR's components receive such descriptors and extract information to populate the database.

```
{
    budget: "200 USD",
    requirements:{
        protection_type: "Reactive"
        region: "Europe",
        deploymentTime:[
            "minutes"
        ],
        leasingPeriod:[
            "days"'
        ],
    }
    infrastructure:{
        technology: "Openstack"
        services_running:[
            "Apache Web Server",
            "MySQL Database"
        ],
        protection_running:[
            "IPtables"
        ]
        priority: "high"
    },
    attack:{
      type: "SYN Flood",
      log_file: "attack.pcap",
      fingerprint: "attack.json"
    }
}
```

Listing 4.3: Example of JSON File Describing a Customer Profile

The prototype implemented also allows for uploading log files to provide feedback on protection services. The users' feedback can feed a reputation system for SPs and customers. Thus, a reputation system can provide more accurate recommendations, decreasing the necessary trust placed in information advertised by the SP.

By using the input of the user, a JSON file, as shown by Listing 4.3 is automatically created via the dashboard, thus, describing requirements and attack characteristics. Also, user infrastructure information can be described to refine MENTOR's filters. For example, some protection services can be highly recommended for specific technologies (*e.g.*, Openstack-based infrastructure), while other on-site protections (*e.g.*, IPtables-based Firewalls) are already running. This file can be created manually by any SP interested in offer a protection, following the standard defined by MENTOR. This file is used as one input for the recommendation engine (*cf.* Figure 4.21) and, based on the require-

ments described on such a file, MENTOR can apply filters and determines the similarity between each service and the customer profile.

4.8 Supplementary Solutions

Besides the solutions introduced above to satisfy the main layers of the framework proposed by the *CyberTEA* approach, there are a set of supplementary solutions designed and implemented to provide additional elements and features that can also contribute for an adequate cybersecurity planning.

Therefore, although optional, it is highly recommended to consider solutions like those to address known demands of the cybersecurity community and also to highlight opportunities that the cybersecurity field can explore, such as cyber insurance models, information sharing enablers, marketplaces for protections, and mechanisms to deploy and host protections as a service. All of the solutions introduced in this section are placed in the *Supplementary Layer* of the *CyberTEA* framework and also cover key steps of the *CyberTEA* methodology.

4.8.1 Automating Cyber Insurance Models using Blockchain (BC)

As discussed previously in Section 2.1.3, the costs related to cybercrime are increasing fastly. In this sense, to reduce the impact of successful attacks and to enable companies to recover faster and with fewer costs, different cybersecurity investments can be considered; in which one of the most prominent strategies includes cyber insurance coverage models [178]. Although the cyber insurance market is fast-paced and is under intense development [139, 141], cyber insurance approaches still have room to advance from a risk transfer tool to a critical requirement for companies' risk management.

Currently, different cyber insurance approaches are explored by companies, effectively expanding the market, either *(a)* introducing new business models and mechanisms to gain advantages or *(b)* improving their insurance services by using new technologies. However, critical open challenges for a cyber insurance adoption exist, *e.g.*, the information asymmetry that has to be considered during the contract's design and the customer's eligibility for coverage [24]. Thus, different cyber insurance approaches have been proposed, and new paradigms have been applied in such a context [241]. One such new paradigm that is a suitable catalyst in the insurance market is the BC, which allows for reducing intermediaries, automating the deployment and management of insurance contracts, and supporting novel insurance models [100]. Due to the automation enabled by SCs and the immutability of the BC, BC-based cyber insurance models can provide a trustworthy and immutable agreement between cyber insurers and customers.

Thus, in order to explore opportunities in this field, **SaCI** is proposed as a BC-based approach for the creation, deployment, and management of a cyber insurance contract [81]. SaCI correlates relevant customers' aspects and cyber insurance companies' (*i.e.*, insurers) requirements, such as business information, contract constraints, and security aspects, to create an SC that describes and manages the agreement between customers and insurers. Based on this, both stakeholders can interact with the SC to proceed with coverage requests, contract updates, and premium payments. SaCI ensures a trustworthy record of the contract coverage and all changes along time; thus, not only *(i)* providing automation of the process, but also *(ii)* acting as a referee or proof in case of disputes (*e.g.*, customers requesting payment for a loss due to a cyberattack that the insurer has denied payment for). Further, if funds are available and contractual requirements are satisfied, SaCI automatically transfer funds between stakeholder to execute payments, such as those related to premiums paid and loss coverage due to a cyberattack.

SaCI describes a JSON file structure to store relevant information about the contract and translate it to SC code within well-defined functions allowing for interactions between customers and insurers. Therefore, SaCI allows for the *(i)* payment of premiums and contract updates, *(ii)* request of damage coverage and dispute resolutions, and *(iii)* check of contract information and its integrity, whenever it is required (*e.g.*, in case one of the parties involved are not following the agreement defined). Before the development of SaCI, as a first investigation, the cyber insurance stakeholders were mapped, and relevant information related to the cyber insurance market was collected. This helped to have a better understanding of the challenges and also the opportunities within this market. Both mapped stakeholders and collected steps (mapped as a framework) are available in the Appendix B. Also, a set of interviews with cyber insurance underwriters working in Switzerland were conducted to validate the view of the cyber insurance scenario.

The architecture of SaCI (*cf.* Figure 4.25) highlights the layers and components designed for the blockchain-based cyber insurance model. It determines two relevant stakeholders (*i.e.*, customer and cyber insurer) for the approach at the top and enables the interaction with the system using those components running on their respective layers (*i.e.*, on their own infrastructures). The *User Layer* is composed of a Web-based interface, with which the customer can access and add all information related to business and demands (*cf.* Table 4.9). This information is forwarded to the *Contract Builder* in charge of mapping this information into the JSON format. The respective JSON file is sent to the *Insurer Layer* using the SaCI's API.

Within the *Insurer Layer* the *Contract Processor* reads information from this JSON file and stores a copy of all contract information. The *Premium Calculator* estimates the premium for this contract's

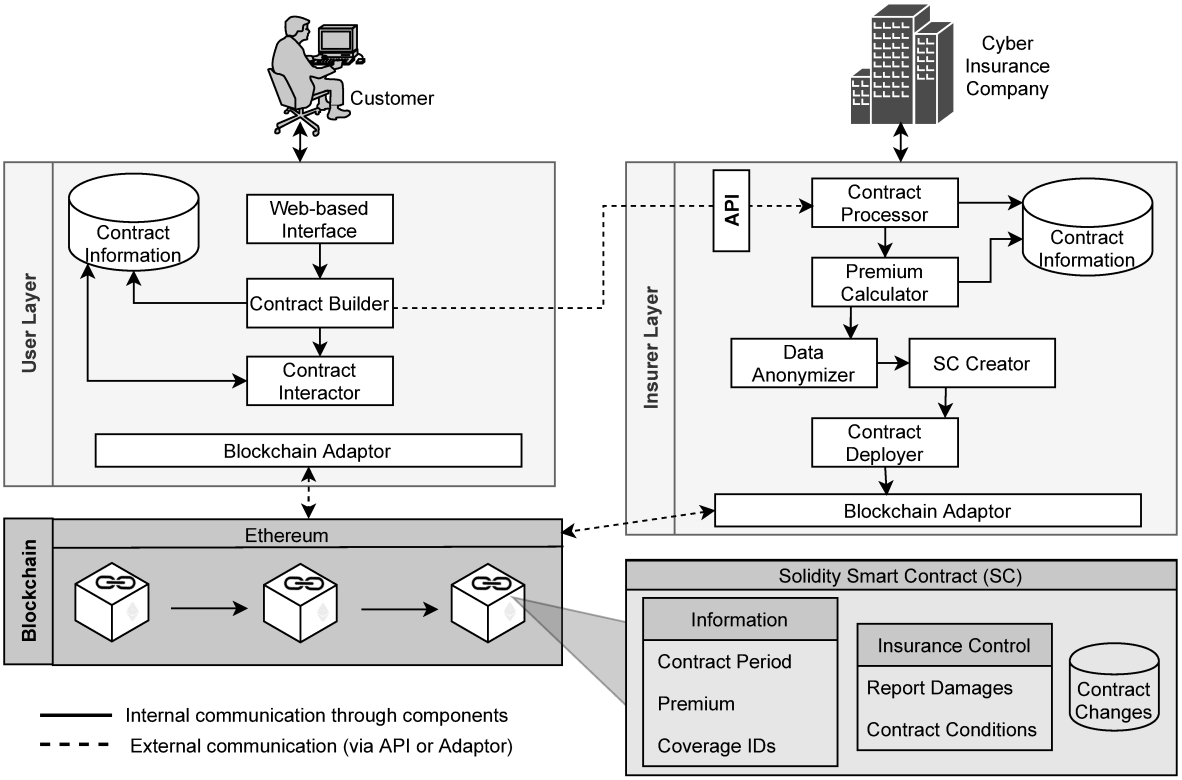


Figure 4.25: SaCI Architecture

coverage. While SaCI does not focus on an optimal premium calculation, it provides relevant information in a standardized format, *e.g.*, as input for a base rate pricing in which adjustments can be accommodated according to insurer preferences.

After the premium calculation, the *Data Anonymizer* component is in charge of removing from the contract all information that can be critical to identifying the company and its risks. This is essential before deploying the contract within a public BC (*e.g.*, Ethereum or Cardano). The *SC Creator* uses all other information to transform the JSON file into an SC based on a previously defined one (*i.e.*, Solidity code) and fills in missing information in those fields mapped. Finally, the contract is deployed on the BC and available for interactions between all stakeholders (Actors) involved (*cf.* Table **??**).

In order to define the relevant information for the creation of the cyber insurance contract and, consequently, the SC, the necessary information was defined based on the related cyber insurance market. Table 4.9 provides an overview of these main categories considered by SaCI. Every characteristic demanded by a customer is assigned to one of these categories. Note that this type of infor-

Table 4.9: Contract Information

Category	Description	Example
Business Information	Standard Information about the company, which is not relevant for the premium, but which is needed to identify the company.	Company name, Company address
Contract Constraints	Information about the non-technical constraints of the contract, which have to be completely defined in each contract.	Duration of the contract, Payment frequency
Company Conditions	Non-technical information about the company's business number, which affect the premium.	Yearly revenue, Number of employees
Company Security	Information about the measures of the company to increase its cyber security as well as different metrics to measure it.	Risk assessment metrics, attack history, security software, security training
Company Infrastructure	Information about the hardware and software used by the company.	Used technologies, Critical data amount
Contract Coverage	Information about what attacks and impacts are covered by the contract and by which conditions.	DDoS attack: Business interruption: coverage at 50%; data breach for third-person damage: coverage: at 100%

mation has to be provided by customers, resulting in "inaccurate" information, and can be impacted by companies' biases, such as metrics related to risk assessment and threats impacts.

The business information contains standard information about the company, which is most likely to be known publicly. This information is needed to identify the company but is irrelevant for a premium calculation. Basic conditions (*e.g.*, contract duration) are stored in contract constraints. Company conditions comprise all non-technical characteristics and mainly include information about business numbers. The following two categories are significantly related to each other, and they encompass all technical characteristics. With the information of these two categories, the probability and partially the impact of a successful attack can be estimated to understand all risks by both actors better.

While the company security category describes different metrics about security deployed and measures taken to improve the security, the company's infrastructure includes all information of hardware, software, and technology as well as critical parts of those. Finally, details about every contract's coverage are stored in an unlimited list within the contract coverage category. For every attack, the costs covered and possibly other constraints of the specific coverage (*e.g.*, maximum indemnification

of insurer) are defined. The contract coverage is the most important part besides the risk assessment to calculate the premium. Listing 4.4 shows an example of a contract coverage against four different threats (*e.g.*, business interruption due to a DDoS attack and third-person damage due to a data breach) defined in the JSON file's descriptor. Finally, upon entering information of all categories, the content is forwarded to the *Premium Calculator*, which calculates the premium for the SC creation.

At this point, the contract is deployed on the BC and can be accessed by the insurer, and the customer utilizes functions available in the contract (*cf.* Table **??**). This list is not exhaustive, and other functions are also available in the SC. All details are available within the implementation at [160].

After the premium is paid and the contract is enacted, the actors can interact. For instance, in case an attack happens, the customer can call the *reportDamage()* function to ask for refunding or help. The insurer can accept or deny the coverage requested. If accepted (*i.e.*, *acceptDamage(id)*), the payment is made automatically via the SC according to what was defined previously in the contract. Note that the customer can also provide a hash of a log file as proof of the attack. This hash is also stored in the BC to enable an integrity check further. At the same time, the file itself has to be stored off-chain, especially inside the contract information datasets maintained by both actors.

```
"contract_coverage": [
  { "name": "DDoS",
   "coverage": [{
     "name": "Business Interruption",
     "coverage_ratio": 100,
     "deductible": 1000,
     "max_indemnification": 300000 }]},
  { "name": "Data Breach",
   "coverage": [
    { "name": "Third-party damage",
     "coverage_ratio": 100,
     "deductible": 1000,
     "max_indemnification": 300000 }]}]
```

Listing 4.4: Contract Coverage in a JSON Format

If the parties cannot reach a conclusion, counteroffers can be made by the insurer (*i.e.*, payment for a specific loss but not for all financial losses). Figure 4.26 shows the state diagram of possible interactions after a *reportDamage()* is called by the customer. The report damage process has one of the following states: *New*, *Paid*, *UnderInvestigation*, *Dispute*, *Resolved*, or *Canceled*. This diagram exemplifies the usage of the different functions (*e.g.*, *reportDamage()*, *acceptDamage()*, and *acceptCounterOffer()*) to claim a settlement.

The *Canceled* status is an ending state, reached only if the customer cancels the request. *Paid* status defines that the insurer accepted to cover the damage, and it was automatically paid. If the contract has a lower balance than the value to pay out, the insurer must transfer funds to the contract, when

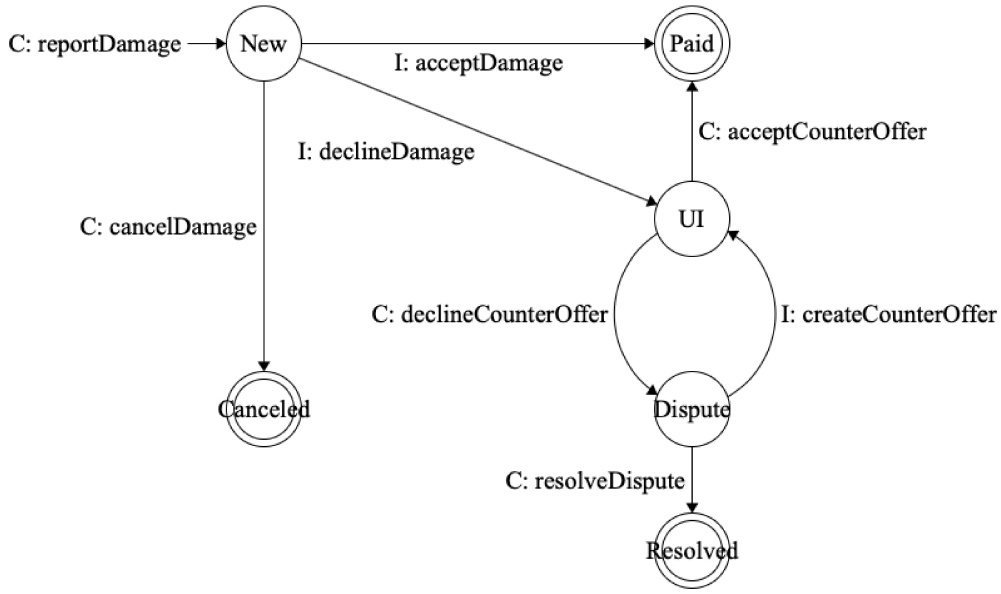


Figure 4.26: Claims Settlement State Diagram for SaCI

accepting the coverage. If the insurer declines the coverage payment, a reason is provided, and a counteroffer is issued. If a counteroffer is not possible to be offered at that time, the status is defined as *UnderInvestigation*, which means that further manual investigations have to be placed off-chain before a counteroffer can be placed.

If the insurer provides a counteroffer (*e.g.*, a lower amount than the initially requested compensation for that incident) and the customer does not accept it, the state changes to *Dispute*. This refers to the fact that no agreement has been found yet. Either the insurer creates a better counteroffer, or the two actors have to solve the dispute off-chain for which a third party may be considered. If the dispute can be solved, the final status of *Resolved* will be achieved. Using the SC function *getAllReportedDamagesWithStatus* all reported damages with a specific status can be returned, which also allows verifying the history of past interactions, *e.g.*, accepted, declined, and under investigation coverage requests.

A prototype of the SaCI was implemented using Python as backend language and Solidity for the SC development. The Ethereum blockchain running on the Ganache testbed has been used for the deployment and tests of SC functionality. Flask was used for SaCI's Application Programming Interface (API) in its latest version. Finally, for the off-chain storage, the prototype uses SQLite. The source code and all documentation are publicly available at [161].

Example of Application Scenario for the SaCI

Suppose that a customer wants to protect her business from financial loss possibly caused by DDoS attacks. The customer will access SaCI's Web-based interface and fills in all information related to her/his business and individual requirements, such as the company's conditions (*e.g.*, sector, revenue, and the number of employees), security aspects (*e.g.*, attacks history, risk assessment, available protections), and coverage demands. The insurer uses this information to propose a contract offering coverage of 90% of all financial loss if a business interruption happens due to a DDoS attack until a maximum amount of US$ 300,000. For that, the deductible amount of US$ 1,000 is considered besides a yearly premium of US$ 2,000. Figure 4.27 provides an overview of all interactions and actors considered for this application scenario.

After the customer and insurer decide about the contract off-chain, this generates a JSON file with all information, and SC is created with the anonymization of private information. Finally, the contract is deployed on the BC, and the hash of the JSON file with all contact information is stored together with the SC. Both actors also store a copy of the JSON file (*i.e.*, all contract information without anonymization) in private databases for further reference, while the hash stored in the BC allows for integrity validation. The customer finally call the function *payPremium(amount)* for coverage.

If an attack happened at the customer's IT resulting in US$ 15,000 of loss, a request for coverage is placed by calling the function *reportDamage(date, amount, type_of_attack, logFile_hash)*. Based on this, the insurer automatically checks if the request complies with the contract and calls the function *acceptDamage(amount)*, ensuring that the amount is available in the SC for the payment. The amount is automatically sent to the customer to pay for her losses. A counteroffer will be placed if the damage was not accepted or if further investigations are required. The logFile_hash allows for the verification of the attack and losses if required. Thus, the insurer can ask the customer to send log files via a secure channel, *e.g.*, containing network traces, reports, or internal analysis data explaining the incident. The hash stored in the BC provides a trustworthy record if a dispute is required.

4.8.2 Enabling Economic Information Sharing

Information sharing is one of the critical concerns toward a more collaborative approach that helps companies better understand the scenarios and cyberattacks behaviors [9, 135, 238]. Today, there are many challenges in making decisions regarding cybersecurity, mainly because of the information asymmetry between companies. Companies have views only of part of the problem and do not share their insights with others. This frequently happens due to privacy concerns and business competition. Therefore, there is the fact that no single organization has visibility over the entire problem space. This

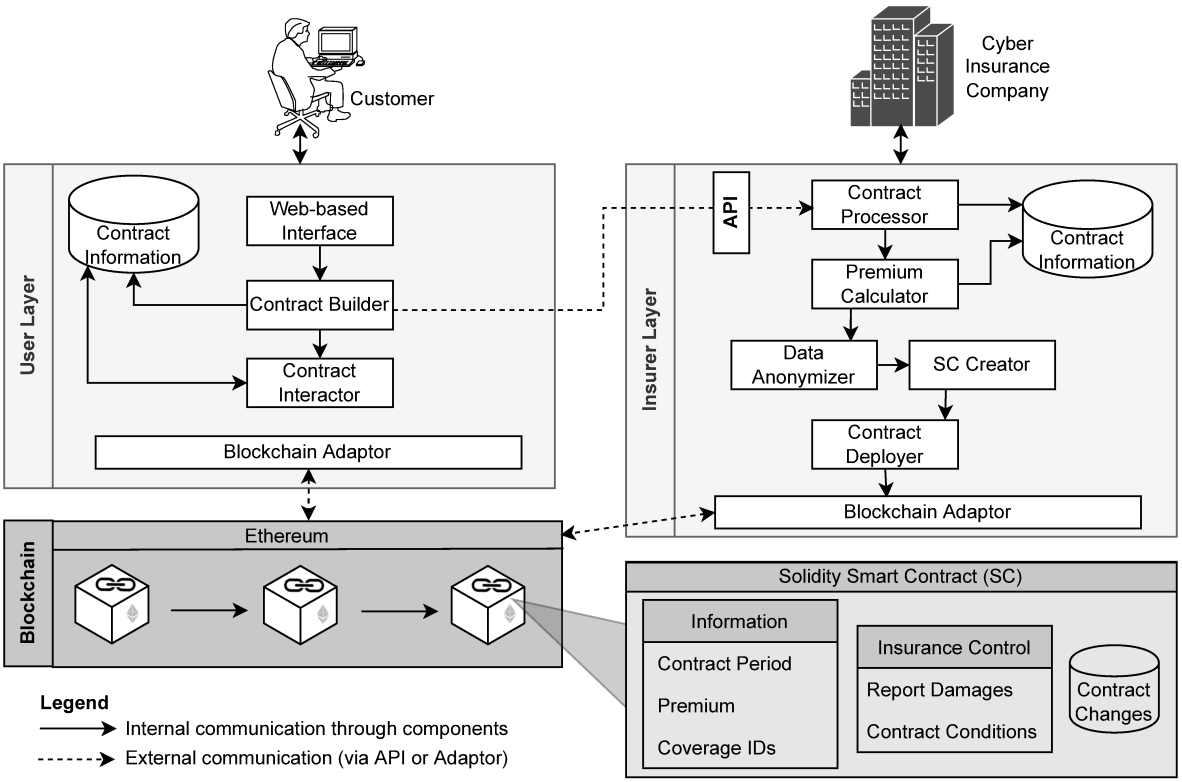


Figure 4.27: Example of Information and Flows for the Application Scenario

makes the collaboration between companies critical for the following years since it is impossible to plan better cybersecurity without sharing information between key stakeholders.

There are different initiatives placed to build communities and alliances that rely on a code of engagement for information sharing [53, 152], provide incentives for collaborations between companies [228], and also platforms that simplify the process of sharing information about security incidents [79, 212]. In this sense, there are still opportunities for approaches that focus on the economic aspects of cybersecurity, enabling not only to share characteristics of attacks but the impacts that certain types of attacks cause in the business, such as how much financial loss due to the attack and the costs of mitigation and recovery measures. In this direction, the **SHINE** is proposed [76] as a solution to enable the sharing of economic information between companies and their partners, thus providing a better view of the economic impacts of cyberattacks and supporting cybersecurity planning and investments.

SHINE is an information-sharing module developed as an extension for the SecGrid solution (*cf.* Section 4.5) that allows for the understanding and sharing of information regarding economic im-

pacts due to cyberattacks within a sector or company. The SHINE solution allows companies to *(i)* share overall economic impacts of a company in a year or for specific attacks, *(ii)* upload technical details regarding an attack (*e.g.*, PCAP files or Netflow records) and its associate costs, *(iii)* obtain an overview of the different sectors in an anonymized way, and *(iv)* share insights of a cyberattack with key partners or interested stakeholders. Different features are implemented on the top of SecGrid to support all interactions, visualizations, and information offered by SHINE. The source code of the solution is publicly available at [39] and in-depth details of this *CyberTEA* supplementary service can be found at [76].

Figure 4.28 shows the different modules and components designed and implemented by the SHINE solution. First, in the *Economic Module*, all finance-related metrics calculation and analysis are performed, including the computation of cyberattack economic impacts and analysis of cybersecurity measures. There are three components within this module, the *Data Processor*, the *Metrics Calculation*, and the *Measures Analysis*. The data is integrated and transformed in the *Data Processor*. Then it is forward to the *Metrics Calculation* to compute different economic metrics (*e.g.*, NPV and ROSI) whenever needed. The results are used to generate visual analysis through the *Measures Analysis*. The output of this module is made visible to users via the *SecGrid's Communication API* and *Web-based Interface* provided.

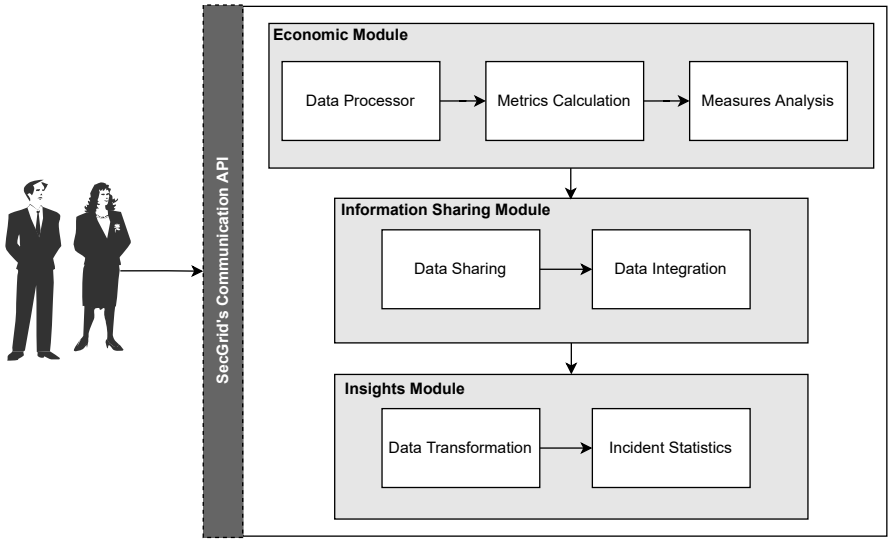


Figure 4.28: Components of SHINE Extending the SecGrid Platform

The *Information Sharing Module* serves as the middleware for data sharing and data integration between *Economic Module* and *Insights Module*. Data from the *Economic Module* goes to the *Insights*

Module just after the *Data Sharing* and *Data Integration* components of the *Information Sharing Module* processes it. This processing includes the definition of which data and calculated metrics are going to be shared, and also it has to be integrated (*e.g.*, per sector or company).

Finally, the *Insights Module* is in charge of generate statistic information (*e.g.*, impact, asset, and adversary) about cyberattacks using the *Incident Statistics* components. This information will be used to build visualizations and reports on the Web-based interface provided by the SecGrid solution. The *Data Transformation* is responsible for handling and integrating data that might come from different sources, such as technical data coming from automated analysis of PCAP files and adversary data coming from the company's manual input.

The integrated and transformed data passes into the *Incident Analysis* component for more specific and in-depth statistics and analysis. This component provides multi-dimensional and multi-faceted statistics and analysis, including analyzing cyberattack impacts, the inspection of attackers' motivations, and the statistics of targeted assets/systems. These analyses help companies fully grasp their cybersecurity risks and help them improve their cyberattack countermeasures. Meanwhile, they can help companies get inspired and develop their network security strategies. These analyses allow companies to perform targeted vulnerability repairs and security upgrades on their vulnerable applications and systems.

Examples of information that SHINE supports include: income loss, productive loss, SLA loss, indirect loss, duration of the attack, targets, type of attack and affected assets/systems, cost to recovery, and discovery method used to understand the incident. This is not an exhaustive list, since additional metrics are also supported. Therefore, it is possible to see that different elements and key details can be shared with interested stakeholders. Then, by using visual representations and reports provided by SHINE, companies can better understand the cybersecurity situation and economic impacts on their sector, supply chain, and their own company. Figure 4.29 highlights some economic impact information being shared using SHINE. Besides that kind of information, *Basic Information* regarding the business and its sector and many technical details regarding the *Incident Information* can be shared using the form.

Sharing Information and Analyzing Cybersecurity Trends using SHINE

Suppose that a company wants to review the overall situation of the cyberattacks in the last year to find a reference for which categories of cybersecurity to pay attention to or invest in for the following year. Suppose that relative datasets and sufficient information have been uploaded and shared by other users using SHINE, and all information is available. Because the more information sets are in-

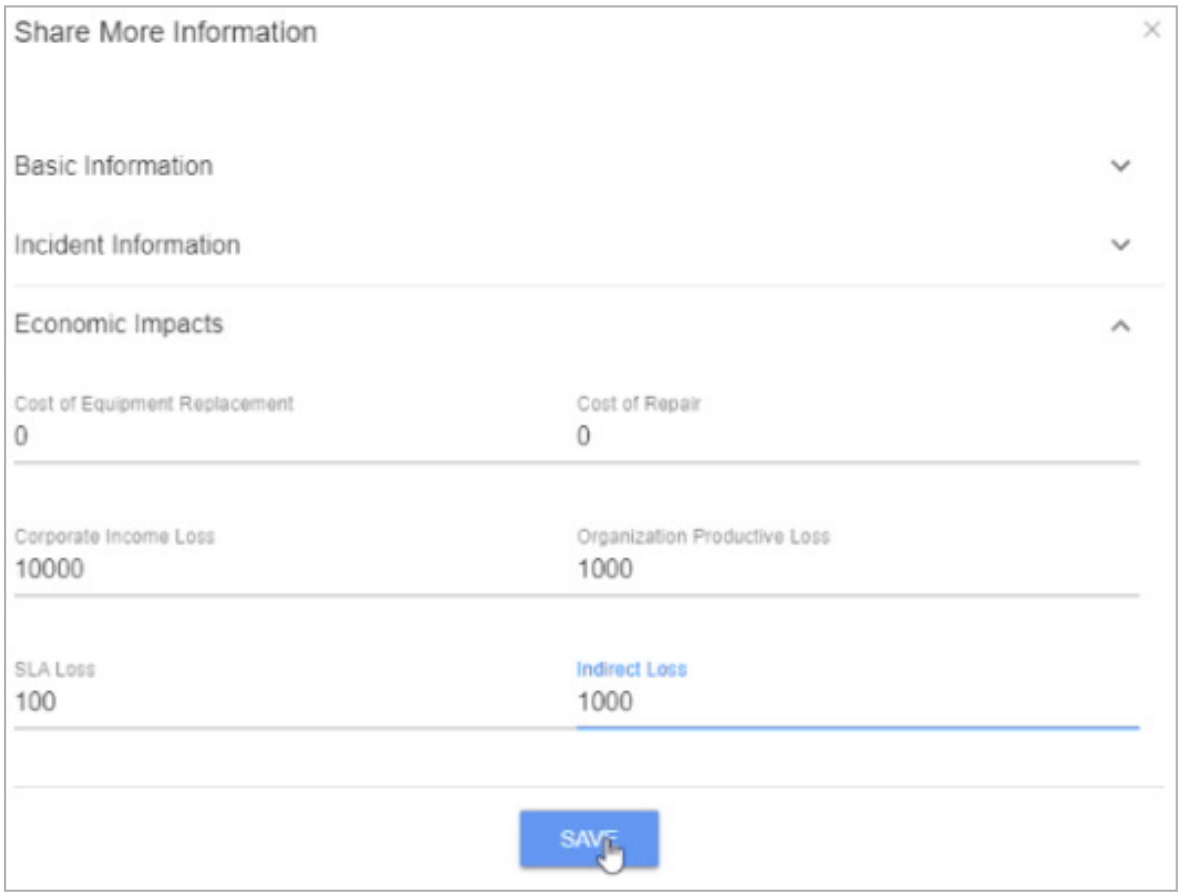


Figure 4.29: Example of SHINE's Form for Submission of Economic Impacts

cluded, the more reasonable and comprehensive the results are, the user (*i.e.*, companies) is supposed to acquire information from others' shared datasets and upload his/her datasets.

Figure 4.30 shows the SHINE dashboard with the most critical results of economic impact and incident statistics regarding the under analysis. The first chart in the economic view tab is a time distributing chart concerning monthly losses caused by cyberattacks. The user could obtain some insights from this visualization, for instance, which month of the year is more vulnerable to all types of cyberattacks. The second one is a pie chart showing the proportion of losses caused by various cyberattacks in a certain period for all sectors. From this visualization, the user could find the cyberattacks that lead to the most severe financial aftermath for her/his business.

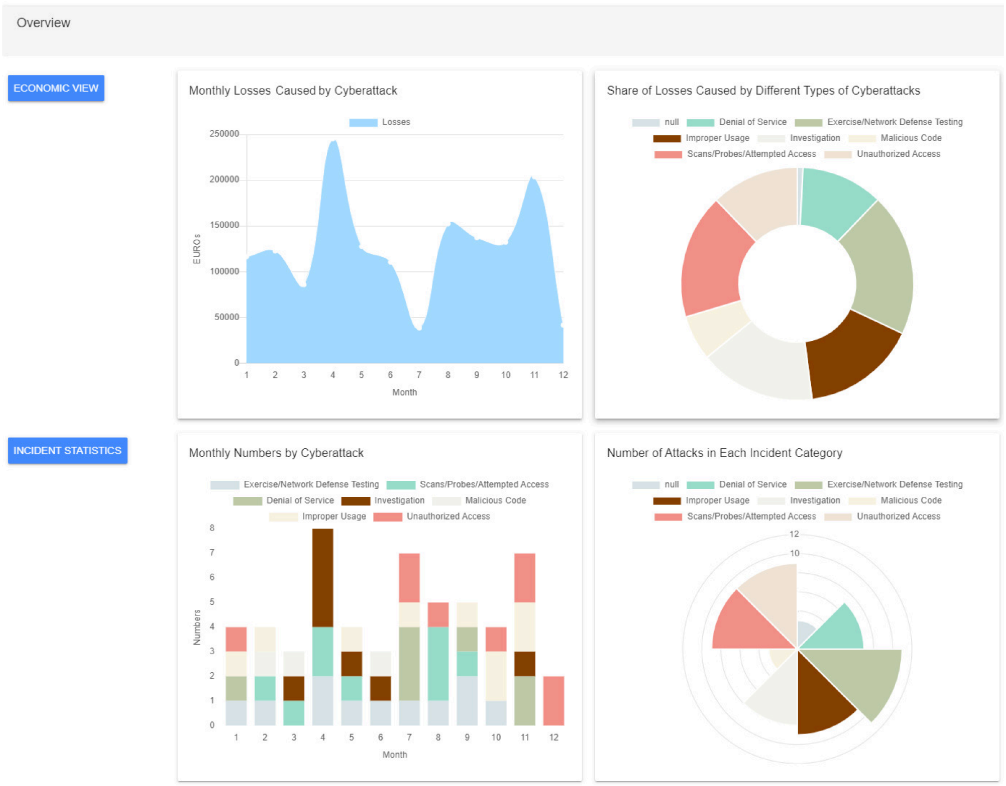


Figure 4.30: Company's Overview Page provided by SHINE

The first visualization shows a stacked bar chart reflecting monthly numbers of cyberattack incidents occurring in an organization for the incident statistics section. Each of the bars shows the number of attacks each month, while each of the colors composing the bar represents the number of a type of attack. For example, the gray part in the first bar means that the Exercise/Network Defense Testing in January appears once. This chart could uncover either the composition of attacks appearing each month or the overall number of attacks across the year. The second visualization then shows a radar chart demonstrating the number of attacks in each incident category for an organization in a year. Each sector color represents an incident, and a larger space of color reveals the higher occurrence probability of a cyberattack incident.

Also, the user can move to the *Sector View* page and select the sector of his/her company in the business profile. For this example, the Finance sector was selected. As over ten features are contained in the sector view to enable the user to have deep analysis results of the entire sector and find the features easier, a menu on the left of the section name is offered to select a particular category of metrics (*i.e.*, Impact Analysis, Adversary Analysis, Attack Analysis, Asset Analysis, and Discovery Method Analysis). Figure 4.31 shows the view of the sector, when selecting the statistics regarding

Impact Analysis. This consists of impact rating, loss duration, security compromise loss property, and incident effect. This helps the company to understand economic-related information related to cyberattacks in the Finance sector, which include the duration of the attack, the losses identified, how relevant was the attack to the company, and when an attack was compromised or not, the security of a company in the same sector.

Figure 4.31: Impact Analysis of Cyberattacks using the Sector View

This application scenario shows benefits for companies that want to gain and share insights on cyberattacks, especially the economic impacts. As can be seen, SHINE allows them to collect, process, and calculate the relative uploaded attack information and gives out intuitive interfaces and visualization results. The insights are organized in several levels and aspects. For instance, the user can check the most critical features and results using an Overview Page, such as which types of attack occur the most or generate the most significant losses. To inspect the overall conditions of a specific sector, the

user could switch to the Sector View and have access to additional reports. Furthermore, the solution provides interesting results about economic impacts.

Based on that, and taking the SHINE solution as an example, solutions of its kind can contribute to companies and interested stakeholders better understanding the cyberattack scenarios they are facing (or will face). By enabling the sharing of companies' insights and information regarding technical and economic impacts, solutions can promote more collaborative cybersecurity to build more robust and efficient cybersecurity strategies for a company or even an entire sector. As discussed in Chapters 2 and 3, this problem being highlighted and addressed by SHINE is still a challenge for the cybersecurity field and a key element for building threat intelligence.

4.8.3 Marketplace and SLA Monitor for Cybersecurity

Trust management in distributed systems has always been a topic of active interest in the research community to understand how to foster and manage the trust. In this sense, Distributed Ledger Technologies (DLT) and BC emerge as an alternative for shifting trust assumptions between users to the protocol that regulates the interaction, fostering trust in distributed systems. Especially, reputation management systems [26] have enabled several applications to be revisited as applications running based on an underlying distributed system. Thus, a clear understanding of major properties, threats and vulnerabilities, and challenges of reputation systems based on different DLTs and BCs (*i.e.*, , permissioned and permissionless) is key to determining their usefulness and optimization potentials. In this sense, a use case of a BC-based reputation system within the context of the cybersecurity market illustrates such benefits and drawbacks of exploiting DLTs for reputation systems.

In order to address the challenge of trustworthy reputations and SLA for cybersecurity providers, the **Kirti** solution [44] is proposed as a supplementary service of the *CyberTEA* approach. Kirti is a BC-based reputation system for the cybersecurity market, including automated SLA enforcement. Kirti's key scientific design consists of developing reputation systems integrated with SLA enforcement while remaining intuitive for end-users' usage. In order to provide a full-fledged platform, a basic marketplace is also developed and integrated, which allows service providers to upload protection services and customers to buy and rate said services. The underlying reputation system was designed considering different attack vectors regarding rating fraud. The SLA details of all services uploaded by providers are automatically encoded into SCs, which handle the underlying protection service's payment, compensation, and termination. Further, the system allows the integration with external parties, such as the recommendation system implemented by MENTOR (*cf.* Section 4.7), by exposing reputation data via a RESTful API.

As mentioned, the ultimate goal of Kirti is to implement a decentralized reputation system for cybersecurity providers, including the generation and enforcement of SLAs using SCs. For that, Kirti allows the upload and purchase of cybersecurity solutions whose SLA terms are encoded into SCs running on a BC, providing automatic customer compensation in the event of agreement violations. Major system events, such as uploading customer reviews and checking provider reputations, are fully auditable by notarizing them in the BC and storing a reference to the BC record (*i.e.*, transaction hash). Kirti's reputation system is designed following a decentralized approach to resist specific attacks, such as Ballot Stuffing and Bad Mouthing. Additionally, its reputation data is available to external parties via a provided RESTful API. Figure 4.32 introduces the conceptual architecture of Kirti and describes its main components, showing the main functionalities and actors supported by the solution.

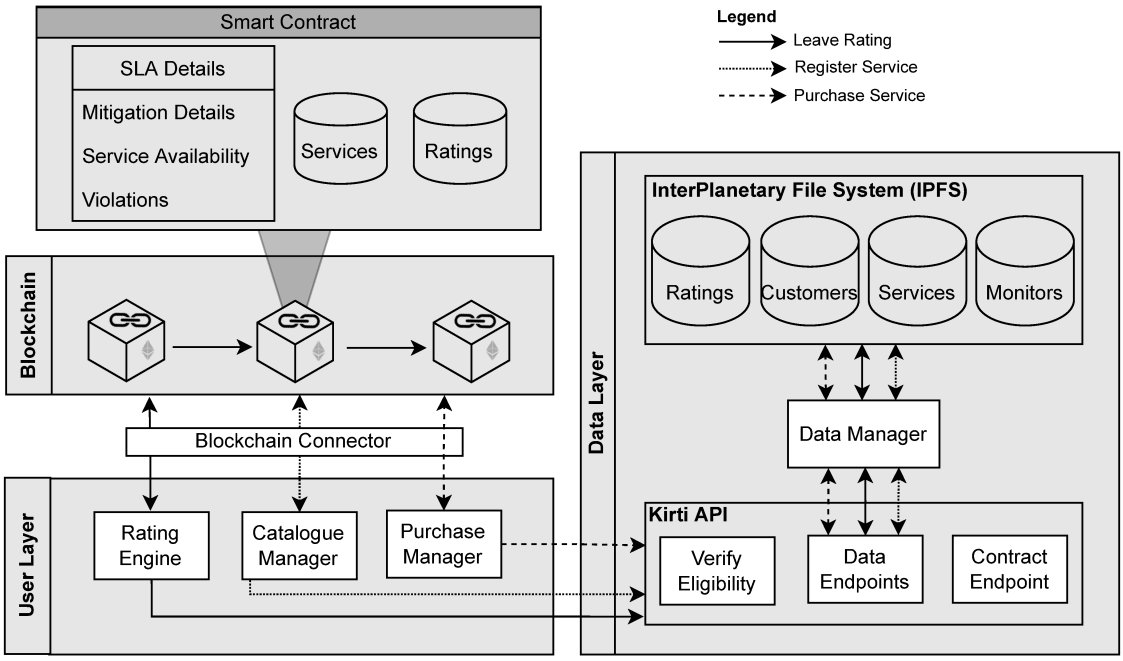


Figure 4.32: Kirti Architecture

The User Layer provides a front-end, allowing users to interact with the system. Users can be divided into two groups: Those selling and those buying protection services, referred to as service providers and customers, respectively. The Catalogue Manager displays the currently available services in the system and provides SPs with an interface to list a protection service up for sale. The Purchase Manager enables a customer of Kirti to purchase a protection service and informs him about the current state of her/his purchased SLAs. This information includes the current violation count and the

time until the SLA expires. Figure 4.33 depicts a summary of an example of an SLA defined and listed using the Kirti's Web-based interface.

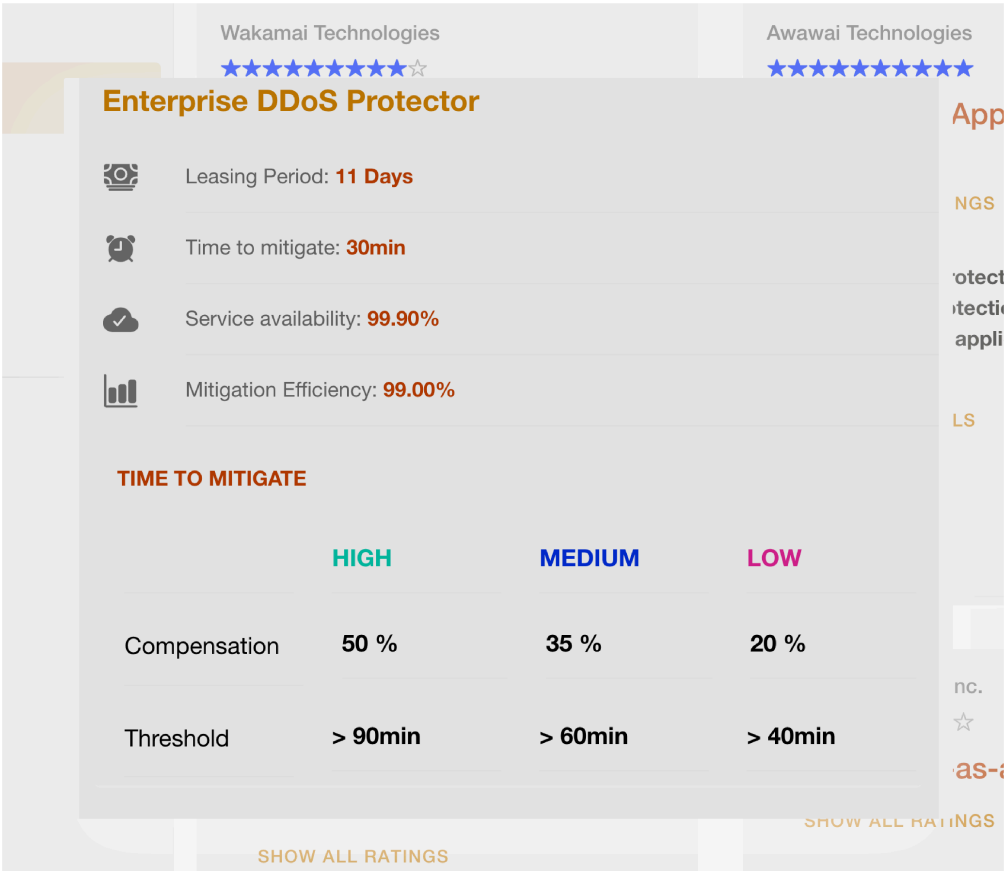


Figure 4.33: SLA Details of a Protection Contracted using Kirti Solution

An appropriate data storage mechanism had to be identified to design Kirti in a decentralized manner. The storage of data in the BC seems initially a possible approach. However, the associated costs are prohibitive. All computations on Ethereum have an associated operational cost measured in terms of gas. The price for a gas unit is termed as gasPrice and most commonly specified in units of Wei, where a certain amount of Wei equals one Ether. The storage operation of 256 bits carries a computational cost of 20,000 gas [244]. Therefore, storing data on the blockchain is very expensive.

Thus, the InterPlanetary File System (IPFS) emerges as a feasible alternative to circumvent BC developers' data storage problem. Regardless of the size of the uploaded content on IPFS, the cryptographic algorithm SHA-256, most commonly employed in IPFS, always returns a hash of 32 bytes. Hence, the data storage overhead can be effectively reduced by uploading data to IPFS and storing only the associated 32 byte-hash in the BC.

Kirti was designed to make reputation data available for external parties via a RESTful API from the external communication perspective. However, the data retrieval is slow using a BC, which approaches unsuitable for some scenarios. Therefore, IPFS also becomes a suitable storage medium as it harnesses the power of decentralized storage while allowing for quick data access. In an endeavor to maximize data verifiability in Kirti, each major event triggered by a customer is first recorded in the BC before being stored in the data layer. The service upload by a service provider, rating generation by a user, and an SLA contract creation are all handled similarly. In this way, audibility and transparency are ensured. Each customer rating includes the transaction hash of the transaction triggered by the Data Registration SC. Assuming a production deployment to the Ethereum main net, each rating could be audited by verifying the transaction details via the transaction hash.

The Kirti solution was implemented using different technologies. The front-end was implemented using the Ionic Angular mainly because of its support of Typescript. Ethereum was used as the BC platform and Solidity as the SC language. For the IPFS layer, the OrbitDB was used. The source code and all documentation required to run the Kirti is publicly available at [1]. An in-depth description of all details and the development process of Kirti is available at [44].

Example Use of Kirti in the Cybersecurity Market

To showcase the system's functionality in a real-world setting, suppose a user of Kirti is either a service provider, a customer, a monitor, or an external party interested in the reputation data of cybersecurity services. As a first step, the owner of a monitoring solution named ArgusEyed is interested in acting as a monitoring solution for Kirti. The owner then makes a POST request to the end-point of the Kirti RESTful API and receives a successful message confirming the monitoring solution's registration at the BC and the IPFS Data Layer. Therefore, now the solution is selected as the monitoring solution for a deployed protection service.

Next, assume that the provider Piranha Networks wants to make his/her protection service Piranha Web Application Firewall (WAF) available to customers via Kirti. Thus, he/she navigates to the appropriate section in the front end to enter her/his service's general details and its SLA specification, which takes no more than two minutes. Upon confirming the service upload, the provider is informed by a popup that her/his service upload was successful and is displayed the hash of the transaction which registered her/his service upload with *registerService()* of Kirti.sol.

Now supposing that a specific customer is interested in purchasing a WAF to secure his/her Web application. He/She navigates to the overview of available protection services in the front-end, as shown in Figure 4.34. After a short inspection and comparison of a potential solution, he/she opts

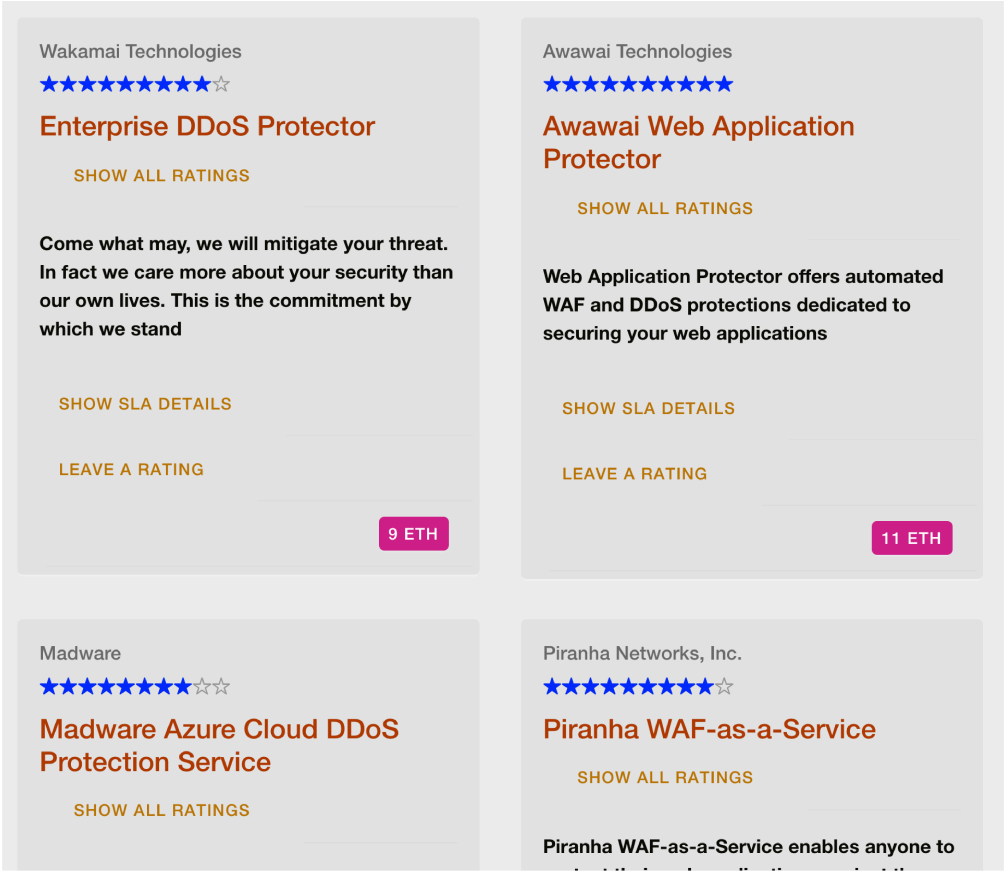


Figure 4.34: Kirt's Marketplace and Catalogue

to purchase Piranha WAF-as-a-Service as the service that matches his/her technical requirements, offers a generous SLA compensation, and is well rated by fellow customers. The fact that he/she can verify each review on the Ethereum BC further increases his/her trust in the validity of customer ratings. After confirming the purchase, the front-end displays a popup asking the customer to select a service in charge of monitoring the protection service and reporting violations to the SLA SC. After selecting ArgusEyed as the monitor, a popup shows that an SLA SC as encoded by SLA.sol has been deployed at address *0x545d8...4D91FCAc*. Next, the MetaMask (a BC wallet plugin) pops up, with the transaction details regarding the newly created contract's address and its price already filled out. The user now has to confirm the transaction.

If the transaction was successful, the user is informed and may also verify the transaction details. The user may now navigate to the My Services section of the Kirti's dashboard to inspect the current state of his/her newly purchased service, as shown in Figure 4.35. Of particular importance is the *Current Compensation* field, which displays the up-to-date value of the SLA's compensation as calcu-

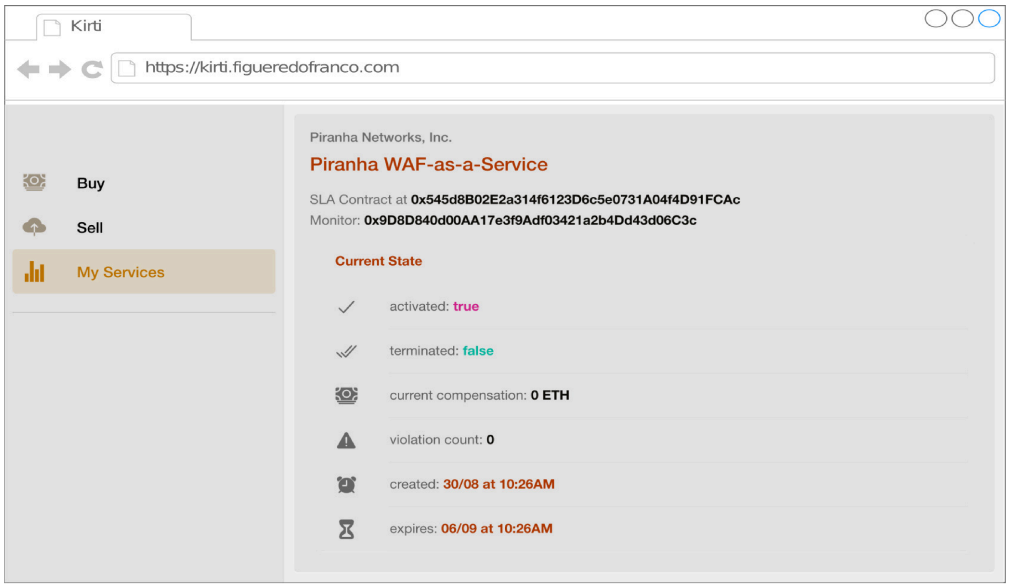


Figure 4.35: State of a User's Service

lated by the number and severity of reported violations. Now that the SLA SC is activated through the user's payment, the monitor must check the deployed protection service. Suppose now that a DDoS attack on the customer's Web application occurs. Luckily Piranha WAF-as-a-Service includes DDoS protection. While the attack is successfully mitigated, the monitor notices that the mitigation took 62 minutes instead of the promised 30 minutes specified in the SLA agreement.

The monitor may now call the */contracts/0x545d8...4D91FCAc/thresholds* endpoint to receive information about the SLA's threshold values regarding the violation. Using the obtained data, he/she concludes that he/she should report a violation of the severity medium of the Time to Mitigate metric. Note that to make a successful request to contracts/:address/violation, a monitor must include a message and signature to verify her/his identity. The monitor then generates a unique message and signature using Ethereum's Elliptic Curve Digital Signature Algorithm (ECDSA).

```
{
"message": "b9f9e1ee -55e9 -4 df7 -a83a - d5156813e192",
"signature": "0 x4184f ...24 fef00",
"violationType": 0,
"violationSeverity": 1
}
```

Listing 4.5: Request Body Reporting a Medium Severity Violation of the Metric "Time to Mitigate"

The monitor now sends an HTTP POST request to */contracts/:address/violation*, including the obtained values for message and signature, as highlighted in Listing 4.5. Note that the values of 0 for *violationType* and 1 for violationSeverity correspond to Time to Mitigate and medium, respectively. A monitor is informed about the encoding scheme regarding both violationType, and violationSeverity in the response body of a call to */orbitdb/monitors/add*. Meanwhile, the customer sees in the front-end that a violation has occurred. The current compensation has been updated to 2.45 Ether (*i.e.*, 35%) compensation at a price of 7 Ether). After seven days, the service and its associated SLA SC expires, and the contract terminates by refunding 2.45 Ether to the customer and releasing the remaining funds to the provider.

Finally, after the contract is finished, the user can provide feedback in the form of a rating. For that, the user can evaluate the different dimensions of the services, such as features, price, usability, the accuracy of the promised protection, and the support received from the provider. Figure 4.36 shows an example of the interface provided by Kirti for the rating process.

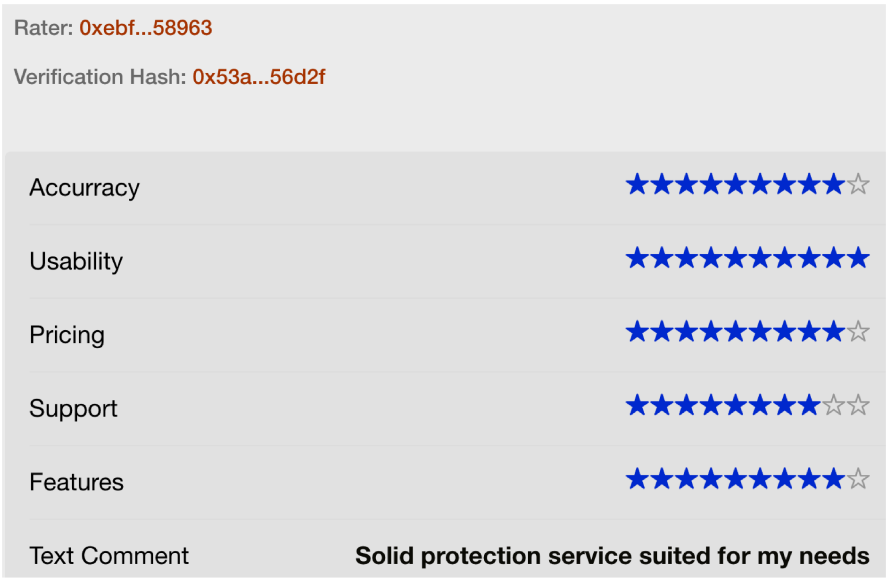


Figure 4.36: Rating of Service using the Kirti's Interface

4.8.4 Infrastructure as a Service (IaaS) for the Deployment of Protections

Once the end-user acquires protections, they need to deploy it in their or third-party infrastructures that satisfy specific requirements. This is the case for Virtual Network Functions (VNF) that implement security (*e.g.*, virtualized firewalls, DDoS mitigation, and Deep Packet Inspection) [17, 95] and

network functions [34], which have to be deployed in an infrastructure that supports Network Functions Virtualization (NFV) and dynamic resources allocation [115]. Suppose the end-user does not own a physical substrate to host acquired VNFs. In that case, the user can still choose between hiring generic infrastructures (*e.g.*, Amazon AWS or Microsoft Azure) or marketplaces' infrastructures. In both cases, companies usually expose the conditions and prices of their services in an open fashion, *i.e.*, any user can observe the market and pick the more affordable or suitable infrastructure. Competition, in this case, is open but relatively static: prices are not tailored according to end-users demands. The introduction of strategies enabling real-time, user-tailored competition between Infrastructure Providers (InP) favors lower prices and also contributes to the expansion of marketplaces for VNF while meeting specific demands of end-users [113]. Both established and new InPs can achieve a large audience and offer their infrastructures by estimating costs based on each demand according to their current business model (*e.g.*, lower prices for a firewall with more significant memory than one with CPU core demands). To address such issues, the concept of reverse auction mechanism [240] has been used over the years to enable an efficient and flexible approach to support fair and auditable competition between providers.

Inspired by these concepts, a solution named **BRAIN**, a blockchain-based reverse auction for infrastructure providers [91], was designed and developed. BRAIN uses SCs to provide competition and reliable records. Such records contain agreements between end-users and InPs during the auction and even bids' history. Thus, end-users can benefit from lower prices, while InPs can offer their infrastructure to a broader audience. The proposed solution determines a straightforward path to integrate it with generic marketplaces, since a few components should be inserted inside marketplaces catalogs, while the remainder of the solution is running in a distributed way. Marketplaces must only implement a parser to create SCs regarding available information and run a component to control the auction (*i.e.*, Auctioneer). By looking at the framework of the *CyberTEA*, BRAIN is proposed and developed to be a supplementary solution that can support, whenever is the case, the process of selecting infrastructure to deploy virtualized protections in companies without in-house infrastructure. Although BRAIN showcases a VNF scenario, this can be extended to any marketplace for protections that need specific performance and resource demands.

BRAIN explores the concept of the English reverse auction [171] to define how bids are processed. Bidders place their bids in a sealed envelope and simultaneously hand them to the *Auctioneer*. Envelops are then opened, and the bidder with the lowest bid wins, paying the amount bid. Based on this, concerning a VNF-as-a-Service (VNFaaS) scenario, InPs will send their bids without knowing the amounts placed by other bidders. All such bids will be recorded in the SC, which will reveal the winning bid only, when the auction ends. After the auction, the information about the auction

will be available to the other bidders for audition purposes. Such reverse auction is supported by a blockchain implementation that guarantees a joint trust assumption between InPs and end-users. Therefore, each bid is processed as a blockchain transaction from the InP to the SC, defining the correspondent auction.

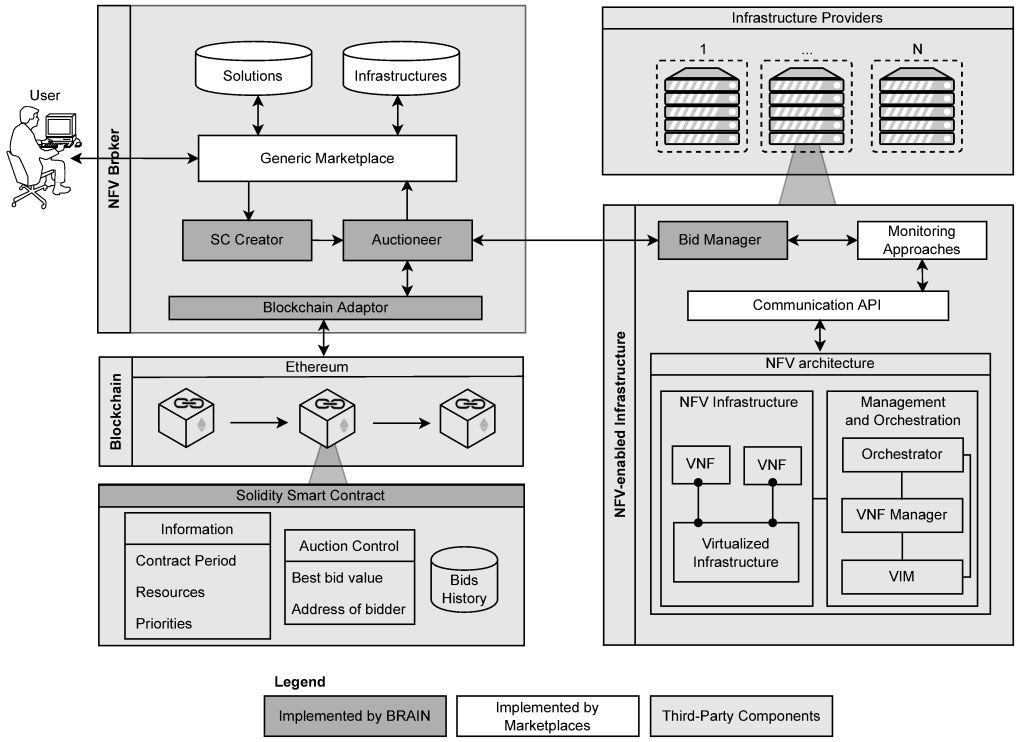


Figure 4.37: BRAIN Architecture

Figure 4.37 presents the architecture of the BRAIN solution. White boxes represent optional components that should be implemented by marketplaces or InPs that desire to use the proposed auction solution, while the dark gray boxes highlight the BRAIN components. The *NFV broker* is the entity that manages and offers VNFs. Thus, current marketplaces can be viewed as brokers implementing the auction components inside their architecture to support BRAIN. Additionally, every candidate NFV-enabled infrastructure is implemented following the ETSI standards [58] for NFV management and orchestration. Thus, InPs in such an approach can host VNFs and end-users to sustain their demands, when renting/deploying VNFs, since their infrastructure is not available. In addition, this may simplify VNF deployment after the auction conclusion. The chosen InP is aware of the VNF configurations, and code can be quickly deployed to offer the service according to end-user preferences.

The architecture flow is described as end-users first accessing a catalog (*i.e.*, marketplace) and acquiring a VNF. Next, priorities defined by end-users during the acquisition process and requirements of the selected VNF are sent as a Profile Descriptor (PD) file to be processed by the *SC Creator*. The PD is a structured JSON file. Then, the *SC Creator* processes the information received and created an SC according to the specifications. After its creation, the SC is sent to the *Auctioneer*, which deploys the SC in the blockchain and communicates the InPs, via an interface provided by the *Bid Manager*, that an auction is opened. In addition to establishing communication, the *Bid Manager* also implements algorithms that will issue automated bids according to their configuration and the infrastructure status (*e.g.*, resources available and costs). The *Auctioneer* can send a command to the SC to finish the auction and return the best bid. Finally, after knowing which is the best infrastructure, the *Auctioneer* forwards it to the marketplace, and the process of VNF deployment can be started as implemented in the NFV Broker.

A prototype was implemented to demonstrate the feasibility and effectiveness of the BRAIN solution, taking as a scenario the offering infrastructures to host VNFs (*e.g.*, virtualized firewalls, proxies, and Deep Packet Inspection). The source code is available at [148]. The Python programming language was chosen, in its latest version 3.7.1, to implement the auction mechanism. This decision was due to multiple programming paradigms' possible support and focus on code readability. The development integrates well-defined libraries to deal with blockchains and SCs. Flask 2.0.3 implemented the RESTful APIs supporting the communication between components.

SCs were coded using Solidity 0.4.24, an Ethereum contract-oriented programming language. In order to validate such implementations, the Ganache Framework in its latest version was configured and executed to simulate the blockchain where the SC will run. It allows for creating a development blockchain to run tests, execute commands, and inspect states. Ganache itself provides the Remote Procedure Call (RPC) server. Thus, a behavior similar to the Ethereum blockchain and its operations can be emulated to support calls from all auction components.

Payment issues are out of the work scope. However, BRAIN was designed generically to be integrated with innovative payment methods that address the auction phases and a VNF billing. Automatic payments can be implemented by using the Ethereum cryptocurrency Ether. To this end, the payment can be processed inside the blockchain, and transactions containing the respective value can be done between different wallets (*e.g.*, end-users pay directly to InPs). Monitoring tools (*e.g.*, BC-based SLAs monitors and malicious behavior detectors) can be helpful to measure if stakeholders (*i.e.*, end-users and InPs) involved in the auction are complying to contract clauses, thus, executing the full payment or applying monetary penalties to the parties that not follow the deal, *e.g.*, when an

InP promises to host a VNF with a specific requirement that cannot be achieved by using the provided infrastructure.

Example of Application Scenario for the BRAIN Solution

Suppose a marketplace that provides a Web-based interface, where the end-user can interact with a catalog composed of specific VNFs for protection. The end-user decides to acquire and instantiate a VNF, but he/she does not operate his/her own NFV-enabled infrastructure. Such a marketplace concept is similar to the one proposed by the FENDE project [34]. Hence, one customer (*i.e.*, end-user) wants to contract a VNF that implements a state-of-the-art firewall for more than one month, which is available to be purchased in the marketplace. The desired VNF has a descriptor (*i.e.*, VNFD) defining as minimum resources for the firewall the following: 4 GB RAM, 2 GB disk space, and 2 CPU cores. Additionally, the end-user requests two additional GB of memory to be used only in unusually high demand periods and defines a maximum latency of 20 ms. With such information, the contracted VNF is instantiated in an NFV-enabled infrastructure. Thus, the marketplace should know the best infrastructure available that supports these demands and provides a cost-efficient solution. For this, the BRAIN solution is executed.

After VNF acquisition by the end-user via the marketplace (*cf.* Figure 4.38), an SC is created by the *SC Creator* component based on the VNFD (provided by the marketplace) and end-user particular demands that were defined during the acquisition. After that, the *Auctioneer* identifies, based on a database request, that there are four infrastructure candidates available to supply the VNF demand. The *Auctioneer* deploys the SC inside the blockchain and sends the SC address to each InP via the RESTful API. Thus, they can obtain information about the end-user request and issue bids based on their implemented algorithms. Table 4.10 presents the information defined in the PD file, which represents priorities previously indicated by the end-user. Note that only the contract period input is mandatory. Other fields are optional for users. Besides this information, the VNFD containing the network service description is also used as an input to the bid calculation.

The bid is calculated by using a customized algorithm that is part of the *Bid Manager* and runs inside each infrastructure. This algorithm obtains information from the SC and calculates the final bid based on resources required, VNF type, and end-users priorities (*e.g.*, maximum latency and geolocalization). Each one of these InPs has its algorithm configured with actual values. Thus, based on the input containing information from the auction, the output with the final bid is provided and recorded on the blockchain. Finally, the *Auctioneer* sends a last transaction to the SC in order to ter-

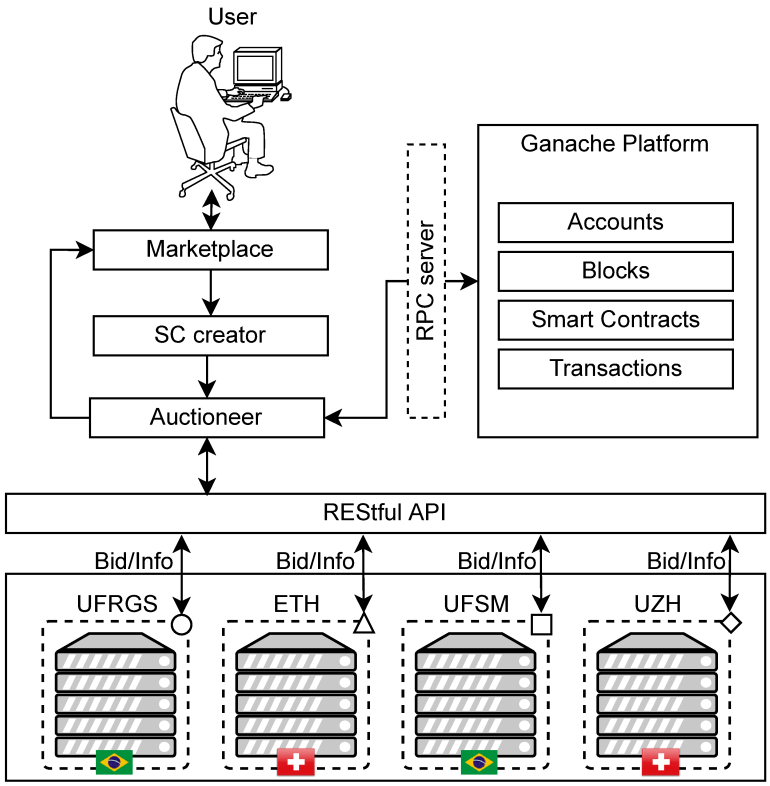


Figure 4.38: Case Study Scenario

Table 4.10: Priorities Defined by End-Users in the Profile Descriptor File

Parameter	Value	Required
Contract period	Weekly	Yes
Geolocalization Preference	South America and Europe	No
Additional CPU	+2 core	No
Additional Memory	+2 GB	No
Additional Disk Space	+20 GB	No
Maximum Latency	10 ms	No
Traffic Supported	10.000 packets/s	No

minate the auction. Hence, the final bid and auction winner is revealed to the marketplace, and the process continues with the deployment of the VNF.

Table 4.11 shows each candidate InP and their available resources. The value calculated for each bid algorithm shows that UFRGS and UZH provide lower prices to supply VNF demands. These lower prices are due to the number of resources available and their cheaper operational costs (*e.g.*, infrastructure optimized to deal with firewalls with high demands) to host the VNF. Note that it is

not guaranteed that the infrastructure with more resources will provide the best price. The final bid depends on several factors defined inside the bidding algorithm, presenting the business model. In such a case, UFRGS provides the best bid. Therefore, the *Auctioneer* will let the marketplace know the bid value and the UFRGS address of the blockchain.

Table 4.11: Infrastructure Providers Overview

Provider	Country	Free Resources	Final Bid
University of Zurich UZH	Switzerland	40 CPU cores 128 GB memory 15 TB disk	US$ 49.22 monthly
Federal University of Rio Grande do Sul (UFRGS)	Brazil	20 CPU cores 3 2GB memory 1 TB disk	US$ 43.63 monthly
Federal University of Santa Maria (UFSM)	Brazil	4 CPU cores 16 GB memory 1 TB disk	US$ 55.02 monthly
Swiss Federal Institute of Technology (ETH)	Switzerland	5 CPU cores 32 GB memory 2 TB disk	US$ 59.18 monthly

Finally, the communication between the marketplace and UFRGS to effectively deploy the VNF starts. UFRGS has to deliver the promised performance and resources; if that is not delivered, mechanisms to punish such an InP can be defined based on the SC (*e.g.*, compensations or reputation decreased).

4.9 Solution's Overview and Key Takeaways

The methodology described by the *CyberTEA* approach shows the key phases, steps, elements, and information required for adequate cybersecurity planning and investment. This contribution is relevant to helping companies, especially those without a technical expert, understand the nuances of cybersecurity before implementing a cybersecurity strategy. The methodology can be extended to address other elements and information, but its current version summarizes the most critical details. This is one of the contributions that allows moving in the direction of investigating the components and solutions required to apply this methodology in companies.

Table 4.12: Overview of Solutions Implemented as part of the *CyberTEA* Approach

Solution	Description	Phase Addressed of the Methodology	Components of the Framework Implemented
SecRiskAI [92]	A ML-based tool for risk assessment in companies	Phase A and B	Business Layer and Risk Analyzer
SecBot [86]	A conversational agent for cybersecurity planning and management	Phase A and B	Business Layer and Threat Advisor
SecGrid [90]	A platform for the analysis and visualization of cyberattack traffic	Phase B	Data Processor, Threat Advisor, and Risk Analyzer
SECAdvisor [173]	A GL-based tool for optimal investment in cybersecurity	Phase D	Cost Estimator and Investment Calculator
MENTOR [88]	A recommender system for protections	Phase C and D	Recommendation Engine
ProtectDDoS [89]	An extension of MENTOR for recommendation of protection against DDoS attacks	Phase A and C	Business Layer and Recommendation Engine
SaCI [81]	A BC-based cyber insurance model	Phase B	Supplementary Layer
SHINE [76]	An economic information sharing module for the SecGrid platform	Phase B	Supplementary Layer
Kirti [44]	A BC-based marketplace and SLA audit system for the cybersecurity market	Phase C and E	Supplementary Layer
BRAIN [91]	A BC-based reverse auction for infrastructure providers	Phase E	Supplementary Layer

As a second contribution, introduced in this chapter, a framework was proposed highlighting all components, actors, and relationships required to consider, when designing, implementing, and integrating solutions to satisfy the requirements of cybersecurity planning and investment. The third contribution includes introducing a set of novel solutions designed and implemented to address the different phases of the methodology while also satisfying all components of the framework. Most of these solutions are already integrated (*i.e.*, via APIs) to work as an ecosystem for cybersecurity, thus providing and obtaining key information, when needing to perform tasks required by companies to achieve a proper cybersecurity strategy and level of protection.

Table 4.12 summarizes all solutions developed. It highlights which methodology's phase is addressed and which framework's components are implemented by each proposed solution. Therefore, as can be seen, all phases of the methodology (*cf.* Figure 4.1) and components of the framework (*cf.* Figure 4.2) are covered by at least one solution. Thus, these solutions address specific challenges and issues of cybersecurity and show clear examples of how cybersecurity planning and investment tasks can be addressed by using simplified mechanisms, user-friendly interfaces, and trend technologies. It is important to note that these solutions do not aim to provide a final answer for the problem

of cybersecurity planning but shed light on how to evolve this field with well-defined scenarios and prototypes that can benefit companies.

The contributions described in this chapter provide answers to specific Research Questions (RQ) investigated: RQ2, RQ3, RQ4, and RQ5. The methodology introduced at the beginning of this chapter addresses **RQ2**. The solutions proposed show how to abstract technical details to guide SMEs during the plan and execution of cybersecurity strategy, which answers **RQ4** and **RQ5**. Furthermore, the proposed framework covers **RQ3** by defining the architectural components and actors to integrate all solutions. The evaluations and discussions provided in the following chapters lead to the final answers for all RQs, which is revised in Chapter 6.

Science is a way of thinking much more than it is a body of knowledge.

Carl Sagan

5 Evaluations and Discussions

Different dimensions must be considered during the evaluation to emphasize what is being analyzed, why, and how, thus, highlighting the feasibility of approaches and their actual contributions. The evaluations are organized and conducted to provide measurable results for each one of the contributions of this thesis. The evaluation methodology relies on independent quantitative and qualitative evaluations for each contribution whenever possible, *i.e.*, specific experiments are conducted based on the nature, requirements, and key indicators of the solution under evaluation. These experiments might include performance (*e.g.*, time to execute certain tasks and resource constraints), usability (*e.g.*, questionnaires and case studies), accuracy (*e.g.*, Precision, Recall, and F1-Score), and economic costs associated with the BC-based solutions. Therefore, each evaluated solution has its experiments defined and the results discussed in a dedicated section, followed by a discussion on the experiments and solution's limitations.

This chapter is organized as follows. First, evaluations for each solutions introduced in Chapter 4 are presented. Next, an end-to-end case study is conducted to show an application of the *CyberTEA* approach in a company, thus covering the planning of a cybersecurity strategy and the key investments to fulfill its requirements. Finally, key observations are provided at the end of the chapter to clarify and summarize important findings resulting from the evaluations.

5.1 Prediction of Risks using SecRiskAI

The SecRiskAI solution was evaluated considering a quantitative evaluation to analyze the performance and effectiveness of the proposed algorithms and the features selection. The experiment setup and all results are discussed below.

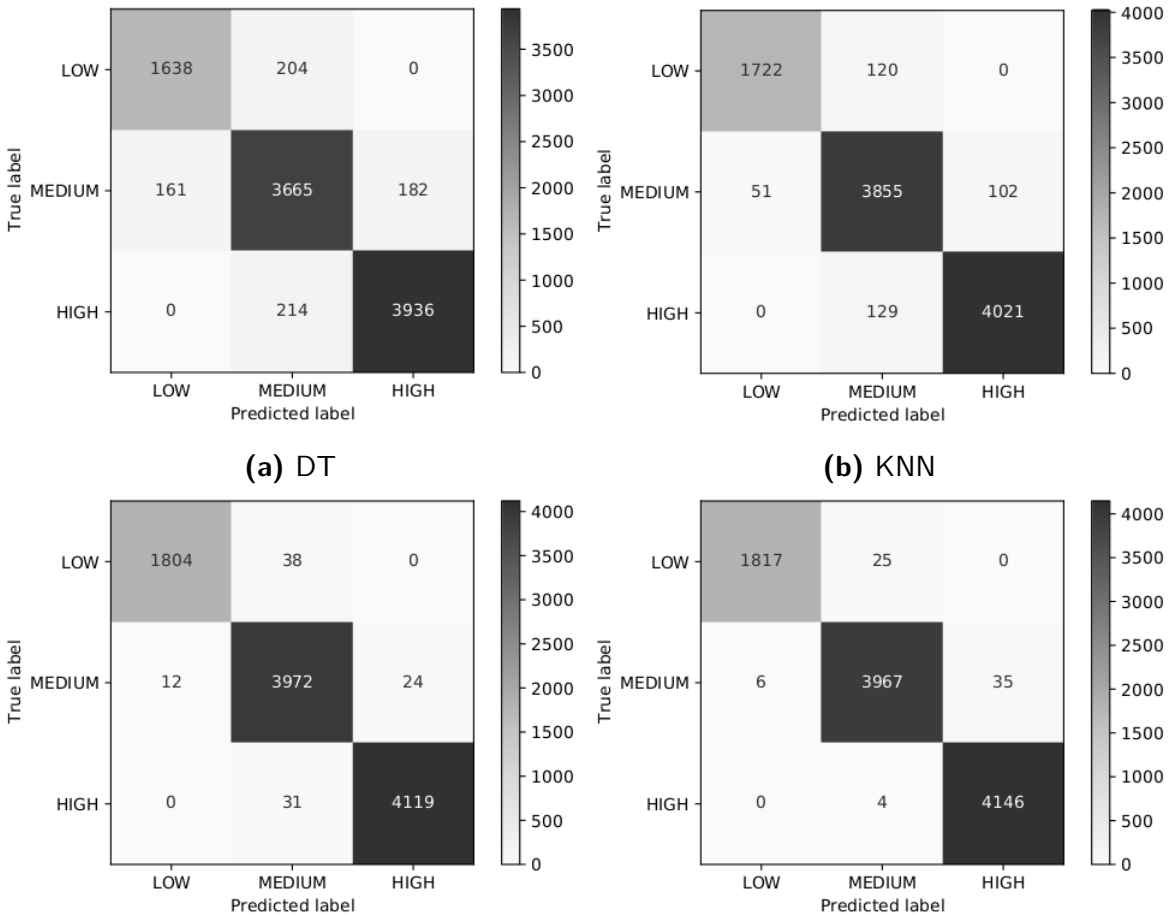
5.1.1 Experiments and Results

The performance evaluation was conducted on a machine using the Apple M1 System on a Chip (SoC) and 16 GB of RAM. For a quantitative evaluation and comparison of the various ML models, the performance metrics of accuracy, precision, recall, and F1-Score were observed. The generation of these metrics is also a significant step in every ML workflow to understand the implemented models' behavior and performance.

The confusion matrix is a widely adopted technique to evaluate the correctness and accuracy of classification models. In practice, confusion matrices can be used for both binary and multi-class classification problems and provide a way to assess and compare the performance of classification models. A dataset containing 50,000 entries was generated to compute the confusion matrix, and an 80-20 train-test split strategy was followed as the most recommended split ratio in literature [132]. After a training and Cross-Validation phase, each ML model was tested using the remaining test set. Examples of the training datasets for widespread cyberattacks and DDoS attacks are available in the training dataset folder available at [56].

This phase aims to test the model on previously unseen data, *i.e.*, data not used during the training phase. The ML model is used to predict the corresponding class for each entry in the test set. Finally, the predicted labels are compared with the actual class, also called true labels, and as a result, a confusion matrix is built. Figure 5.1 shows the confusion matrices generated for each ML algorithm implemented in SecRiskAI.

A confusion matrix defines the summary of prediction results, where each cell corresponds to the number of correct and incorrect predictions, broken down by predicted/true label combination. A best-performing classifier would result in a confusion matrix where only the diagonal is filled with values, meaning that every predicted class corresponds to the actual label. In that case, the model would have achieved an accuracy of 100%. In other words, the accuracy of a model is calculated as the number of correctly predicted classes divided by the incorrect predictions. As shown in Figure 5.1, for the SecRiskAI prototype, every model was able to achieve more than 90% of accuracy.



(a) DT **(b)** KNN

(c) SVM **(d)** MLP

Figure 5.1: Confusion Matrices for the SecRiskAI's ML Model

Table 5.1 shows the computed performance metrics, based on the generated dataset with 50,000 entries. Each model was trained and tuned to maximize accuracy, reduce over-fitting, and provide better results. SVM and MLP achieved similar accuracy scores, although the difference is substantial in terms of computation time. As for the training phase, SVM requires approximately half of the time compared to the MLP model. The training time also impacts the grid search computation time, a hyperparameter technique, which for the MLP model exceeds 200 seconds, since every tuned model undergoes a 5-fold CV. On the other hand, DT and KNN have the fastest training time, while KNN achieved the fastest grid search computation time of around 40 seconds.

Table 5.1: Performance Metrics

ML Model	Accuracy	Training Time (s)	Grid Search Computation (s)
DT	92.64%	0.18	146.77
SVM	99.03%	5.83	149.15
KNN	95.82%	0.08	40.06
MLP	98.86%	10.53	210.55

Based on the confusion matrices presented in Figure 5.1, the important metrics of precision, recall, and F1-score were derived as well. The precision metric expresses the proportion of units labeled by a model that belongs to that class. As shown in Figure 5.1 (a), DT was able to predict a *Low* risk for 1638 profiles out of all predicted profiles (1638 + 161 + 0), resulting in a precision of (1638 / 1799) $\approx$ 91%.

Additionally, the recall metric quantifies a model's predictive accuracy for a particular class, *i.e.*, it represents the ability of a model to find all entries in a dataset that belong to a particular output class. As presented in Figure 5.1 (a), out of 1842 (1638 + 204 + 0) profiles with *Low* as a true label, DT was only able to classify 1638 correctly, resulting in a $\approx$ 89% (1842 / 1638) recall.

The last performance metric considered in this evaluation is the F1-score, which ranges between 0 and 1. This metric aggregates both precision and recall by computing the harmonic mean and compares ML models to determine which one produces the best results. Similar to precision and recall, F1-Score is computed for each output class. Table 5.2 shows an overview of the derived performance metrics calculated for each ML model.

Additionally, the computed performance metrics summarized in Table 5.2 reveal that MLP, despite having a marginally lower accuracy than SVM, was able to achieve an F1-Score of 1.0 for the *High* output class. MLP also marginally outperformed SVM in both precision and recall scores. The small performance gain comes at the cost of training time, which, according to Table 5.1, is generally higher compared to SVM classifiers. This is mainly due to the higher complexity of the MLP algorithm. The other two ML models used by SecRiskAI (DT and KNN) were also able to achieve high precision, recall, and F1-Score. However, similar to the accuracy scores presented in Table 5.1, the metrics presented in Table 5.2 confirmed once again that DT provided the worst performance, despite having faster training times.

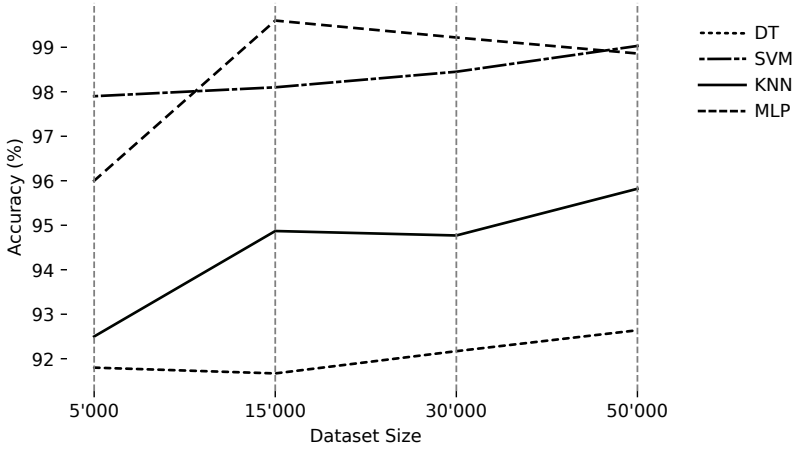
Finally, the impact of the size of the synthetic datasets on both accuracy and training time was investigated. First, datasets of different sizes were generated. Each ML model was equally trained

Table 5.2: Computed Precision, Recall, and F1-Score for each ML model

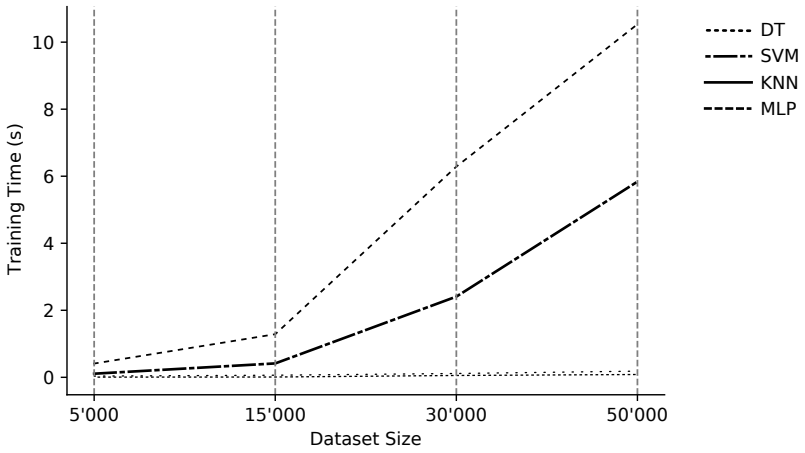
ML Model	Class	Precision	Recall	F1-Score
DT	Low	0.91	0.89	0.90
	Medium	0.90	0.91	0.91
	High	0.96	0.95	0 95
SVM	Low	0.99	0.98	0.99
	Medium	0.98	0.99	0.99
	High	0.99	0.99	0.99
KNN	Low	0.97	0.93	0.95
	Medium	0.94	0.96	0.95
	High	0.98	0.97	0.97
MLP	Low	1.00	0.99	0.99
	Medium	0.99	0.99	0.99
	High	0.99	1.00	1.00

and tuned on every generated dataset using grid search followed by a 5-fold Cross-Validation technique. The results are shown in Figure 5.2. For small to medium size datasets (*i.e.*, between 5,000 and 15,000), the MLP model is able to outperform every other model with an accuracy of almost 100% (Figure 5.2 (a)). Moreover, the impact on the training time is also relatively low, with MLP requiring approximately 2 seconds. However, the outcome is different once the size of the dataset increases. On the one hand, the training time for both SVM and MLP increases drastically, which for MLP leads to a $\approx$ 388% increase with double the dataset size. On the other hand, as highlighted by Figure 5.2 (b), the accuracy of the MLP model suffers a slight decrease while having the highest accuracy score among the other ML models.

Once the generated dataset size reaches over 50,000 entries, MLP performs worst than SVM while requiring twice as much time to be trained. While this may not seem to be a significant difference in seconds, with datasets exceeding millions of entries, the gap may become even more substantial, leading to extremely slow model training and poor scalability. Furthermore, from Figure 5.2 (a), it can be observed that, with larger dataset sizes, SVM has a minimal but constant increase in accuracy. Similarly, KNN and DT also experienced an accuracy gain while maintaining a low training time. Therefore, based on the Figure 5.2, it is possible to conclude that MLPs exceed medium-sized datasets, and SVMs should be taken into consideration, when dealing with large datasets.



(a) Impact of the Dataset Size in the Prediction Accuracy



(b) Impact of the Dataset Size in the Training Time

Figure 5.2: Analysis of the Impact of different Dataset Sizes in the SecRiskAI ML Model

5.1.2 Discussion and Limitations

The quantitative evaluation of the four implemented ML algorithms demonstrated that SVMs achieve slightly higher accuracy for larger datasets while maintaining a lower training time, when compared to the MLP algorithm. Nonetheless, all ML algorithms performed well and achieved more than 90% of accuracy in most cases with the correct training dataset. Moreover, the generated confusion matrices also confirmed that the evaluated ML algorithms could classify most samples correctly. Other metrics (precision, recall, and F1-Score) also provided valuable insights into the performance of the ML algorithm for every output class.

One limitation of SecRiskAI is the current lack of real-world datasets for training the used ML algorithms. To partially circumvent this issue and show the effectiveness of the prototype, a synthetic dataset generation approach was followed. However, although synthetic data mimics various properties and aspects of real-world data, it is usually very challenging to generate high-quality data for complex problems. However, further investigations are still required to determine which is the best information to consider for real-world companies and how each attribute's weight changes according to the application scenario.

If the generated dataset does not match the behavior and properties of the real-world dataset, this will negatively impact the performance of the trained ML models. Also, the current implementation of SecRiskAI supports assessing the risks of DDoS and phishing attacks only. Still, the system prototype is extensible so that new ML models, trained explicitly considering other cyberattacks, can be integrated into the current solution and exposed through the same API. For that, the same ML workflow defined for SecRiskAI can be followed.

5.2 Extraction of Cybersecurity Demands using SecBot

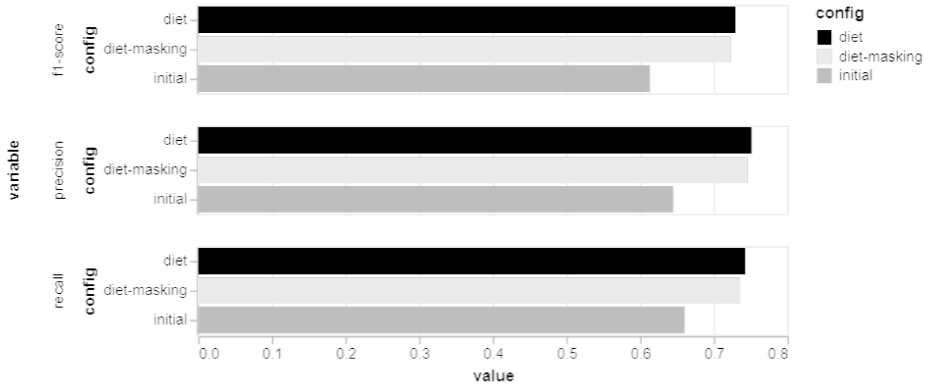
The capacity of SecBot to recognize Entities and identify Intents in conversations is directly related to its feasibility in being used for understanding cybersecurity demands. For that, evaluations have been conducted in terms of accuracy and performance, including the analysis of different configurations to optimize the prototype's performance. The evaluation was performed using a Dell XPS desktop with the configuration of an Intel Core i7-3770 at 3.40 GHz, 32 GByte of RAM, running a Linux Ubuntu 18.04 LTS 64-bit with the Linux Kernel version 5.3.0-53.

5.2.1 Experiments and Results

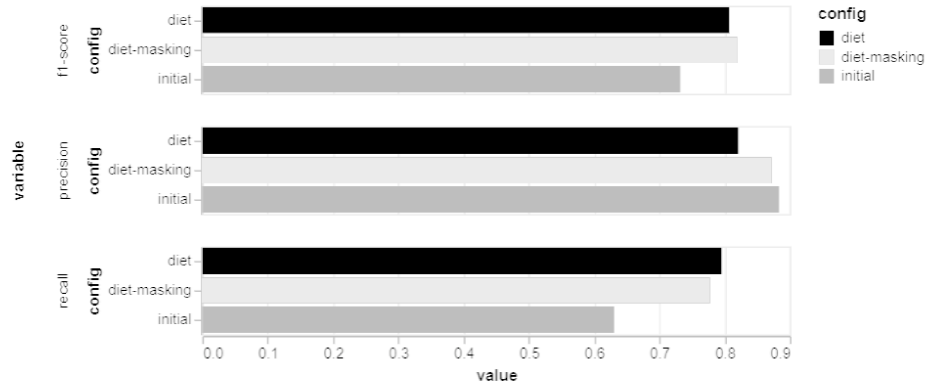
The current training of SecBot is done using a neural network implemented in Rasa to select the next action, which is described as a Long Short-Term Memory (LSTM) architecture defined in [236]. For the training of the neural network, it receives the user's phrase as input and actions as output. During the training phase, it is used as a fitting model with 958 samples (*i.e.*, examples of intents and entities) and a validating split of 0.1 (*i.e.*, 10% of the training dataset as validation data only), which covers 15 different conversation flows with 100% of accuracy for the intent and entities extraction. These preliminary results indicated that SecBot could map the conversation for the correct intent available, thus, also being able to extract entities. However, it is still important to check how it performs with additional flows that are not obvious or previously defined.

In terms of scalability, a stress test revealed that one single instance of SecBot can handle 20 messages per second. Among the currently supported custom actions, a more time-consuming request is the one to identify an attack, using symptoms in the attack tree, which have a higher computational complexity. In a simulation with an attack tree containing 100 symptoms and 30 attacks (*i.e.*, leaves), the time for the SecBot to process the request and return the correct attack is less than 2 s on average, considering 1,000 repetitions.

In a second step, in order to achieve higher accuracy and better performance for the SecBot, the training dataset was optimized with more data and details enriched. Also, specific configurations have been tested, such as changes in the training pipeline and policies directly in the Rasa training setup (*i.e.*, the config.yml file). These configurations were exhaustively investigated and described in [210].



(a) Intent Identification



(b) Entity Recognition

Figure 5.3: Precision, Recall, and F1-Score for the Three Different Configurations Tested in SecBot

Three different pipeline configurations were defined: *(i)* Initial, which uses SKlearnIntentClassifier for intent classification and the CRFEntityExtractor for entity recognition, *(ii)* the DIET, which uses a DIET classifier for both intent classification and entity recognition, and *(iii)* the DIET-Masking, which enables a hyperparameter named *use_masked_language_model* of the DIETClassifier and the number of epochs equal to 400. Each of these configurations was testing running all of the benchmarks available in the Rasa framework. The test was performed three times for each specified configuration to achieve the results for Precision, Recall, and F1-Score.

Figure 5.3 (a) shows the comparison between the different configurations tested for the Intent identification. The *initial* scenario shows the first configuration of SecBot without any refinement. It has the worst performance of the three scenarios, while the DIET performs slightly better than the DIET-Masking. By using the DIET pipeline's configuration, the SecBot increased its performance for both metrics being evaluated. For example, the F1-score for the DIET configuration is 72.96% compared to 66.02% of the initial configuration. A similar methodology was also applied to analyze the capacity of recognizing Entities. Figure 5.3 (b) summarizes the results. Again, the DIET shows to be the best option in the three configuration scenarios for the pipeline. The DIET achieves 88.33%, 82.17%, and 81.93% for the Precision, Recall, and F1-Score. This shows a quite significant improvement from the initial configurations of the SecBot.

The changes in both intent classification and entity recognition have given SecBot a massive performance boost. In addition, after these changes, SecBot works much better on the recall as well. Therefore, since the F1-score is an average of the recall and precision, SecBot's overall performance was improved despite having a slightly lower precision in entity extraction. This results also highlights the importance of calibrating this kind of solution, taking into account the optimal trade-off of each kind of configuration.

5.2.2 Discussion and Limitations

SecBot shows opportunities to simplify the different steps involved in cybersecurity management. The design of chatbots is still challenging, especially because the accuracy achieved by supervised learning methods is directly related to the quality of inputs used. For these scenarios and flows defined, the accuracy of answers provided was precise and useful to address users' demands. As observed in the prototype implemented, the current state provides directions and shows the benefits of addressing cybersecurity-related information using conversational agents. Custom actions, developed as contributions of this work, indicate the path for further implementations and highlight the proposed solution's extensibility.

Given that SecBot's prototype has been evaluated using selected information and scenarios, it is possible to learn new information to handle more requests and conversation flows. There are opportunities to improve the training phase by creating new *Stories* and considering different datasets available for cybersecurity, such as describing more attack characteristics and their relationships. By building a larger dataset of cybersecurity-related information, it is possible to define additional *Entities* to extract from a conversation, thus, resulting in different flows and scenarios covered. In the same way, new *Intents* and scenarios can be defined based on the amount of information that the SecBot can extract. Such *Intents* need to be defined considering the actual demands of businesses, thus resulting in different custom actions to be implemented to address specific requirements.

In terms of scalability, several instances of the SecBot can be provided quickly to address high demands for interactions. As one instance can handle 20 messages per second, it is reasonable to assume that a single instance of the SecBot can be used by many businesses simultaneously, such as processing more than 100 scenarios in one minute. Thus, despite relying on similar underlying data sources, each instance runs independently from the others in a modular fashion via replication. In terms of security, it is an option that each SME can run locally their instance of the chatbot, which increases the means to operate on dedicated resources in a controlled environment, also allowing a knowledge database customized according to the specific demands of that business. It also can scale to complex problems and solutions. However, it depends on how to define the correct training dataset and configurations to avoid an over-fitting of the ML model being used, *i.e.*, ensuring that the model will be able to extrapolate the knowledge of complex scenarios and not only perform with trained scenarios.

Although SecBot is motivated by identifying the benefits and challenges of chatbots for SMEs, large companies can also benefit. Professionals with prior knowledge in cybersecurity can explore this approach to meet different goals. Cybersecurity analysts can interact with SecBot to find a fast and accurate answer for a customer request regarding technical and economic aspects related to SMEs' cybersecurity. Also, mechanisms can be implemented to help large companies justify their investments in a specific solution or cybersecurity strategy, such as understanding requirements to define the directions of their bug bounties programs. This can help build foundations for long-term cybersecurity strategies rather than sporadic engagements of specialists. Another use comprises the opportunity offered to cybersecurity companies to develop their solutions integrated with the SecBot.

5.3 Data Processing for Threat Analysis using SecGrid

SecGrid implements miners that satisfy the requirements of the Data Processor component introduced by the proposed framework. In order to understand how it can scale and its potential, an analysis of the performance (in terms of time and resource consumption) of the implemented miners is required. Also, it is essential to understand the capacity of SecGrid to process the data to provide valuable insights for companies.

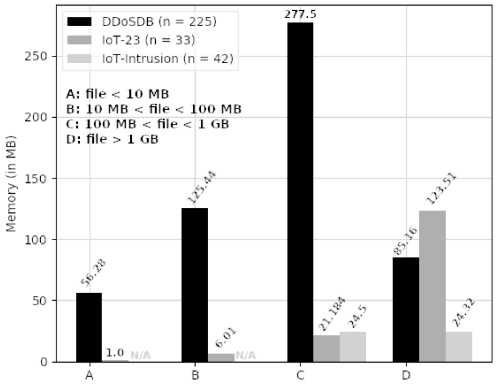
5.3.1 Experiments and Results

For the SecGrid solution, experiments were conducted to evaluate *(i)* the miners' performance and scalability to process information from different datasets composed of real-world cyberattacks, *(ii)* the accuracy of the ML-based attack classification, and *(iii)* SecGrid's overall usability.

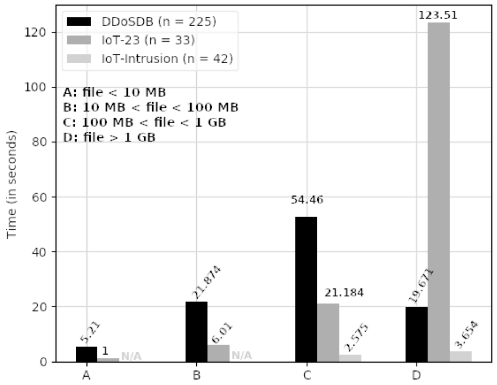
Miners' Performance and Scalability

In order to investigate the performance of the SecGrid's miners and the scalability of the platform, the time to extract the features from different PCAP files were measured, as well as the RAM and CPU used during the process of opening, extracting, and storing information from these files. The experiments were conducted with SecGrid instantiated in a container-based application limited to the usage of 2 GB of RAM running in an Intel Core i7-8650U, with a base frequency of 1.9 GHz, 16 GB of RAM with a clock speed of 2.133 GHz. All evaluation's scripts used are available at [153].

For the analysis, three different datasets of PCAP files are considered: *(i)* the DDoSDB [189], which provides data from collaborators that usually collected the data as a victim, *(ii)* the IoT-23 [3], a dataset of network traffic from IoT devices captured by the Stratosphere Laboratory of Czech Technical University in Prague during the years of 2018-2019, and *(iii)* the IoT Network Intrusion dataset [110], which contains various types of network attacks simulated in IoT environments for academic purposes. The process was conducted as follows. First, the dataset files were stored locally. Then, for each one of the dataset log file, the miners of the SecGrid were applied to extract information from them, and the time and memory used to process each file was recorded. Also, it was recorded if the datasets were successfully processed or not. Finally, the average time to process each dataset was calculated besides processing each file. This approach was applied in 10 different rounds to base the analysis on statistically accurate results. Thus, 300 PCAP files were tested in total, with a total size of 112 GB in datasets. The number of files in each dataset is identified as n in the experiments.



(a) Average Time to Analyze PCAP Files



(b) Average Memory Consumption to Analyze PCAP Files

Figure 5.4: Performance Evaluation of SecGrid for 300 PCAP Files

Figure 5.4 presents the overview of the experiments performed with the SecGrid's miners. The three datasets were separated into four different scenarios (*i.e.*, A, B, C, and D) based on their files' size for a better analysis of the results. Figure 5.4 (a) shows the time to process each one of the datasets. It is possible to see that the response time for smaller files (*i.e.*, those presented in the IoT-Intrusion dataset) seems to increase linearly. Still, when comparing other datasets (*e.g.*, DDoSDB), it is possible to observe that the time required to process files between 100 MB and 1 GB (Scenario C) is higher than to process the files higher than 1 GB (Scenario D). This happens because the response time is dependent on the size of the file and the entropy present on the file (*e.g.*, how much information, complexities of the packets, and characteristics have to be extracted). The dataset that showed large files with higher entropy was the IoT-23 [3]. The average time to analyze the files with more than 1 GB (Scenario D) in the dataset IoT-23 with high entropy was roughly 2 minutes. However, in this dataset, the worst scenario observable required roughly 25 minutes for a file, representing a Gafgyt Malware traffic, with 22.1 GB of size and very high entropy. It was not the larger file analyzed but the one that required more time to process.

The RAM is another critical resource for SecGrid scalability and stability. Therefore, its usage by miners was also measured during the experiments. Figure 5.4 (b) provides the average memory used to analyze each one of the PCAP files. All 300 PCAP files were successfully analyzed, with the highest recorded memory consumption being around 1 GB for a file of 50 GB of a real-world DDoS attack. On average, the highest consumption was 277.5 MB for the dataset of DDoSDB (Scenario C), representing a log file of a massive TCP Flood. Based on the tests performed, it is possible to ensure that SecGrid can process files up to 50 GB without any restriction. It was also measured that the In-

put/Output medium (*e.g.*, Hard Disk Drive or Solid-state Drive), from which the PCAP file is read, has to provide read speeds of at least 50 MB/s; otherwise, it might become a bottleneck for files with huge sizes and high entropy.

ML-based Classification Evaluation

For the evaluation of the performance and feasibility of the ML-based classification implemented inside of SecGrid, different algorithms and datasets were tested, resulting in high overall accuracy for both RF and KNN implemented algorithms. The final model has a total length of 55,349 records and contains 18 datasets, with most of them containing two to four attacks. The defined model had a size of 8.9 MB, which was only a fraction of the original datasets that were often gigabytes in size. A model is trained using data from different data sources that include various DDoS attack types. This also includes regular traffic so that the system does not accidentally classify regular network states as attacks. The model was cross-validated using an 80% train and 20% test split. This cross-validation was performed ten times with a randomized dataset to split. The reported results are in the form of Precision, Recall, F1-Score, and Accuracy. The evaluation procedure was run with two different setups: without duplicates in the dataset (*i.e.*, removing all repeated occurrences of a record in the model) and with duplicates kept.

The results of each evaluation setup are displayed as macro averages (*i.e.*, overall classification of all attacks without distinction of the records available in the model) and as weighted averages (calculates the metrics for high and low-occurrence of records for each attack type in the model separately). This helps to show that not balanced occurrences of records can result in a misrepresentation of attacks in the dataset, which is masked by the correct classification of other attacks. For example, in a model comprised of 95% of TCP flood records and 5% of UDP records, even if the algorithm performs very poorly for UDP flood classification, the total metrics would still result in a good classification supported by many TCP attacks correctly classified. The accuracy was calculated by rounding a floating-point value, while Precision, Recall, and the F1-Score were calculated by averaging percentage integers.

Table 5.3 summarizes the results of the experiments. The Precision, Recall, and F1-Score in all unweighted tests reached 100%, from which it is possible to infer that the system performs very well with attack types for which many records exist in the database. In this test, most records consisted of regular traffic, SYN Flood Attacks, ICMP Flood Attacks, and UDP Flood attacks. Even though not all attack states were classified correctly, the large ratio of attack types classified 100% correctly to falsely classified types averaged out to 100%. Comparing those values to their weighted counterparts, it becomes clear that the system had trouble classifying attacks that were not well represented

in the dataset, such as IP Sweeps and Port Sweeps. Therefore, the metrics could be closer to their unweighted counterparts if the dataset had more records of these underrepresented attack types.

Table 5.3: Evaluation of Random Forest (RF) and K-Nearest Neighbors (KNN) After Cross-Validating the Built Model

Method	Precision	Recall	F1-Score
RF with Duplicates	100%	100%	100%
RF with Duplicates (Weighted)	95.1%	92.3%	92.4%
RF without Duplicates	100%	100%	100%
RF without Duplicates (Weighted)	97.9%	95.9%	96.5%
KNN with Duplicates	100%	100%	100%
KNN with Duplicates (Weighted)	83.7%	81.2%	82.3%
KNN without Duplicates	100%	100%	100%
KNN without Duplicates (Weighted)	85.4%	83.5%	84.3%

All tests that had duplicate records removed performed better than their counterpart that kept the entire dataset. Duplicate records shrunk the model data to 43,714 records, which means a 21% reduction in length. The algorithm RF performed significantly better in the weighted result scores. The RF classifier manages to classify low-occurrence attack types better than the KNN classification. However, both algorithms performed equally well in classifying the well-represented attack types in the model.

Additionally, the time required to build the model with more than 50,000 records was 651 ms, with a classification time of 27 ms for the RF algorithm and 204 ms for the KNN algorithm. This shows that, based on the time required for the classification, real-time analysis is possible, and RF can be a possible candidate for a production environment. Comparing these values achieved by SecGrid's classification with other state-of-the-art approaches available in the literature, it is possible to verify the excellent results of SecGrid's approach, especially from the RF classifier.

Usability

An online survey was conducted to analyze the usability of SecGrid. This was based on eight tasks selected to be performed and followed by a System Usability Scale (SUS) questionnaire [35]. The survey was conducted anonymously with 23 participants from different countries and institutions (both industry and academia), with different levels of scholarship (Bachelors, Masters, and PhDs), and with expertise in Computer Science-related areas (Computer Networks, Information Systems, Software Engineering, and Cybersecurity). The participants' ages varied from 23 to 60 years, all know-

ing at least three or more types of cyberattacks. After filling in the initial information regarding their fields, scholarship, and previous knowledge, each participant was requested to watch a three-minute video introducing the main features of SecGrid. The participants were required to answer the questions as of Table 5.4 using SecGrid, resulting in respective success rates (*i.e.*, how many users answered correctly). Appendix D provides details of all tasks and questions that the participants of the study had to answer.

Table 5.4: Tasks Performed by Users using SecGrid

Task	Answer	Success Rate
T1: How many packets are present in the dataset?	1640892	95.7%
T2: How many hosts participated in the attack?	2678	91.3%
T3: From which part of the world were most packets sent?	Asia	91.3%
T4: Which destination port received the largest number of segments?	80	95.7%
T5: Was the traffic only sent to ports in the 'well-known port range' (1-1024)?	No	69.6%
T6: Which of the following attack vectors describes the attack in dataset "Dataset 1" best?	SYN Flooding	60.9%
T7: Regarding the HTTP traffic in the "Dataset 2", would you consider this traffic as being part of the attack?	No	78.3%
T8: Looking at the metrics, which of the following attack vectors describes the attack in "Dataset 2" best?	ICMP Flooding	69.6%

Most of the tasks achieve very high success rates. However, T5 and T7, even with binary answers (Yes/No), provided results slightly above 60%. This is because some of the participants did not use the visualizations provided to answer the questions but relied mainly upon the overview of statistics provided by the platform. This resulted in wrong answers, since a SYN Flooding (the correct answer for T5) can be easily confused with an HTTP flood (most of the wrong answers for T5) without a more in-depth check. The same happens for T7, in which some participants did not analyze the entire traffic but only the most used port (HTTP 80). Therefore, it is essential to organize visualizations and statistics to improve usability and avoid misinterpretation, thus guiding the users to the most accurate insight possible.

Besides these tasks conducted and according to the SUS questionnaire answers, most users found SecGrid easy to use (91.3% of the answers) and well-integrated (91.3%). Also, users were confident

in using the system (82.6%) and would like to use SecGrid frequently (78.3%). Although most participants' feedback was positive, suggestions to improve the usability were provided at the end of the survey. The most frequently suggested suggestion refers to the feature of freely creating and saving a dashboard using available visualizations and datasets. Thus, this feature was implemented additionally to improve the overall usability. However, other relevant features mentioned by participants can improve the users' capacity to gain insights using SecGrid, such as those related to the analysis of datasets based on time-series plots, more contextual information, and support for insights sharing.

5.3.2 Discussion and Limitations

The experiments conducted show clear evidence of the usability of the platform. A high percentage of success was achieved in the tasks performed by the users interviewed, including the capacity to understand the magnitude and type of an attack, its technical aspects, and its behaviors (*e.g.*, ports and traffic). Besides that, all of the users interviewed indicated a measurable level of interest in using SecGrid to analyze attacks, with 91.3% of them highlighting that the platform is easy to use and well-integrated. Performance tests were conducted with three different datasets (with a total size of 112 GB). They show measurable evidence of SecGrid's capacity to handle large datasets in a few seconds, which is a highly desirable feature to ensure the platform's scalability. Also, SecGrid's memory consumption is low considering other tools, allowing SecGrid to handle files up to 50 GB in commercial off-the-shelf hardware (*e.g.*, personal desktops and laptops).

Although SecGrid was initially designed for postmortem analysis of cyberattacks, real-time analysis is also possible by integrating real-time monitors with SecGrid. This depends especially on the complexity of the traffic (*e.g.*, entropy) and the time to process the information being provided. For example, in an additional work conducted on the top of SecGrid [177], the Netflow protocol was integrated into SecGrid to enable real-time support. This implementation was done by adding live miners that process information directly from Netflow monitors. However, the overhead introduced by the real-time analysis is still unclear, when using the solution in real-life settings.

On the ML side, the results obtained by SecGrid show exciting results for understanding cyberattack behaviors. This, when compared to the literature, achieves a high accuracy considering the F-1 score and the true positive rate. The results proved that high accuracy could be achieved even for the classification of multiple attack types. However, one of the challenges identified during the research is classifying attacks that cover a very short time window. As these short attacks only provided a limited number of time-frames, it is challenging to represent them in the model. Visualizing these short attacks can also be a challenge, especially when analyzing a data set recorded over a day or more. Even if correctly classified, the data points only appear as very points on the over-time classification and

might be ignored by a user or accepted as falsely classified records. The solution to this problem and visualizing day-long data sets, in general, could be solved by implementing clustering methods that either use the most-occurred attack type over time or by using anomaly detection that analyzes the time frames before and after each record.

The opportunities for the usage of SecGrid as an enabler for research, teaching, and protection activities are vast. Different works have proven it by relying on SecGrid's core to achieve their goals. For example, [215] developed an ML-based model for the detection of malicious DNS-over-HTTPS exploring the concept of miners introduced by SecGrid, [121] implemented a traffic sinkhole for the analysis of cyberattacks having the SecGrid as the underlying platform, and [54] proposed, on the top of SecGrid, a distributed analysis of cyberattacks in which multiple stakeholders can analyze interrelated network traffic in a collaborative setting. The SHINE solution (*cf.* Section 4.8.2) uses SecGrid as the basis to enable economic information-sharing regarding cyberattacks. An instance of SecGrid called DDoSGrid has been considered as a supplementary service for the initiative named DDoS Clearing House for Europe [40].

5.4 Calculation of Optimal Investments with SECAdvisor and GL

The evaluation of GL specifically is out of the scope, since it is already extensively evaluated in the literature, such as in [247], [163], [112], and [144]. Therefore, this section focuses on evaluating the capacity of the SECAdvisor tool to achieve the correct values of optimal investments by applying the GL model. Also, the feasibility of the solution is highlighted, and the ROSI calculation is described. A qualitative evaluation based on case studies is performed, thus showing the benefits of each investigated scenario. The first case study focuses on calculating the optimal investment of segments. The second case study is dedicated to cybersecurity solution recommendations, while the last one shows the calculation of the ROSI metric for supporting the decision between different recommended protections.

5.4.1 Experiments and Results

The case studies covered by this evaluation were initially introduced by the previous supervised work of [173]. The basis for the case studies is a hypothetical company named Montana AG. This company is based on real-world data of companies with similar characteristics. However, as some specific data are not publicly available, assumptions had to be made using public available reports [43, 184, 202] with cybersecurity and business statistics. A hypothetical company is considered here because real-

world companies are not fully open to providing all information needed for this kind of case study, since it might need companies' sensitive information.

The main business of Montana AG is, on one hand, to sell electronic devices, such as hardware, computers, and cameras. On the other hand, they distribute household and garden products. The headquarters of the company is located in Switzerland. Montana AG owns ten big retail stores spread all over the world. In addition, they also sell their products with the help of two online stores. One store offers the electronic assortment, while the other sells household and garden products. The company employs 2000 people, and its annual revenue is US$ 600 million. As can be seen, this company is not an SME but an MNE. These values were defined for demonstration purposes. However, the same approach fits also if it was the case of an SME.

The company's CEO is very concerned about the ever-increasing threat of cybersecurity attacks, so she asks an IT manager to analyze the current business segments and propose suitable cybersecurity solutions. The CEO emphasizes that the budget for cybersecurity investments is minimal and that the IT manager should choose the most efficient solution. He/she has also heard of a tool that calculates how much money should be invested in cybersecurity and presents suggestions for cybersecurity solutions, so he/she should use this one. After the CEO's prompting, the manager gets to work. First, he/she creates a business profile that depicts Montana AG. Due to the headquarters being located in Switzerland, the manager has decided to use *Europe* as the region.

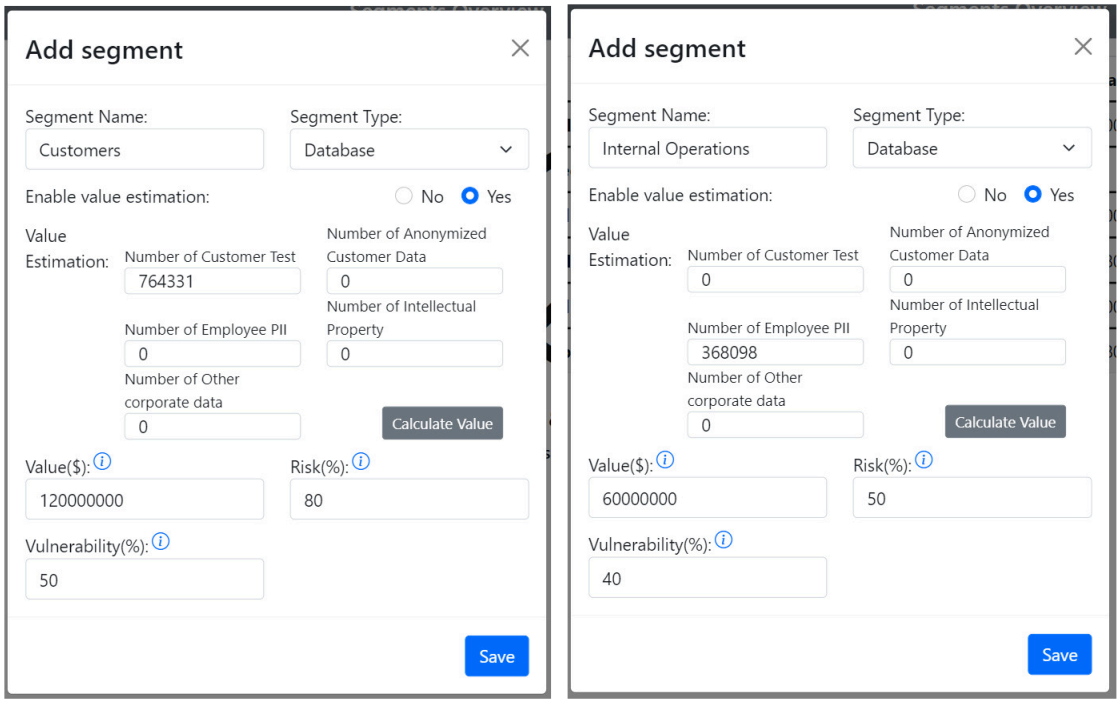
Case Study: Calculating the Optimal Investment

For this case study, suppose that an IT manager is focusing on investing in security for the databases of Montana AG. The company owns three databases and the manager's goal is to determine the optimal level of investment for each database.

The first database manages customer data such as credit card information and customers' data. Currently, 764,331 entries are stored in the customer database. The manager estimates that the probability of an attack is 80% and 50% that a cybersecurity attack will be successful. The second database contains information about internal operations. This database stores information about employees. This database has 368,098 entries. It is estimated that the probability of an attack is 50% and 40% that an attack will be successful. The last database manages records about external operations. This database contains information about business partners. This database contains 133,333 records, and the risk of a cybersecurity attack is 20%. The probability of a successful attack was estimated at 50%.

After analyzing the databases, the manager creates an information segment for each database using the SECAdvisor interface. To determine the value of the databases, he/she can use the feature provided by the solution for value estimation. The creation of the segment for the customer data is

shown in Figure 5.5 (a), while Figure 5.5 (b) shows the dialog for creating the segment for internal operations. The same process is used to define the segment for external operations.



(a) Customer Segment Creation **(b)** Internal Operations Segment Creation

Figure 5.5: Definition of Segments in SECAdvisor

After creating the segments, the IT manager is presented with the table shown in Figure 5.6. These segments created are displayed as columns. The first row represents the values of the segments, and in the *Total* column, the sum of the values is displayed. The final vulnerability of each segment is calculated by multiplying the risk and vulnerability previously defined by the manager. The third row makes statements about how high the expected loss would be if no investments were made in cybersecurity. From the row *Optimal Investment* the IT manager gets information on how much money he/she should invest in cybersecurity. It can be seen that the optimal investment level for the *Customer* database is US$ 2,400,000. The optimal investment for the *Internal Operations* database is US$ 788,528 and for the *External Operations* database the optimal investment is US$ 180,000.

Moreover, it can be seen from the table that the sum of all optimal investments is US$ 62,000,000. The last column of the table shows that the information segmentation saves almost US$ 73,000 of investment costs. The second row shows the expected loss with the optimal investment amount in-

vested. The last line gives the manager an overview of the total cybersecurity cost, composed of the sum of the optimal investment and the expected loss with optimal investment.

	Customers	Internal Operations	External Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	120'000'000	60'000'000	20'000'000	200'000'000	200'000'000	
Calculated Vulnerability	40%	20%	10%		31%	
Expected Loss Before Additional Investments	48'000'000	12'000'000	2'000'000	62'000'000	62'000'000	
Optimal Investment	2'280'000	788'528	180'000	3'248'528	3'321'363	72'835
Expected Loss with Optimal Investment	2'400'000	848'528	200'000	3'448'528	3'521'364	72'836
Total Cybersecurity Costs	4'680'000	1'637'056	380'000	6'697'056	6'842'727	145'671

Figure 5.6: Overview and Information Calculated by the SECAdvisor for the Database Segments Considered in this Case Study

In the last column, the manager gets an overview of the total costs that can be saved thanks to the information segmentation. He/she is surprised to see that the information segmentation results in a benefit of US$ 145,671. Thanks to this table, the IT manager has learned how much to invest in each segment and what advantages information segmentation offers. By comparing this information with the original work of the GL model [144], it is possible to verify the correctness of the calculation performed by SECAdvisor, since it obtains precisely the same values for the given scenario. In order to refine or adapt the calculations for specific scenarios, it is possible to determine different security breach probability functions, which can be easily changed directly on the SECAdvisor database.

After obtaining the overview of optimal investments and their economic benefits, the company can move to the next step of obtaining recommendations for protections that fits this budget. For that, the MENTOR engine (*cf.* Section 4.7) is integrated with the SECAdvisor to provide the recommendations for each segment based on cyberattack demands and the budget available. Suppose that the company now wants to invest up to US$ 120,000 in a *proactive* protection against a Ransomware attack. The protection has to be offered by a provider is from *Europe*. Also, the leasing period is long-term (*i.e.*, several months), and there is no urgency in terms of deployment time (*i.e.*, days). This scenario is shown in Figure 5.7. After filling the form on the top and submit, the MENTOR engine recommends two protections: one offered by Portwell and another by Sophos. The monthly price is shown in blue right after each protection.

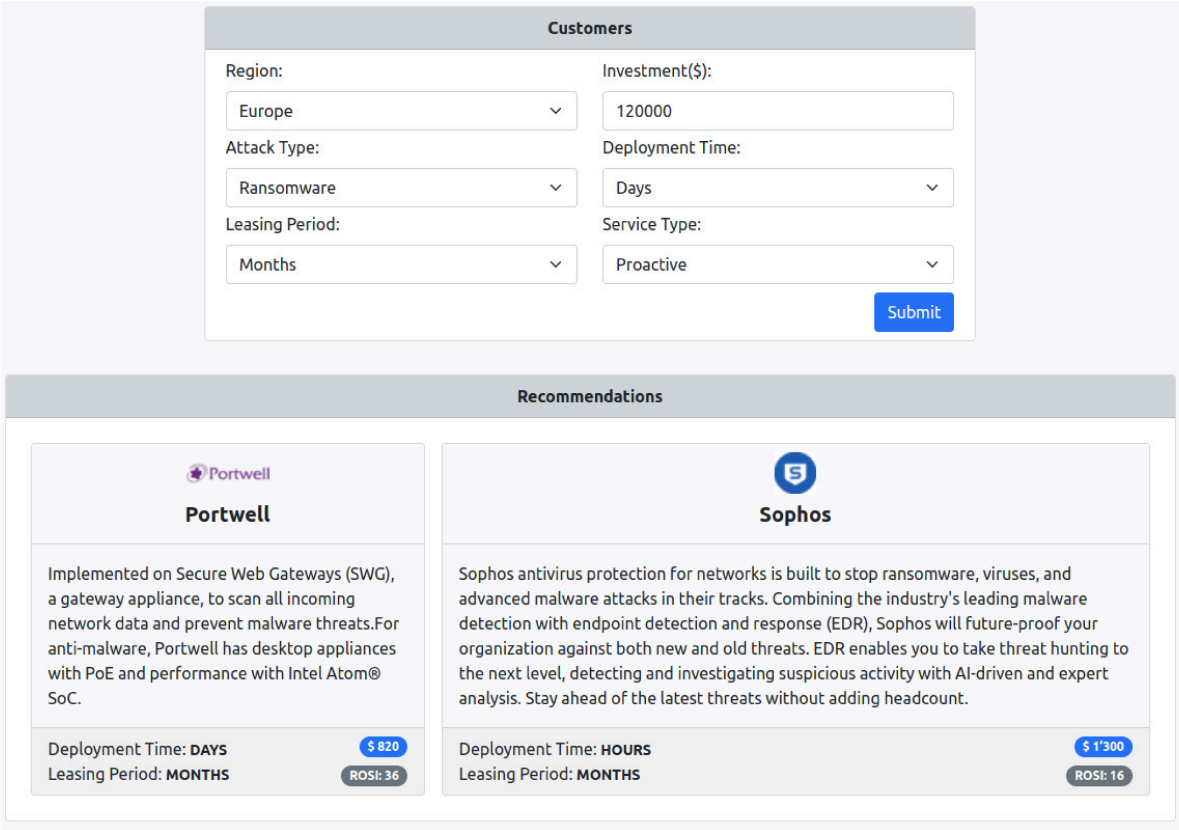


Figure 5.7: Recommendation of Protections against Ransomware and ROSI Calculation for Each of the Protections

Below the price, the ROSI automatically calculated by SECAdvisor is shown. In this case, it is possible to see that the cheaper one (*i.e.*, Portwell) also has the best cost-benefit in terms of the value and the mitigation rate offered. The parameters used to calculate ROSI and also the results for these two protections are summarized in Table 5.5. As can be seen, the calculated ROSI is equal to 36 and 16, respectively. It means that the Portwell protection provides a payback of 3600% ($36 \times 100\%$) while Sophos a payback of 1600% ($16 \times 100\%$). This result is obtained by applying the general equation of ROSI previously determined in Section 2.2.3. Therefore, the IT manager can use these recommendations to decide on the Portwell as a proactive solution against Ransomware. It is important to note that the human operator has an important role in deciding if the features offered by the protections satisfy the demands of the company, since *(i)* the ROSI relies only on mitigation rates and costs of the protection and *(ii)* the MENTOR focuses just on the attack type covered and not in the actual technical demands of the company.

Table 5.5: Parameters and Results of the ROSI Calculation for Each Protection Candidate

Parameter	Portwell	Sophos
Cost (Monthly)	US$ 820	US$ 1,300
Mitigation Ratio	80%	60%
ARO	3 times	3 times
SLE	150,000	150,000
Calculated ALE	450,000	450,000
Calculated ROSI	36	16

Annual Rate of Occurrence (ARO), Single Loss Exposure (SLE), Return On Security Investment (ROSI)

5.4.2 Discussion and Limitations

The SECAdvisor tool supports the application of cybersecurity economics models intuitively. For that, it relies on GL and ROSI as well as provides an integration with the MENTOR recommender system. The results of SECAdvisor are hard to measure quantitatively, since it requires an exhaustive evaluation of the GL model and not the tool itself. All of the equations and concepts proposed by the GL model over the years (especially the information segmentation [144]) are replicated with perfect accuracy in the solution proposed. This helps companies and people without know-how or expertise in cybersecurity economic models to have insights into how to perform investments in cybersecurity.

However, the tool still performs as a black box approach, since no feedback for the user is provided about how the calculations are being executed in the backend. This helps in the way to make the tool more adequate for non-experts (*i.e.*, without technical complexities) but also limits the tasks and scenarios in which the tool can be helpful. For example, it is important to allow users to change and interact with security probability functions (*i.e.*, the probability of a system with a certain vulnerability being breached) while also seeing the behaviors of the optimal investment. This can help users calibrate the GL model for their reality and have sufficient information to justify better their investment decision besides only the general scenarios provided by the original GL work.

The evaluation still considers only a hypothetical scenario defined using information collected from public reports and open discussions. However, this still cares for more accurate analysis to understand at which extension the decisions provided by GL, and consequently by SECAdvisor, can be effective for companies from different sectors. Therefore, although the initial investigations are positive, the feasibility of applying the GL model, as implemented by SECAdvisor, in real-world scenarios still requires more investigation, including the definition and execution of experiments that provide quantitative results.

Finally, regarding the value estimation provided by the tool, it is supported by information and reports publicly available. Additional segments can be mapped and added according to the demands of a company. However, it is also limited by the amount of information available about cybersecurity (*e.g.*, trends and financial losses due to cyberattacks). This goes directly to the direction that a culture of collaboration has to be introduced and adopted in the following years, including information sharing and threat modeling approaches [21, 238].

5.5 Recommendation of Protections using MENTOR

The recommendation engine provided by MENTOR was evaluated regarding its capacity to recommend adequate protections based on the demands defined by a company. A dataset was generated for the evaluation, since there are thousands of protections available on the market and most of them does not provide public information about their costs. The dataset contains 10,000 randomly generated protection services, with each service described based on parameters available for the customer profile (*cf.* Table 4.8) and with a price range between US$ 100 and US$ 1,000. Thus, by using such data as an input to the MENTOR, the performance and accuracy of the measurement algorithms to recommend protection services can be analyzed.

5.5.1 Experiments and Results

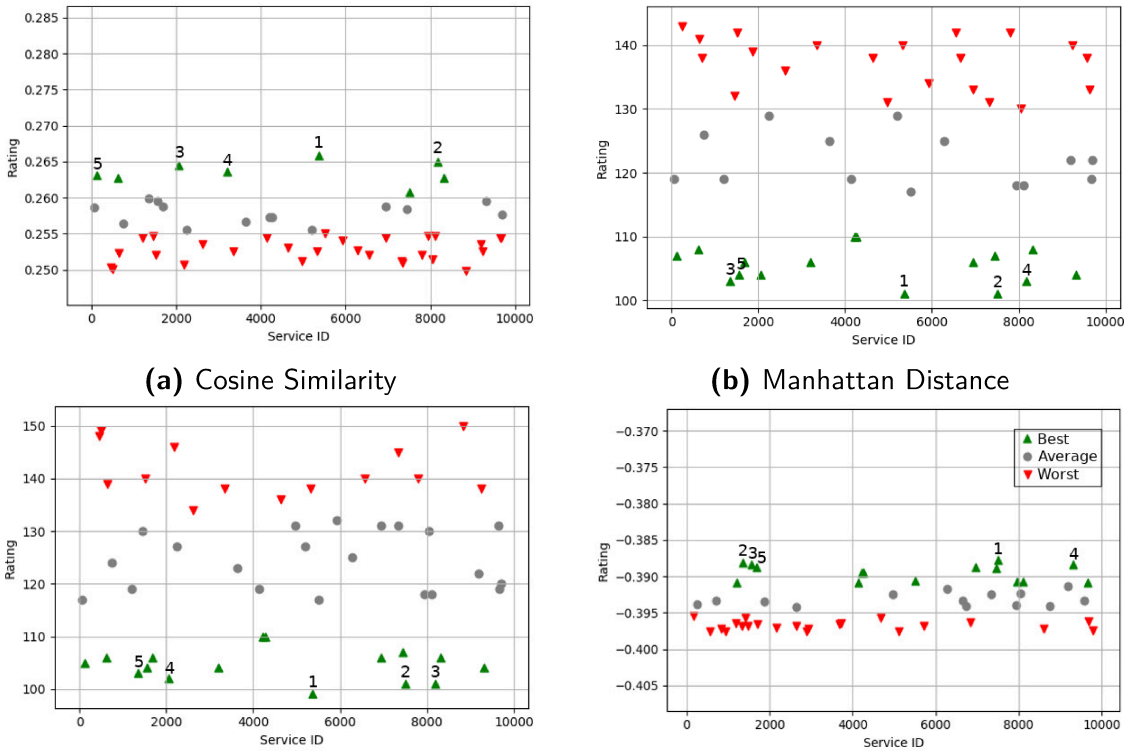
The four similarity measurements described beforehand (*i.e.*, Section 4.7) were used to conduct this experiment. These requirements are indexed and translated into the vector composed of region, service type, deployment time, leasing period, and price, which is given as input to the recommendation engine. The customer profile (*i.e.*, input) was defined to represent a request for a reactive service against a DDoS attack, running in Europe with a deployment time in minutes, a leasing period in days, and the maximum budget to be up at US$ 200. Therefore, the customer profile is represented as follows:

- Budget: US$ 200
- Type: Reactive
- Region: Europe
- Deployment Time: Minute
- Leasing Period: Days

After the dataset's creation and the customer profile defined, the recommendation engine uses both as input and applies a filter to discard unrelated services (*e.g.*, outside the price range, region, or

deployment time). The similarity is calculated based on the given vector (*i.e.*, customer profile) using each algorithm available on the current MENTOR version.

Figure 5.8 depicts the top fifty ranked services for each similarity algorithm, in which the best five are detailed in Table 5.6. However, these recommended services were similar concerning the properties being compared, with significant differences in how these algorithms work depending on how the input vector is mapped. For example, all protection service features are described as a vector in space, in which specific properties can significantly change their direction and, consequently, their rating. Therefore, high-magnitude variables (*e.g.*, price, deployment time, and leasing period) cause a significant influence on the vector's direction in space and, thus, changing the rating of its recommendation. For instance, a "worse" rating can be given to services that may be better than those specified in the customer profile. A service with a slightly higher price and a significantly lower deployment period may have a worse ranking due to the disparity, in absolute terms, between the properties of the protection service.



(a) Cosine Similarity **(b)** Manhattan Distance

(c) Euclidean Distance **(d)** Pearson Correlation

Figure 5.8: Ratings of the Fifty Best-Ranked Protections According to Each Algorithm

Table 5.6: Summary of the Five Best-Ranked Protections According to Ratings Calculated as of Fig. 5.8

(a) Cosine Similarity

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	0.26585	100	Hours	Days
2	8182	0.26493	102	Seconds	Days
3	2062	0.26448	103	Seconds	Days
4	3202	0.26361	105	Hours	Days
5	122	0.26318	106	Seconds	Days

(b) Manhattan Distance

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	101	100	Hours	Days
2	7512	101	102	Seconds	Days
3	1352	103	104	Seconds	Days
4	8182	103	102	Hours	Days
5	1552	104	105	Seconds	Days

(c) Euclidean Distance

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	99.0202	100	Hours	Days
2	7512	101	102	Seconds	Days
3	8182	101.02	102	Hours	Days
4	2062	102.02	103	Hours	Days
5	1352	103	104	Seconds	Days

(d) Pearson Correlation

Rank	ID	Rating	Price	Deployment	Leasing
1	7512	-0.38774	102	Seconds	Days
2	1352	-0.38814	104	Seconds	Days
3	1552	-0.38834	105	Seconds	Days
4	9312	-0.38834	105	Seconds	Days
5	1692	-0.38872	107	Seconds	Days

This is observed in the distance-based algorithms (*i.e.*, Cosine, Euclidean, and Manhattan presented in Table 5.6), in which the price was the most significant factor for the ranking of a service. Figure 5.9 summarizes the decisions of each algorithm in contrast to the costumer profile provided. For example, as can be observed, the service with ID 5362 was the service most similar to the vector specified by the customer profile (according to the distance-based algorithms). However, it was not necessarily the best service. In this sense, services with a shorter deployment time (in the order

of seconds) and without a significant price difference obtained a worse ranking due to the price difference. This happened for services ID 8182 and 7512 in the tables of the Cosine, Manhattan, and Euclidean algorithms.

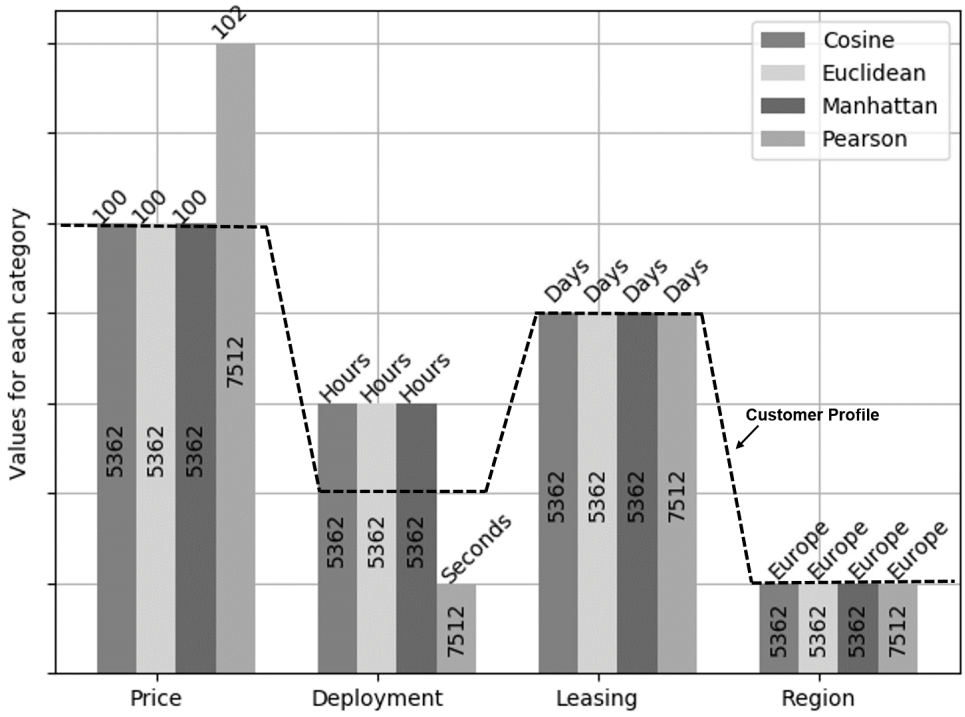


Figure 5.9: Best Ranked Solutions per Algorithm in Contrast to the Customer Profile Represented by the Dotted Line

However, the significant difference between the Pearson correlation and the distance-based algorithms is that it is invariant to the magnitude of elements. Hence, differences in service prices do not cause a major impact on their ratings because it mainly observes whether properties of protection services and the customer profile vary similarly. Thus, the service "ID 7512" is recommended as the best service because they consider an insignificant increase in the price compared to a significantly shorter deployment time. Therefore, considering the mapping of these characteristics of a protection service as a vector in space, the Pearson Correlation algorithm is presented as a better alternative in contrast to other distance-based similarity algorithms.

A possible alternative to circumvent these differences is given by grouping each attribute's vector of protection services. Thus, it is possible to compare these service attributes with customer profile attributes in a 1-to-1 manner. Therefore, the final rating of service is achieved by calculating an average

of the rating of its attributes. However, it should be noted that attributes of protection services offering better conditions than those specified in the customer profile would receive worse ratings. Thus, an alternative can be a rearrangement of input attributes to the best possible conditions, making the recommendation algorithms offer the best alternative instead of the closer to the end-user request. For example, if one wants a protection service with deployment time in minutes, protection services are a bit more expensive, but deployment time in seconds can be the most suitable recommendation, since this still fits the budget and other requirements.

Lastly, such an evaluation indicates that MENTOR can recommend adequate protection services considering the price, geolocalization, and other requirements defined by end-users. The distance-based algorithms recommend the cheapest service that is adequate for the end-user according to their demands. However, this service recommended is not necessarily the best one in terms of performance. The Pearson correlation decided toward a more expensive service fitting the end-users budget while delivering the best performance possible.

5.5.2 Discussion and Limitations

Beyond the evaluation concerning the recommendation process provided above, other technical aspects and open challenges are important to be discussed to improve MENTOR and shed light on further directions for cybersecurity research on the recommendation of protection services.

Although many protection services are available in the market, this number will arise together with a global deployment of novel paradigms, such as NFV and SDN. Also, novel business models can be used as an incentive to develop innovative cybersecurity solutions. Based on that, a recommendation system should understand the nuances of services running on different technologies to recommend a service efficiently. Besides, mechanisms to deploy the service directly on the customer's infrastructure or in a third-party host should be available, thus, simplifying the acquisition of such protection services by non-expert end-users.

The MENTOR evaluation used 10,000 possible protection services randomly generated. Such services contain general information (*e.g.*, price, deployment time, and leasing period) to demonstrate the feasibility of the solution. However, those services do neither represent the actual amount of protection services available nor contain exhaustive information on protection services. Most studies should be conducted to create a data model (*e.g.*, descriptor) able to define different services and demands, which may include the categorization by technology supported, features provided, and performance aspects.

Also, the reputation of the SP and protection services themselves can be considered during the recommendation process. One should be able to verify the feedback provided by other customers

as well as verify performance logs and issues related to past experiences. Besides, mechanisms to apply penalties to SP that do not meet the agreement demands should be considered. In such a direction, decentralized reputation mechanisms (*e.g.*, a BC-based one as proposed in Section 4.8.3) can be developed to provide a trustworthy and immutable record of reputation regarding the protection services and its different vendors.

Another critical aspect of the recommender system is related to the trust of customers to share data. This discussion is critical, and it is still an open challenge, not only for the MENTOR but for other work related to cybersecurity that demands actual data to achieve an accurate output. Currently, as a proof-of-concept, it is assumed a consortium of companies and institutions that trust each other. Thus, one trusted node receives data from customers and offers the MENTOR recommendation. Besides, the MENTOR is designed to run locally as well, which means that a customer can run his/her own instance of MENTOR in private infrastructure, thus, ensuring that the data will not be shared with third-parties.

Lastly, the process of recommending protection services assumes that end-users can provide data and the correct parameters to find adequate protection. However, users may not know the kind of attack they are under in some cases. Therefore, reactive service matching based on user input would be impractical. In addition, it is a challenge to integrate a recommender system with a variety of logs because, for example, there is no single standard of logs concerning the different types of services and technologies. There is still a lack of mechanisms to deal with the deployment and management of different technologies in an integrated solution, such as APIs and wrappers that help automate the deployment of recommended services without additional user interactions.

5.6 Economic Analysis of BC-based Solutions

A set of solutions backed by Blockchain (BC) have been developed as supplementary solutions to *CyberTEA* approach. These solutions have been motivated by *(i)* the need for decentralized approaches that increase the trust and automate specific cybersecurity processes and *(ii)* the hype of BC as paradigm-shifting technology [205]. Therefore, besides the clear benefits of BCs to these solutions, there is also an exploratory aspect involved, since the application scenarios for BC are vast and still yet not a consensus between experts in different areas.

Based on that, evaluations were conducted to verify the additional costs (in terms of money) that BC-based solutions have. The feasibility of BC-based solutions have to be investigated also in scenarios where the costs to operate solutions are critical. Therefore, the remainder of this section focuses on investigating and discussing the costs of operating and interacting with the *(i)* SaCI, a BC-based

cyber insurance model, *(ii)* Kirti, a BC-based marketplace for cybersecurity, and *(iii)* BRAIN, a BC-based reverse auction for infrastructure as a service.

5.6.1 Experiments and Results

Gas defines the internal pricing to run a transaction or a contract in the Ethereum BC. Gas does provide a measure for the computational usage in terms of monetary costs (*e.g.*, Gas per Swiss Franc or United Stated Dollars (US$). These Gas costs in Ethereum were estimated using the function *estimateGas* provided by the Web3 library. Gas costs were converted into Wei (smallest denomination of Ether) and Giga-Wei (GWei). 1 GWei (*i.e.*, 1 billion of Wei) is equal to 0.000000001 ETH.

Thus, evaluations are conducted to analyze the costs of deploying and operating an application that runs on top of SC. For that, the Gas required to act has to be calculated, then calculating how much it is in US$. It is possible to use a Gas cost of 20 GWei per unit of Gas, which is the default value of the Ganache platform (the most well-known for local tests). However, for this experiment, the amount of Ethereum's main net is considered, which is 35 GWei per unit of Gas as of May 7th, 2022. The Ether (ETH) value was converted into US$ using an exchange rate of US$ 2,548.28 per Ether, which was the valid exchange rate that day.

Table 5.7 summarizes all costs for calling functions available in the SC of SaCI, the BC-based Cyber Insurance model described in Section 4.8.1. This includes the costs of the deployment and interaction with the contract. As can be seen, The most expensive function is the one that deploys the contract (*i.e.*, Constructor), followed by the *reportDamage* function.

Table 5.7: Cost Estimations of SaCI's Functions

Function	Number of Calls	Estimation in Ether (35 GWei/Gas)	Converted in US$ (US$ 2549.94/Ether)
Constructor	1	0.10893	278.69
paySecurity	from 1 to ∞	0.00080	2.05
payPremium	from 1 to ∞	0.00084	2.15
reportDamage	from 0 to ∞	0.00435	11.13
acceptDamage	from 0 to ∞	0.00109	2.79
declineDamage	from 0 to ∞	0.00174	4.45
acceptCounterOffer	from 0 to ∞	0.00082	2.10
proposeToUpdateContract	from 0 to ∞	0.00264	6.75
agreeToUpdateContract	from 0 to ∞	0.00098	2.51

These functions represents high values, since it is paid only if the respective function is called. Therefore, almost US$ 300 has to be paid for the contract deployment, and US$ 11.13 must be paid if a coverage request is made. Note that all of these values already represent the worst-case (*i.e.*, most expensive), in which the blocks are mined as fast as possible. Taking a Gas cost of 2 GWei, which is considered a price that usually persists a transaction in a block within the next minutes in the Ethereum network [192], the final cost to deploy a contract can be divided by eighteen, thus, resulting in a cost around US$ 15. Also, the approach proposed by SaCI can be implemented using any permissioned or permissionless BCs that support SCs implementation [205]. The decision might depend upon the insurer's performance, privacy, and scalability demands.

There are also costs related to the Kirti solution, the BC-based marketplace, and the SLA monitor introduced in Section 4.8.3. Two SCs are part of Kirti: *Kirti.sol* have to be deployed only once, while a new instance of *SLA.sol* has to be deployed for each purchased service. The deployment of *Kirti.sol* is associated with a cost of 3,383.264 Gas (around US$ 300, while the deployment of the *SLA.sol* amounts to a cost of around US$ 213.54 (2,397.165 of gas). The Gas costs of the publicly callable functions of *SLA.sol* are further displayed in Table 5.8. It should be pointed out that both SCs were optimized in terms of deployment cost-efficient. As such, SCs providing similar functionality could be significantly more cost-efficient. The source code of both SCs is available at [1].

Table 5.8: Publicly Functions of *SLA.sol* Sorted by Gas Cost

Function	Number of Calls	Gas Cost	Converted in US$ (US$ 2549.94/Ether)
`init`	1	473717	42.20
`initOraclizeCallback`	1	123659	11.02
`reportViolationFromAPI`	from 0 to ∞	116283	10.36
`payForService`	1	86852	7.74
`getState`	from 1 to ∞	29599	Not payable
`getValidityPeriod`	from 1 to ∞	25815	Not payable
`updateCompensation`	from 1 to ∞	24471	2.18
`getViolations`	from 1 to ∞	23693	Not payable
`terminate`	1	16352	1.46

Note that three different functions only are implemented to return information available in the SC. Therefore, as these functions just work as a GET function, they have no monetary costs (*i.e.*, Not payable). These functions include the *getState()*, *getValidityPeriod()*, and *getViolations()*. The other functions that store new information or change the contract then have a monetary cost.

The last BC-based solution introduced here is BRAIN. Despite the benefits introduced by BRAIN as a BC-based reverse auction for IaaS (*cf.* Section 4.8.4), drawbacks have to be considered for deploying such a solution. The drawbacks are mainly regarding additional fees and time, similar to the case of SaCI and Kirti. The fees should be considered to deploy the auction on a large scale. An analysis of the current state of the Ethereum blockchain was conducted to investigate costs. For this, the Gas used was calculated by each auction call and analyzed regarding the Gas price and average time.

The deployment of the SC requires an average of two minutes to be mined by the blockchain, and the cost is US$ 30.25, which must be paid by the *Auctioneer* during the opening and call phase. The time can be decreased to a few seconds, but the fee for deploying it in the blockchain is US$ 66.49. On the InPs side, there is a cost of US$ 4.39 to submit a bid. Each bidder should pay this value to participate in the auction and guarantee that the bid will be processed in at most 40 seconds. There is no additional cost and time to handle the requests for resources and priorities information, as they are GET functions.

Based on the time that a transaction requires to be processed (*i.e.*, mined) in the blockchain, the auction time is more than 2 minutes. Thus, the marketplace should consider such additional time to avoid a negative impact on the quality of the end user's experience or during the protection deployment phases. BRAIN can be used to supply a large variety of services. However, since the blockchain cannot achieve real-time transactions, there are specific scenarios (*e.g.*, hosting VNFs to mitigate imminent cyberattacks and moving target defense scenarios) where other approaches should be considered to reduce the deployment time. Solutions could reduce costs (*e.g.*, Gas usage optimization) and the time required for the auction. Moreover, according to the evolution of blockchains and the next-generation blockchains, new opportunities can be expected to deal with such issues [205].

5.6.2 Discussion and Limitations

The BC-based solutions evaluated above and their functions are for proof-of-concept only. Therefore, they are not yet optimized in terms of Gas costs nor considering all security issues required for real-world deployment. The costs can be reduced for production deployment by *(a)* using different implementations of BC, which support SCs, and also *(b)* by optimizing the overall process, such as by refining the code or by increasing the time to process transactions to reduce the amount of Gas that have to be spent. Furthermore, as many BC projects promise efficient features, they can enable the cheapest and most efficient way to implement solutions like those that rely on SCs. Hence, these solutions can be implemented using any permissioned or permissionless BCs that support SCs implementation, such as Ethereum, Cardano, Polkadot, and Hyperledger Fabric [205].

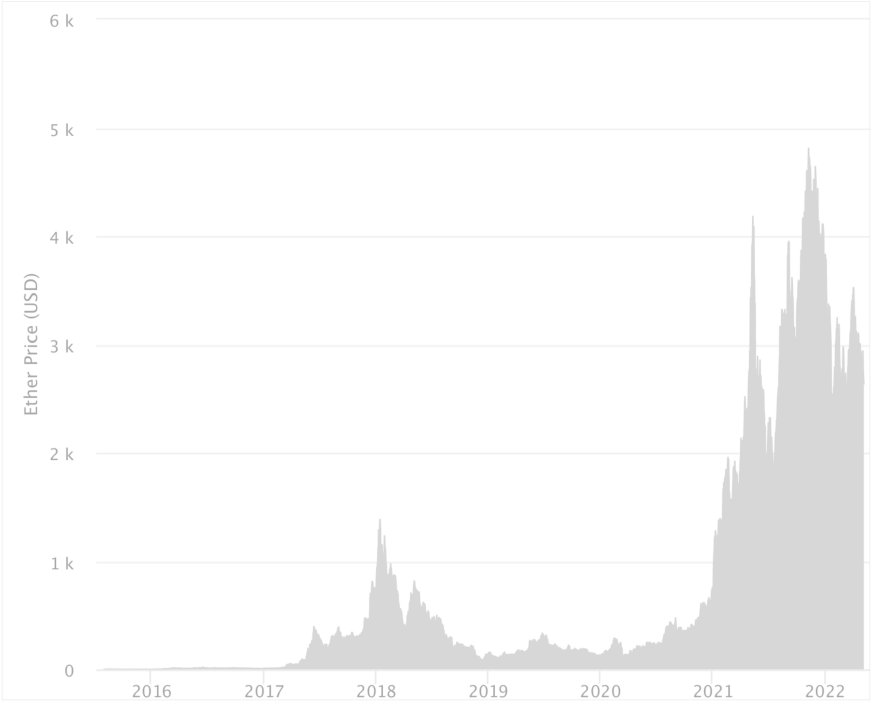


Figure 5.10: ETH Price from 2016 to 2022 [57]

As mentioned, the choice of the BC technology to be used impacts directly the costs. Ethereum was used in all solutions for convenience due to its support of SC, extensive documentation, and frameworks for development. During the evaluations, the specification of equivalent fiat currency values for the Gas price has been provided. However, extreme fluctuations in Gas prices and ETH (as most of the current cryptocurrencies) have to be considered. For example, as of March 15th, 2020, ETH was priced at US$ 123.53, and the average Gas price was around 17 GWei. On March 15th, 2022, ETH was valued at US$ 2,619.61, while the average Gas price was 40.48 GWei per Gas unit. Thus, executing any operation on the Ethereum network, such as a contract deployment, has become more expensive by a factor of over 2.5 over the period of fewer than two years. It was not even the peak, since situations in which the average Gas prices were much higher can be identified.

Figure 5.10 shows the ETH price over the year from 2016 until mid of 2022. As can be seen, the fluctuation is very high and can directly impact the costs, since all operations in the Ethereum blockchain are calculated based on the ETH price, too. Also, Figure 5.11 shows the variation in the Gas price from 2019 to 2022. The Gas price is a bit more stable than the ETH price but still has spikes that directly impact the costs of operating BC-based solutions.

Figure 5.11: Gas Price from 2019 to 2022 [249]

Thus, although BC-based solutions and the advent of the Web3 concept [164, 242] paved a path for several opportunities in terms of new solutions and business models, different aspects have to be carefully considered during their design and implementation. For example, not only technical feasibility of a solution is required (*e.g.*, in terms of features and security), but it also checks the feasibility in terms of cost to deploy and operate such a solution. This can be achieved, for example, by *(i)* selection of BC platforms with lower fees [206], *(ii)* usage of technologies to support cost-intensive operations, such as IPFS for data storage, and *(iii)* code refactoring together with good practices for developing decentralized applications [183].

5.7 Case Study: Definition of a Strategy using the CyberTEA Approach

In Switzerland, micro-enterprises (from 1 to 9 employees) comprise 89.73% of all companies. In comparison, small enterprises (from 10 to 49 employees) comprises 8.44% of the companies, and medium-sized (from 50 to 249 employees) comprises 1.55% of the market. These numbers are provided by a national study conducted in 2019 by the Swiss Federal Office for Statistics [184]. More than 75 of these companies are in the tertiary sector, composed of retail, wholesale, restaurants, and telecommunications services. The average net revenue of SMEs in Switzerland was CHF 29 million, and an average of 25 employees [94]. Considering these market facts, a hypothetical company was defined for this case study. This company is considered hypothetical but supported by information and scenarios from the real Swiss SMEs.

This hypothetical company is the PARME Pharma AG, a small-sized pharmaceutical company with 27 employees based in Basel, Switzerland. The main business of this company comprises the development and testing of new pharmaceuticals, chemicals, and cosmetics. The company works in a Business-to-Business (B2B) business model, thus, selling input production directly to other com-

panies to develop their products and medicines for drug stores. Table 5.9 summarizes the numbers and business of the PARME.

Table 5.9: Overview of Information of the PARME AG being Considered for the Case Study

Information	Value	Description
Sector	Pharmaceutical Industry	The company sector is an important information to be considered, since it gives indication about possible cyberattacks that might target specific sectors
Employees	25-30 people	The number of employees describes partially the size of the company, thus, helping to decide for strategies that fits SMEs or MNEs
Revenue	US$ 15 million yearly	The revenue and others financial metrics are important to understand the value of the business, its assets, potential budget for investments, and also its market value
Country	Switzerland	The country where the company is placed helps to understand the cybersecurity scenario and which regulations have to be followed when implementing cybersecurity strategies (*e.g.*, GDPR and the Cybersecurity Act for Europe)
Portfolio	Development and distribution of pharmaceuticals	This information gives an overview of the products and possible impacts of cyberattacks in the company. It is important to consider during the risk management tasks

PARME AG wants to evolve its business by having an E-Commerce business in which they can have contact directly with potential customers. This E-Commerce will be focused on both B2B and Business-to-Consumer (B2C), in which the customers can buy products directly from PARME AG and their partners. The company's prediction is to increase the company's revenue by US$ 5 million in the first year of E-Commerce operation, thus, having a total revenue of US$ 20 million. Therefore, with this new business that the company will run, it is required to adequate the current cybersecurity strategy and consider the new E-Commerce platform now operating under its umbrella.

This case study then focuses on mapping the company's stakeholders, threats, and cost-efficient strategies to plan the safe operation of the new E-Commerce system of PARME AG, which can result

in more competitiveness in the market and introduce new challenges due to potential financial losses due to cyberattacks. For that, the *CyberTEA* methodology will be applied, supported by different solutions developed here to achieve a cost-efficient strategy that fits the requirements of the company.

All information required for this case study was obtained from four different sources: *(i)* public information from the Swiss market, *(ii)* reports available regarding cybersecurity trends and threats for specific sectors, *(iii)* interviews and discussions with cybersecurity experts and SMEs employees, and *(iv)* arbitrary information based on a literature review to fulfill gaps of information that are not possible to be obtained from the others sources.

5.7.1 Phase A: Briefing and Business Demands

The methodology starts in Phase A, where all information related to the business has to be collected and a briefing conducted among the company decision-makers. For that, the information mapped in Table 5.9 is initially considered. This information is based on example of companies in Switzerland from the same sector and also the reality of the Swiss market [94, 184]. This gives initial insights into the sectors and size of the company. Next, the personnel expertise of the company is analyzed as an indicator to understand possible challenges or technical weaknesses to be considered during the planning of a cybersecurity strategy.

In the case of PARME AG, the employees allocated and contracted to work in the E-Commerce department have low awareness of cybersecurity. However, they have basic skills to operate computers, since they perform different daily activities, such as navigating the Internet, processing sales requests, and using office suites. Most employees have a bachelor's degree in a non-related technology field. Therefore, based on that information, it is possible to assume that the employees have a high level of education but without too much information technology background. This lack of background can be explored as an attack vector in the future. Therefore, this has to be considered for the planning of cybersecurity strategies.

Understanding the maturity level of the business and its processes is also important during this initial phase, since it can highlight possible weaknesses/strengths to adapt to new processes introduced by a cybersecurity strategy. In the case of PARME AG, it is a company operating for over 15 years, with processes well-defined defined in the pharmaceutical sector. However, information technology is still being validated, since the company's E-Commerce platform is very recent. Therefore, there is still a path to follow to integrate and control all current and new processes, which is still a more significant challenge without contracting dedicated technical people to handle that.

Finally, the history of past attacks on the company has to be considered. This is an important metric, since it can have a key role in adopting the cybersecurity strategy combined with other statistics

and security trends. However, this information is very sensible and confidential for companies to avoid malicious attackers from exploiting it. Therefore, based on a literature review and the most common attacks on the company's sector, the following information has been considered valid for the last three years:

- The PARME AG had a yearly average of five phishing attacks, and three Malware attacks;
- The success rate was respectively 15% (Phishing) and 10% (Malware), which means a percentage of these attacks impacted somehow the company in an economical and technical way;
- Although this information shows possible attack vectors, no critical impacts on the operation of the business were identified in the past.

This information can trigger alerts for the rest of the planning steps. While the company did not face any critical impact in the past, there are high success rates for these attacks. Also, the number of attacks might increase, including additional attacks (*e.g.*, DDoS and Ransomware), as the company becomes more digitally exposed to E-Commerce businesses. For example, a phishing attack can be used to infect the entire company infrastructure with a Ransomware attack and cause business disruption, leak of customers' data, and financial loss due to data recovery. Also, DDoS attacks can target E-Commerce directly to put the system down and impact the revenue and reputation of the company directly. Thus, it is important to have this past attack history in mind and map possible risks and threats during the next phase.

5.7.2 Phase B: Risk Management

For the risk analysis, three company's assets are to be taken into consideration: *(i)* the E-Commerce Web Server, which is responsible for maintaining the platform running, *(ii)* the E-Commerce platform, which provides all features for the user to interact and buy products from PARME AG, as well as allow the PARME AG employees to manage the logistics and the financial processes, and *(iii)* the databases that store information about customers, payments, and products. Also, the stakeholders have to be mapped.

The stakeholder is any individual or group that cyberattacks the platform can influence. Therefore, for this case study, the stakeholders are the *(i)* PARME AG decision-makers, *(ii)* customers, *(iii)* companies part of the PARME AG supply-chain, and *(iv)* the infrastructure manager of PARME AG. The threat sources are defined as of in [117]. Therefore, employees may cause intentional and unintentional damage, amateur and skilled hackers can exploit vulnerabilities for financial advantage or sabotage, and competitors might hire someone to damage the company's reputation.

The threat modeling is then conducted, taking this information into account. Also, the OWASP vulnerabilities [175] and trends for the sector are considered during this step. Table 5.10 summarizes the main threats identified, including their likelihood of happening, possible economic impacts on the company, and also which dimension of the STRIDE framework [246] the threat is classified.

A total of six Threats (T) were identified, named from T1 to T6. The selection of these threats is based on the risk assessment previously conducted on the company and the trend of specific cyberattacks in the company's sector. Also, four major economic impacts were considered: Loss in Revenue (LR) due to business interruption, Costs for Mitigation (CM) before or during an attack, Reputation Harm (RH) due to a successful attack, and Legal Costs (LC) associated to third-party impacts and data breaches. Note that the LR and CM are examples of direct impacts of a cyberattack, while the RH and LC can be classified as indirect impacts.

Table 5.10: Overview of Threats that Might Face the Company and Possible Countermeasures for Risk Mitigation

Threat	Likelihood	Economic Impacts	STRIDE Classification
T1: Denial-of-Service Attack	Likely	LR, CM, and RH	Denial-of-Service
T2: Phishing Campaign	Likely	CM	Spoofing, Information Disclosure
T3: Ransomware	Moderate	LR, CM, RH	Denial-of-Service, Information Disclosure
T4: Insiders and Supply-Chain Attacks	Moderate	LR, CM, RH	Repudiation, Information Disclosure, Elevation of Privilege
T5: Cross-Site Request Forgery (CSRF)	Moderate	CM	Spoofing, Privilege Escalation
T6: SQL Injection	Not Likely	RH, LC	Tampering, Information Disclosure

Loss in Revenue (LR), Costs for Mitigation (CM), Reputation Harm (RH), Legal Costs (LC)

Next, a risk analysis is conducted to highlight the threats that introduce more risks for the business in terms of economic and technical. A risk assessment matrix is built, considering two different scales: Likelihood and Impacts. Based on that, it is possible to map the risks of each threat as Low, Medium, and High. For example, one threat that have a *Moderate* likelihood of happening but the impacts are *Acceptable* is classified as *Low* risk. On the other hand, a likelihood defined as *Likely* and impact as *Tolerable* is classified as *High* risk.

Figure 5.12 shows the risk assessment matrix for PARME AG, taking as input all of the six threats initially mapped. As can be seen, the most critical threats (*i.e.*, High risk) are the T1 (DDoS), T2

(Phishing), and T3 (Ransomware). The threats T4 (Insiders and Supply Chain Attacks) and T5 (CSRF) have also to be considered, since they have a *Medium* risk. The T6 (SQL Injection) does not offer too much risk (in terms of likelihood vs. impacts), therefore should not be the priority at this step. Here, the SecRiskAI and SecBot solutions developed can also be used to support the understanding of risks and priorities.

	Risk		
Likelihood	Acceptable	Tolerable	Unacceptable
Not Likely	T6	-	-
Moderate	-	T4, T5	T3
Likely	-	T2	T1

Low Risk
Medium Risk
High Risk

Figure 5.12: Risk Matrix for the Threats Mapped in the PARME AG

Based on that threat modeling and risk analysis, it is possible to determine what is critical and the priorities to achieve the level of protection needed. Thus, by analyzing this information, the conclusions to be taken into consideration are the following:

- The risk of phishing and ransomware is increasing, and it has become one of the most significant threats for the company. Training and Protections are a must;
- DDoS attacks are one of the biggest threats to the availability of the E-Commerce platform. Protections are a must;
- Insiders and Supply Chain attacks are also a cause of concern [125], and new processes and protections have to be defined to reduce their possible impacts;
- Training and education of employees have to be done focusing on the most common threats identified for the company;
- Best practices of development and tests have to be applied to avoid threats like CSRF, Cross-Site Scripting (XSS), and others Web Application security risks.

5.7.3 Phase C: Cybersecurity Requirements

After the briefing and analysis of all threats and risks, it is now required to determine the cybersecurity requirements of the company. This includes services and equipment required, additional training for the employees, and the definition of new processes that have to be implemented by the PARME AG to have a proper strategy to run their E-Commerce safely. The decision-makers define these requirements during the planning of the cybersecurity strategy. Table 5.11 summarizes all of the cybersecurity requirements. These requirements are looked into because of the company's characteristics and initial demands. However, different requirements can be considered according to the initial information collected during the briefing and brainstorming (*i.e.*, Phase A).

The requirements are defined from R1 to R7, including constraints defined by the business team, and possible providers for these kinds of solutions are mapped. For example, R1 describes that cloud-based DDoS protection has to be contracted to protect against specific types of DDoS attacks. Possible providers for this kind of solution are Imperva, Verisign, Akamai, and Cloudflare. Furthermore, as highlighted by R6 and R7, some more general requirements can be defined, including the definition of new processes for software updates and training activities for the company's employees. Thus, Table 5.11 gives the information required to determine the budget and total costs of the cybersecurity strategy to be defined.

Note that a list of possible providers can be selected based on the business demands and also consider providers' reputation and characteristics of the protection products. This information can be obtained by contacting companies, using publicly available information, such as the catalog provided by CyberTango [50] or also relying on marketplaces and SLAs provided by Kirti (*cf.* Section 4.8.3) implemented as a supplementary service. With the requirements defined and possible providers, it is possible to estimate the costs and determine how to ensure the cybersecurity strategy's economic feasibility.

5.7.4 Phase D: Cost Management

It is important to determine how much budget must be available for this phase as an initial step. This amount can be achieved by applying the GL model (*cf.* Section 2.2.2) equation and concepts. For this case study, the GL model is applied to calculate two different values: the *(i)* maximum budget for cybersecurity and *(ii)* optimum investment per segment (*i.e.*, assets). This helps the company have a broad understanding of how to determine their budget and the costs of the cybersecurity strategy.

The company's total revenue was previously determined as US$ 15 million yearly, and the E-Commerce itself as a value of US$ 5 million for the company. Therefore, this last will be considered as the poten-

Table 5.11: Overview of Defined Requirements for the PARME AG and Possible Providers

Requirement	Constraints	Possible Providers
R1: Cloud-based DDoS protection	Must be cloud-based and provide defenses against at least SYN, ICMP, and UDP flood	Arbor, Verisign, Akamai, and Cloudflare
R2: Email security and phishing protection	-	Proofpoint, Abnormal Security, IronScales, and Barracuda
R3: Software against viruses and malware	Must provide endpoint security protection for all computers connected in the company's network	Symantec, McAfee, Microsoft Defender, and Bitdefender
R4: Implement a monitoring and logging strategy	Must be stored out of the company premises	-
R5: Security audit and code review before deployment of new features on the company's solutions	Must consider all of the stakeholders, threats, and risks mapped for the business	Internal analysis, consultancy companies, and security experts
R6: Monthly updates for critical software and semiannual updates for others software	All software must run the last stable version with the most recent security patches	-
R7: Education and training of employees against phishing and Social Engineering attacks	Must have online courses contracted for continuous education and face-to-face training for selected threats	Coursera, consultancy companies, and Swiss universities

tial loss if a successful attack happens in the E-Commerce and underlying infrastructure. Without any investment (*i.e.*, z = 0), the risk of an attack happening is equal to 64%, and the success rate is equal to 41%. This information is related to the worst scenario possible. Thus, the GL model equation for maximum investment (z_{max}) is applied. The results is shown in Equation 5.1. It means that the investment in cybersecurity should not exceed US$ 485,440 annually to protect PARME's E-commerce.

$$\begin{aligned} vL &= 5,000,000 \times 0.64 \times 0.41 \\ vL &= US\$1,312,500 \\ z_{max} &= 1,312,500 \times 0.37 \\ z_{max} &= US\$485,440 \end{aligned} \tag{5.1}$$

This calculation indicates the maximum budget but is still not the optimum investment possible. In order to calculate the optimum investment (z^*), the SECAdvisor tool (*cf.* Section 4.6) will be used. The SECAdvisor can help with this task by applying the different equations of the GL model in a user-friendly and straightforward way. First, the company must add information about its segments and assets in the SECAdvisor tool. Next, the SECAdvisor calculates a set of metrics to determine the

optimum investments for each segment and the investments' economic benefits. Figure 5.13 shows the optimal investment calculated for three different segments of PARME AG. This case study focuses on the first one: The E-Commerce running as a Web Server. For this one, with a value estimated at US$ 5,000,000 (total yearly revenue), the optimal investment calculated is equal to US$ 75,623. This means that the optimal amount to protect the E-Commerce platform is roughly only 15% of the previously calculated z_{max}. It is important to state that in the backend, the SECAdvisor is running the GL equations as defined in [144]. The Appendix E shows examples of different values calculated until achieving this optimal investment.

Segments Overview

Name	Type	Risk	Vulnerability	Value($)	Optimal Investment($)	Actions
E-Commerce	Web Server	64%	41%	5'000'000	75'623	
Databases	Database	51%	43%	2'000'000	27'665	
Internal Network	Network	6%	12%	20'000'000	43'246	

Figure 5.13: Optimal Investment for the PARME AG Segments Calculated Using SECAdvisor

With this amount now at hand, it is possible to start the search to satisfy all seven requirements by spending not more than US$ 75,623 annually. Therefore, it is possible now to analyze the different requirements and estimate what is possible to do with this budget determined by the GL model.

R1 (Protection against DDoS attacks), R2 (Email security), and R3 (Antivirus) need a decision about which of the protections available are more suitable in terms of technical and economic demands. The MENTOR recommendation engine is used and provides four candidate providers. The ROSI model can be applied to determine which is the most cost-efficient protection. In order to automate this process, the MENTOR is used integrated with the SECAdvisor. This then relies on the engine of MENTOR for the recommendation process and calculates the ROSI for each recommended protection.

Figure 5.14 shows how the protection that satisfies R1 was selected. The exact process happened for protections that satisfy R2 and R3. At the top, the PARME AG can configure all of the information needed for the recommendation engine to process the request. In this case, the company wants protection against DDoS attacks, and the maximum investment is the one calculated before. After submission, the solution recommends four different protections that fits the budget available and the technical demands of the company. In blue, on the bottom, there is the solution's price per leasing pe-

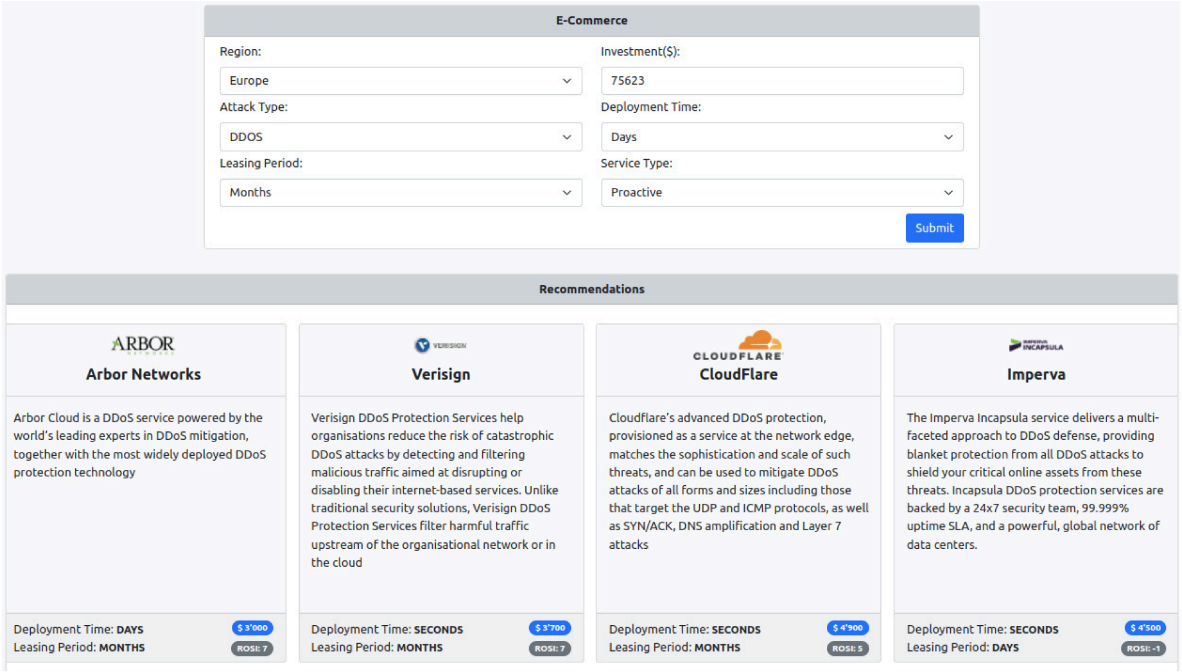


Figure 5.14: Optimal Investment for the PARME AG Segments Calculated Using SECAdvisor

riod. Right after, in grey, there is the calculation of the ROSI metric for each solution, which indicates which one is the most cost-efficient.

For this recommendation, the annual rate of occurrence of DDoS attacks is defined as three. The loss due to DDoS attacks is measured as US$ 2,000 per hour of the attack, with an average of seven days of the week. This means an incident costs equal to US$ 144,000. Based on this information and protection characteristics, the calculation of ROSI can be performed. For example, the ROSI of the Verisign is equal to 7 (rounded), which means that the payback on this investment is 700%. This is an excellent ROSI and means this is a cost-effective solution. The Verisign DDoS Protection calculation considered a mitigation rate equal to 80% of DDoS attacks and the cost of the solution equal to US$ 3,700 per month. Equation 5.2 shows the calculation for the Versign DDoS Protection. The SECAdvisor automates the calculation for all protections by applying the same process but with different information whenever needed.

$$
\begin{aligned}
ROSI &= \frac{((144,000 \times 3) \times 0.7) - (3,700 \times 12)}{3,700 \times 12} \\
ROSI &= \frac{(432,000 \times 0.7) - 44,400}{44,400} \\
ROSI &= 6.78 \ (\textit{i.e.}, \text{Cost-effective})
\end{aligned}
\tag{5.2}
$$

Besides identifying protections, all other expenses have to be identified, and products that fit the budget available (not exceeding the GL values) have to be mapped and selected. Thus, following the CyberTEA methodology, the costs to achieve a cybersecurity strategy that fits all company requirements are defined. Table 5.12 summarize all costs mapped to achieve the requirements of the company in terms of the level of security.

Table 5.12: Summary of Costs to Address All Requirements of the Cybersecurity Strategy

Investment	Requirement Covered	Provider	Product	Cost (Yearly)
Protection against DDoS	R1	Verisign	DDoS Mitigation Service	US$ 44,400
Email security	R2	Barracuda	Premium Email Protection	US$ 1,800
Anti-Virus and Anti-Malware	R2 and R3	Bitdefender	GravityZone Business Security	US$ 3,000
Storage and management of critical logs	R4	SolarWinds	Log Event Manager	US$ 1,900
Security analysis and code verification	R5	PwC Switzerland	Source Code Analysis	US$ 10,000
New process for continuous update and upgrade of software	R6	SolarWinds	Patch Manager	US$ 2,000
Online security awareness education and on-site training	R7	Coursera and University of Zurich UZH	Cybersecurity Awareness Training and Hands-On	US$ 5,200
-	-	-	**Total**	**US$ 58,300**

The Verisign DDoS Mitigation Service was selected from the list of recommended protections. Note that not necessarily the cheaper solution is the best one. In this case, the protection provided by the Arbor Networks was cheaper, but the mitigation rate and the attack types covered by Verisign were preferred. Thus, R1 can be addressed by spending roughly US$ 44,400. This is by far the most costly requirement for this scenario.

For R2, the Barracuda offers a complete suite of Email protections against phishing and other attacks, with a cost of US$ 5 monthly per user. PARME AG wants to protect 30 users (number of employees). Therefore, the total cost is US$ 1,800 per year (number of users $\times$ US$ 5 $\times$ 12). Next, after checking with the Bitdefender providers, the GravityZone Business Security price for 100 devices coverage during one year equals US$ 3,000. This satisfies all requirements to address R3 and partially R2.

R4 needs the storage of logs monitored by internal solutions. These logs can be stored on a secure cloud provided by Loggly using the SolarWinds Log Event Manager. This solution allows for the integration of different types of logs (*e.g.*, Linux system logs, HTTP events in the endpoints, and database access control). The price for this solution is US$ 159,00 monthly in its Pro version, recommended

for growing companies. Thus, US$ 1,900 can be allocated for this tool. Cheaper solutions (*e.g.*, open source and free tools) can address this requirement but would require additional time and expertise for the usage and deployment.

For R5, the PwC branch in Switzerland will be contracted for occasional security and code verification before a new critical feature is added to the company. A total amount of US$ 10,000 will be allocated for this matter, which can vary according to the demands.

R6 stands for the continuous update and upgrade of the company's software. Different costs have to be considered for this requirement, such as new software licenses, additional hardware to run the software, and allocation of people to conduct the updates. However, PARME AG decided to automate the process by contracting the SolarWinds Patch Manager with a price of US$ 2,000 per year.

Finally, R7 requires the education and specific training of the employees of PARME AG to increase cybersecurity awareness and reduce potential attack vectors (*e.g.*, Social engineering techniques and phishing). Based on the reputation and ease of access, one paid course available at Coursera was selected for the online security awareness training, which allows for up to 50 employees to access the content with the investment of US$ 2,200 in the first year. Also, an on-site training conducted by the Communication Systems Group (CSG) of the University of Zurich UZH was preferable since previous collaborations between the group and the company have been placed. This on-site training will cost US$ 3,000 per year for the company. Therefore, the total amount in training and education is defined as US$ 5,200.

Thus, as summarized in Table 5.12, after the costs calculations, the amount to plan to invest in a cybersecurity strategy that fits all requirements of the company is equal to US$ 58,300. This amount is 78% of the optimal investment previously defined by the GL model. Therefore, there is still an amount of US$ 17,300 that can be used to address additional requirements or to be invested to cover not expected costs during the deployment and operation of the cybersecurity strategy, such as contract consultancy and experts to support and train the company's team in specific activities. Also, this amount can be used to buy additional equipment if needed or to increase the IT team (*e.g.*, allocate people partial time to work on security aspects of the company).

5.7.5 Phase E: Execution and Deployment

Finally, the last phase of the *CyberTEA* methodology involves executing and deploying the cybersecurity strategy. If not placed in the company already, technical support can be achieved by contracting consultants. Also, a clear deployment schedule must be defined, since some company sectors might need to stop their operations for a few hours to deploy the solutions and new processes fully. Suppose the infrastructure to deploy the solutions is not available to the company. In that case, it is possible

to host that on the cloud, also being supported by solutions like BRAIN (*cf.* Section 4.8.4) that offers a reverse auction model for infrastructure providers to host virtualized protections.

After deploying the cybersecurity strategy, continuous operation and maintenance tasks have to be performed, such as continuous monitoring of critical activities and analysis of new threats. These tasks can be done using the new protections contracted or additional open-source solutions like SecGrid that allow for post-mortem analysis of cyberattacks to redefine the cybersecurity strategy and priorities in the future. These tasks must also be covered by the budget available, the technical expertise, and the new processes implemented by the company. Also, information sharing can be considered to support partners and the entire sector with helpful information regarding cybersecurity trends. The SHINE supplementary solution proposed in Section 4.8.2 can be used to share the economic impacts of cyberattacks. The company's management board must consider which kind of agreements must be placed. These agreements might allow for information sharing to strengthen the cybersecurity of the sector and the company's supply chain.

For this case study specifically, these operation and maintenance tasks involve the continuous analysis of critical logs stored, the request for code analysis (and fixes it whenever needed) before a new feature is deployed, the update of software, continuous training and education, and maintenance of the solutions implemented for protection (*i.e.*, ensure that all is working according to the needs). It is key to have a responsible employee for all of these operation and maintenance tasks for all of these operation and maintenance tasks. Even if that is not possible to have one full-time responsible employee due to budget constraints, the company must know who is the point of contact in case of any specific request or problem.

Thus, after following in detail all of the phases and steps provided by the *CyberTEA* methodology, the PARME AG was able to *(i)* define its cybersecurity demands based on the current company structure, *(ii)* determine the threats and risks of potential impacts (*e.g.*, economic losses and technical disruption) due to cyberattacks, *(iii)* describe the requirements to achieve an adequate level of protection according to its needs, and *(iv)* manage the costs to obtain a cost-efficient cybersecurity strategy. After deploying the strategy, the company is expected to achieve the right level of protection according to the demands to run its new E-Commerce business without putting critical risks to its assets, reputation, and revenue.

5.8 Lessons Learned from the Evaluations

Different evaluations were conducted to obtain measurable results about the feasibility and performance of the *CyberTEA* approach (*i.e.*, Methodology and Framework) and the solutions implemented.

For that, quantitative evaluations were performed when required and possible, while qualitative evaluations were conducted for solutions with dimensions validated using case studies or interviews with real-world stakeholders.

Lesson 1. ML-based solutions are an ally for specific cybersecurity planning tasks but the definition of datasets with real-world data is still a challenge. The solutions proposed to support Risk Management using ML have been evaluated in their models' performance, feasibility, and accuracy. Both SecRiskAI and SecBot achieving high accuracy for the evaluated scenarios. More specifically, SecRiskAI was able to predict correctly the risks of DDoS attacks and phishing based on selected attributes of the company, while SecBot was able to extract intents from conversations and provide cybersecurity guidance against threats. However, as the evaluations were based on synthetic datasets and data obtained from publicly available sources, these results must be checked against real-world scenarios. The methodology defined and the proof-of-concept implemented for both solutions provide a clear path to define datasets and train new models that satisfy the reality of companies. Thus, proving that ML-based approaches like SecRiskAI and SecBot can be an ally for companies, especially SMEs. The major limitations that can be highlighted concern the limited real-world information available to train and test the solutions more in-depth.

Lesson 2. Solutions to process and analyze cyberattacks traffic are possible and efficient resources usage are key. For the processing and analysis of the threat, one of the main pillars to be evaluated is the capacity to process a large amount of traffic. Different dimensions have to be analyzed, such as the time and resources required to process datasets containing malicious traffic. Also, the capacity to extract meaningful information from these datasets are key. Thus, a quantitative evaluation was conducted on the miners implemented by SecGrid to obtain results about the efforts required to process large datasets (around 100 GB of PCAP files), including the consumption of RAM, CPU, and time to run each miner. These results show that SecGrid efficiently processed different files and cyberattacks in a commercial off-the-shelf laptop. Also, the ML-based classification of cyberattacks was evaluated, resulting in a final model able to correctly identify different DDoS attacks in PCAP files without introducing overhead in data processing and classification. However, as stated before, this model also has to be adapted for specific cyberattacks that have to be identified. A list of DDoS attacks from datasets publicly available was used, thus, allowing for the detection of the most common types of DDoS attacks.

Lesson 3. Visualizations have a key role the for analyzing and understanding cyberattacks behaviors. Still, the feasibility and usability of the SecGrid were evaluated. For that, qualitative evaluations were conducted. First, interviews with potential users were conducted following the SUS questionnaire approach. The results were excellent regarding usability and how useful the users con-

sider using solutions like SecGrid. Next, case studies show scenarios in which SecGrid can be applied. This provided evidence that approaches like SecGrid can positively impact the analysis of cyberattacks, especially for people who do not have a complete background in cybersecurity. It is important to decouple the complexities of packet analysis and present the results visually and interactively to users, as done by other cybersecurity tools that already rely on information visualization (*e.g.*, ELK and Splunk). Also, extensibility was one of the most important features in this case, since solutions should not limit the use cases. The extensible design followed by SecGrid allowed for a couple of works to be developed on top of SecGrid, thus, helping the community with still additional features without reinventing the wheel.

Lesson 4. Cybersecurity economic models supports the cost management when planning a cybersecurity strategy; however, these models have to be calibrated according to company's characteristics. The optimal investments calculated using the SECAdvisor were demonstrated using case studies with three different information segments. This shows that the application of the GL model is a practical and automated way, thus, simplifying the decision process on optimal investments for companies. Besides, the ROSI calculation was performed, and recommendations of protections during the case study. Additionally, quantitative experiments are possible still required for the GL model itself, but it was out of the scope. Therefore, the evaluations on optimal investments demonstrated how the SECAdvisor could contribute to applying well-known cybersecurity economics metrics.

Lesson 5. Recommendation mechanisms can be placed to filter protections and indicate adequate solutions according to companies demands. The recommendation of protections was evaluated quantitatively, more specifically, the different algorithms fr correlation measurements and their performance in different scenarios. This allowed determining which one is more suitable for the development of MENTOR. Also, the integration with a couple of tools (*e.g.*, ProtectDDoS [89], SERViz [123], and SECAdvisor [41]) highlighted how recommendation of protections can contribute for a key decision that is part of any cybersecurity planning approach. The role of reputation is also shown to have a critical impact on the decision process for protection. This topic was partially covered by implementing and evaluating traditional and BC-based reputation systems.

Lesson 6. Reputation mechanisms can be an ally for selection of protections and market analysis. Nevertheless, there is a path that academia and industry can move in the direction of reputation in cybersecurity solutions. Also, the vast amount of protection available on the market makes it hard to define which metrics to consider. For the evaluations conducted, we defined a set of metrics that can be common for the decision process combined with specific characteristics of cyberattacks

(*e.g.*, protections against families of malware or specific DDoS attacks). This resulted in a solution that can be used as an ally to limit the search list for the proper protection for a company.

Lesson 7. Blockchains are a viable approach (but with additional costs) that can be explored to simplify cybersecurity-related tasks and to develop trustworthy cybersecurity solutions. Regarding the BC-based approaches, there has been a hype of applications trying to address different problems using the decentralization, non-repudiation, and immutability concepts provided by the BC. However, as was shown during the experiments, additional costs have to be considered for proposing such applications. For example, the SaCI allows for the automation of cyber insurance contracts and increases the amount paid besides the premium. The Kirti allows storing protection information and monitoring SLAs, relying more on the IPFS to reduce storage costs. Then, finally, the BRAIN proposed a reverse auction that helps find the best infrastructure (in terms of resources and costs) to host a virtualized protection. However, the case studies conducted for these three BC-based solutions show that the BC can be used. However, such approaches' key contributions are more on simplifying complex processes (*e.g.*, cybersecurity contract underwriting, protections marketplace, and deployment of virtualized protections) than on the decentralization that BC enables.

Lesson 8. Approaches that defines the phases and guides cybersecurity planning and investment are useful to support the decision-making and the adoption of cybersecurity, specially in SMEs. Finally, an end-to-end case study was conducted to show all of the phases of the *CyberTEA* methodology being covered. For that, a hypothetical company was defined but taken as the basis of real-world data of a Swiss SME market. All phases and steps were covered to show how to build a new cybersecurity strategy from scratch, including understanding business demands, modeling threats, the definition of cybersecurity requirements, optimal investments, and deployment of the strategy. During each phase, examples were provided of how developed solutions can contribute to simplifying the task of obtaining specific information needed for each decision. Thus, the feasibility of the methodology and the benefits that each solution can provide during the cybersecurity planning and investment were demonstrated. It gives evidence of how the framework proposed as part of the *CyberTEA* approach covers relevant tasks required.

Lesson 9. Scientific advances and knowledge gain proved that novel models and approaches considering cybersecurity economics, cost management, and cybersecurity planning are possible and needed. This includes the validation of already existent models as well as the development and evaluation of novel solutions that address particular security problems that companies are facing today and in the next decades, specifically those with technical and economic dimensions. The scientific results validates technical problems and their relevance, thus, paving the path for developing novel research and solutions for a safer digital world. Each of the solutions designed and developed

has measurable results and contributions. Also, the developed solutions give examples and motivation to researchers explore a rich field with open problems ready to be addressed. At the same time, the methodology and framework proposed open opportunities for extensions and guided new market-ready implementations.

The journey is its own reward.

Homer

6

Summary, Conclusions, and Future Research

CYBERSECURITY has become a cause of concern for companies and governments due to their increased dependency on digital systems and the destructive capacity of cyberattacks shown in the last years. Cyberattacks are mainly motivated by financial incentives that attackers can make and affect companies from an economic, technical, and legal perspective, causing impacts on people who need services from a specific company or sector. An adequate cybersecurity strategy is one of the pillars of avoiding business disruption and financial losses due to cyberattacks. Also, governments worldwide are discussing how to enforce a minimum level of cybersecurity to companies, since weak cybersecurity can impact the entire supply chain of a sector, thus, impacting society's economy, well-being, and overall security.

However, the current scenario presents several challenges, since most companies (especially SMEs) still do not have an adequate level of cybersecurity to protect their business. Companies tend to allocate a low budget for cybersecurity, often do not have experts in-house, and react only if an attack happens instead of proactively planning their cybersecurity strategy. Even though this mindset is gradually changing, it is still a challenge for SMEs to understand their cybersecurity requirements and how to conduct all of the steps required for an adequate cybersecurity strategy.

This PhD thesis improved such a scenario by proposing an approach that simplifies the understanding, planning, and investment in cybersecurity. For that, the *CyberTEA* approach developed offers *(i)* a straightforward methodology to guide companies in the cybersecurity strategy definition process, *(ii)* a framework of components that have to be considered for implementing solutions to support SMEs, and *(iii)* a set of solutions that simplifies different processes of cybersecurity planning and investment, also satisfying the proposed framework.

6.1 Summary

This PhD thesis has initially provided an analysis and overview of the threat landscape and major impacts of cyberattacks on companies. This analysis helps the reader understand the current scenario of cyberattacks and the reality of companies of different sizes and from different sectors. Also, the current related work of cybersecurity planning and investment was mapped, thus, highlighting the current direction that researchers, governments, and industry are following to increase companies' cybersecurity. This includes effective regulations and organizational guidelines, clear methodologies, novel models and techniques, and user-friendly and automated solutions that simplify cybersecurity-related tasks.

After this analysis and understanding of the overall scenario, this PhD thesis has proposed a straightforward 5-phases methodology that allows companies to split the cybersecurity planning into small steps that provide the information and artifacts required by the next phase. As the output, the company can obtain a cost-efficient cybersecurity strategy that addresses all of the requirements identified and fits into the company's budget. The methodology starts with understanding the business and its demands (Phase A), followed by risk management (Phase B), which involves threat modeling and risk assessment. Next, the cybersecurity requirements must be defined (Phase C), including the new software, processes, and infrastructure needed. Then, cost management (Phase D) has to be performed to determine the best approach based on the budget and risks. Finally, the cybersecurity strategy can be deployed and operated (Step E) to protect the company and its assets.

A framework was then proposed to map and provide the components required to be considered, when developing solutions to support cybersecurity planning and investments. This framework is divided into four layers integrated by APIs. The first layer (Business) provides all components required for the interaction of users and business analysis (*e.g.*, characteristics, profile, and revenue). Next, the Risk Management Layer implements the components required to receive, process, and analyze data to conduct a company's threat modeling and risk analysis. Then, the Decision Layer is in charge of providing cost management components and selecting the best protections to satisfy all cybersecu-

rity requirements. A layer with supplementary solutions is also mapped, since different information might be required to address specific demands. Therefore, a fully integrated ecosystem can be created with different solutions that can contribute to the successful planning of the cybersecurity strategy.

Finally, five different solutions were designed and developed as part of the *CyberTEA* approach to perform different tasks mapped in the methodology and implement the components determined in the framework. These solutions were designed to abstract technical details as much as possible to support both technical and non-technical users during cybersecurity tasks and decision-making. *SecRiskAI* was proposed as an ML-based approach for risk assessment of companies based on selected (and well-known) attributes, such as the number of employees, sector, and business processes. *SecBot* provided a conversational agent to guide SMEs during the risk management tasks and also to help the understanding of cybersecurity demands. *SecGrid* was proposed as a platform for the analysis and visualization of cyberattack traffic, thus, helping companies to understand anomalies and potential threats. *SECAdvisor* provided an automated and user-friendly way to apply cybersecurity economics metrics to determine cost-efficient investments in cybersecurity. Finally, *MENTOR* was implemented as a recommender system for protections to support the decision process of selecting the best protection that fits business demands and budget. Four supplementary solutions were also implemented to address specific challenges, including *(i)* SaCI, a BC-based cyber insurance model, *(ii)* SHINE, a module for financial information sharing, *(iii)* Kirti, a protection marketplace, and *(iv)* BRAIN, a reverse auction for infrastructure supply.

Evaluations were performed to show evidence of the feasibility of each of these solutions. These evaluations were conducted quantitatively for performance and accuracy analysis, while qualitative analysis relying on interviews and case studies were also placed to show applications and benefits of the solutions proposed, the methodology, and the framework. Measurable results from the evaluations include *(a)* an end-to-end application scenario for the methodology, *(b)* the analysis of accuracy for risk assessment using SecRiskAI, *(c)* the capacity of SecBot to understand conversations and provide proper answers based on the intents of users, *(d)* the capacity of SecGrid to process a large amount of data to provide insightful visualizations and ML-based classification of cyberattacks, *(e)* the benefits of SECAdvisor and its usability for defining optimal investments and cost-effective solutions, and *(f)* the accuracy of MENTOR to recommend protections that fits the demands previously defined by companies. Also, these solutions' extensibility and integration were proven valid with proof-of-concept implementations. A case study was performed showing all of the phases of the proposed methodology being covered with the support of information obtained by using the proposed solutions whenever is needed. Furthermore, an analysis of the economic costs of the usage of

BC to ensure decentralization and immutability of cybersecurity solutions (*e.g.*, cyber insurance and marketplace) was provided.

The lack of approaches supporting cybersecurity planning was addressed considering technical and economic dimensions. Technical because the methodology and solutions proposed to consider and reduce the complexity of cybersecurity tasks by providing user-friendly interfaces, technical abstractions, and automation of specific tasks (*e.g.*, risk assessment and threat analysis). The economic perspective then comes from the focus on optimizing cybersecurity costs, thus, considering all economic impacts of cyberattacks and the benefits of cybersecurity investments to plan cost-efficient cybersecurity strategies that help achieve a proper level of protection even for companies with restrictions in budget.

6.2 Review of Research Questions and Contributions

The contributions can be summarized as the **three main contributions** (*i.e.*, methodology, framework, and set of solutions) followed by additional research and finds on the cybersecurity planning field. These contributions answers all of the five RQs previously defined. An overview of the major contributions of this thesis and their relation with each RQ is shown in Figure 6.1.

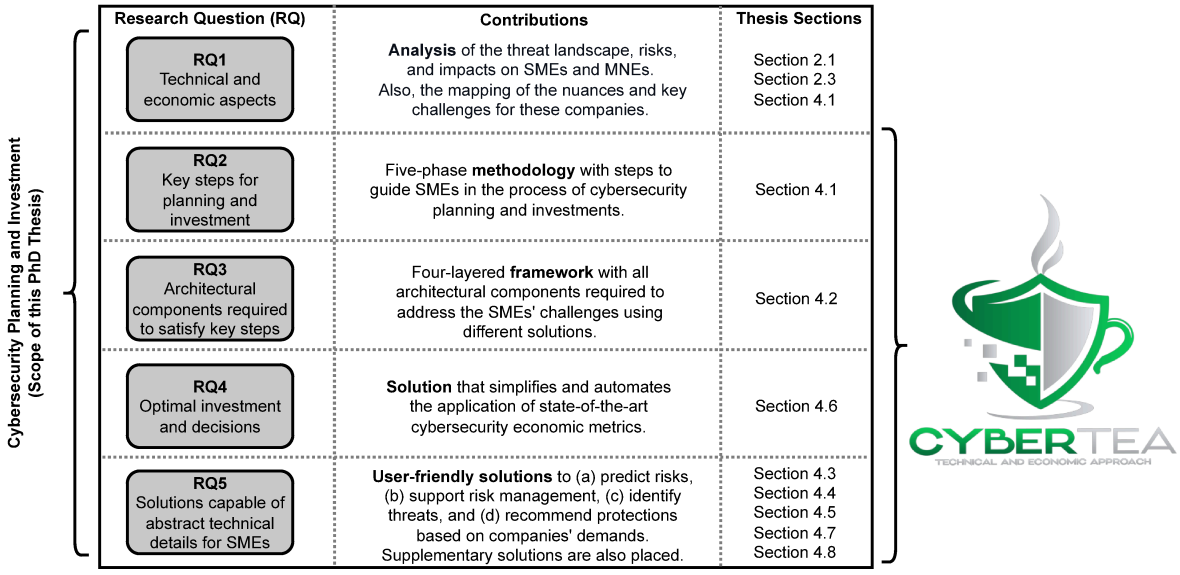


Figure 6.1: Overview of the Contributions and Research Questions of This PhD Thesis

Additional contributions include the analysis of the threat landscape and challenges that SMEs and MNEs are facing, the investigation of the state-of-the-art of the cybersecurity economics to propose

novel approaches that integrate the ones already existent, and the exploration of trend technologies and approaches (*e.g.*, ML/DL, blockchains, and visualizations) to address open challenges and explore the cybersecurity planning and investments problems from different perspectives.

RQ1: ***Which technical and economic aspects have to be considered during the planning and investing process to adopt cybersecurity strategies in SMEs?***

Understanding the different technical and economic aspects involved in planning and investments in cybersecurity is a key element, including the socio-economic impacts that a company might face in the case of a cyberattack. In order to answer RQ1, the threat landscape and the current SME scenarios in Europe were mapped. Also, a research on the market, its cybersecurity culture, and its main challenges were conducted **to determine phases and steps** required for cybersecurity planning and investments in SMEs.

Thus, an overview and mapping of the threat landscape, risks, and economic impacts were provided. Also, cybersecurity economics models were analyzed to understand economic behaviors of cyberattacks. The mapping of threats and risks was conducted based on the different domains identified and discussed in the literature, backed by the cybersecurity threat taxonomy defined by ENISA. The risks and impacts of companies were investigated by analyzing several reports from European agencies and worldwide consultancy companies. The answer of this RQ1 **is used to further define and validate** key aspects of planning and investing in cybersecurity, such as the risks, trends, and impacts SMEs are facing.

RQ2: ***What are and how to organize and simplify the key steps, information, models, and techniques required for an effective definition of a cybersecurity strategy in SMEs?***

This RQ2 required mapping and selecting the essential phases and steps to guide SMEs in planning and defining a cybersecurity strategy. Determine these elements is not a trivial task, since there is no simple answer that fits all possible scenarios. However, inspired by the different approaches already available in the literature, it is possible to determine a methodology that lists the main input and outputs expected from each phase as well as examples of steps to perform in each phase. This kind of methodology must have a flow that is easy to understand by all stakeholders and provide, as an outcome, a cost-efficient cybersecurity strategy.

Thus, a **five-phase methodology** was introduced as a contribution of *CyberTEA* approach to support SMEs in addressing all the different requirements, steps, and challenges involved in cybersecurity planning and investment. This contribution answers this RQ2 by mapping **the key phases involved in cybersecurity planning** (*i.e.*, Briefing, Risk Management, Definition of Cybersecurity

Requirements, Cost Management, and Execution) and highlighting the different tasks that must be performed to obtain a proper level of security in an organized and cost-efficient way. Evaluations based on case studies and interviews proved that the **well-structured methodology** proposed, supported by different solutions, can be used to guide decision-makers on cybersecurity planning, considering both technical (*e.g.*, threat modeling and protection performance) and economic aspects of cybersecurity.

RQ3: ***What are the necessary architectural components and actors to satisfy key phases and to allow SMEs to implement cost-effective cybersecurity strategies?***

During the research and definition of the methodology for planning and investment in cybersecurity, it was identified that different components and actors must be considered and implemented to satisfy all phases. These components have to allow for an integrated and friendly architecture that simplifies its adoption by decision-makers, developers, and cybersecurity experts, thus, allowing for evolving the approaches and solutions for cybersecurity planning and investment.

To answer this RQ3, a **four-layered framework** with a well-defined flow, architectural components, and actors was introduced. All of the layers (*i.e.*, Business, Risk Management, Decision, and Supplementary) are interconnected, allowing the communication and exchange of information among solutions with different features and goals. These layers and components **satisfies all key phases and steps** mapped into the methodology and guides the research on the design and implementation of solutions that contribute to the state-of-the-art in the cybersecurity planning field. Thus, the proposed framework **can be used** by stakeholders to understand the dependencies, information exchange, and relationships between the different layers of cybersecurity planning as well by developers and cybersecurity experts that want to provide novel solutions or reuse information already available in the *CyberTEA* approach.

RQ4: ***How to determine the optimum amount of resources (e.g., money, personnel, and time) an SME should invest in cybersecurity based on their specific technical and economic demands?***

This RQ4 addresses one of the main challenges identified during this PhD thesis: the decision on how much and where to allocate budget for cybersecurity. For that, an in-depth analysis of cybersecurity economics was conducted, resulting in a solution that simplifies and automates the application of state-of-the-art cybersecurity economic metrics, such as the GL and ROSI. Along with this PhD thesis, it was observed that the **integration of different metrics** in a single solution allows for a better analysis of the trade-offs between investments and protection, thus, helping to define a cybersecurity strategy that provides a proper level of protection but still considers the economic benefits of all investments.

The answer for this RQ4 was provided with **the design and implementation** of the SECAdvisor solution, which allows companies to *(i)* fill their business profile, *(ii)* define information segments and their assets, *(iii)* calculate optimal investments in cybersecurity per segment, and *(iv)* obtain recommendations of cost-efficient protections based on mitigation characteristics and the ROSI metric. Therefore, the answer for this RQ4 also satisfy the *Cost Estimator* and *Investment Calculator* component defined by the *CyberTEA* framework. Evaluations on SECAdvisor proved that cybersecurity economic metrics (*e.g.*, Gordon-Loeb and ROSI) **can be used** during the decision process to calculate the optimal investment, maximum investment, and also compare protections in terms of cost-efficiency. This was shown that these metrics addresses specific SMEs' challenges, such as lack of budget and expertise to decide about different protections.

RQ5: ***How to provide cybersecurity solutions capable of abstracting technical details to guide SMEs during the plan and execution of a cybersecurity strategy?***

This RQ5 had research and engineering nature, since it was required to *(i)* investigate and determine the path and requirements to address challenges and problems of cybersecurity planning and investments previously mapped by the *CyberTEA* methodology and framework, and then *(ii)* design and implement full-fledged solutions that satisfy these requirements in a user-friendly and effective way.

The answer for this RQ5 came as **a set of different solutions designed and developed** to address different challenges identified, such as risk analysis, recommendation of protections, automation of cyberattack classification, and risk sharing. These solutions satisfy all phases and steps defined by the *CyberTEA* methodology and implement all components mapped in the *CyberTEA* framework. Also, different integration among these solutions were placed to prove the capacity of abstract technical details required during the cybersecurity planning and investment. Besides being proven helpful for different scenarios, these solutions can be seen as proof-of-concept solutions to show opportunities and guide novel solutions in cybersecurity planning, especially for those considering technical and economic aspects while determining a cybersecurity strategy. These solutions were evaluated following **both quantitative and qualitative** approaches. **SecRiskAI** was proven to be efficient to classify (99% for SVM classifier) the risks of companies being target of a successful cyberattack using ML models trained with synthetic datasets, while SecBot provided high accuracy (100% for 15 different tested scenarios) in understanding and answering cybersecurity-related conversations. **SecGrid** was able to extract, process, and analyze data from 300 log files with different sizes (up to 100 GB) representing cyberattacks traffic, thus, providing insightful visualizations and ML-based classification of cyberattacks. The **MENTOR's** capacity and accuracy for recommend protections using different

correlation measurements was evaluated and validated using more than 10,000 random generated protections. Finally, **BC-based solutions** were evaluated from the economic point of view. Also, the benefits of decentralization provided BC were explored as an ally to support specific innovations on the field of cybersecurity planning.

6.3 Further Research Outlook

Although cybersecurity is a key concern for some companies, there is still a path to address open challenges (*e.g.*, information asymmetry, complex tasks for non-technical personnel, zero-day attacks) and evolve models and solutions to support a significant adoption of cybersecurity, especially by sectors of society that are still scarce of a proper level of protection. The research on determining and simplifying key steps for cybersecurity planning and investment is essential to the state-of-the-art of cybersecurity management, cybersecurity economics, and related areas. The contributions answered all RQs proposed on such a topic, but there are still various opportunities, open issues, and needs for further research on the topic.

The key steps for cybersecurity planning might vary according to specific scenarios and companies. Therefore, it is worthy of focusing future work on validating the current methodologies available in the literature and the *CyberTEA* methodology with real-world applications and refining it according to the best practices and threat landscape. One factor that has a path to evolve is how to measure the economic impacts of cyberattacks in a precise and well-defined way. This problem can be addressed by empowering ML/DL techniques, collaborative approaches, and information-sharing incentives.

Research on cybersecurity socio-economic models is also one of the main topics to be considered. As of today, most of the literature work applies variations of well-known metrics like GL, ROSI, and NPV to obtain cost-efficient benefits for cybersecurity. One path is to revisit these models to propose and evaluate novel models that fit the reality of companies and provide insightful information for the decision process on investments in cybersecurity. This path needs an in-depth evaluation, since most of today's models are still cumbersome and validated in generic scenarios, lacking evidence of actual benefits in real-world decisions. Also, these models can be extended by defining real-world datasets and creating ML models based on efficient cybersecurity investment decisions. Federated learning can be an ally, in this case, to enable collaboration without exposing critical information to define training datasets.

The solutions proposed in this PhD thesis addressed and paved the path for detailed cybersecurity planning and investment solutions. One of the main aspects of future work is the automation of cybersecurity analysis and risk assessment. This is one of the most significant lacks of cybersecurity.

ML-based approaches can be an ally to understand risks and and identify imminent cyberattacks. The capacity to process a large amount of data to create meaningful information for decision-makers is also a desired feature. Even though zero-touch approaches are emerging in the network management field, approaches that consider humans in the loop are still required to address specific challenges, such as lack of information curation, risk of false positives, and lack of one-size-fits-all solutions.

Regarding the proof-of-concept of the solutions specifically implemented by this PhD thesis, research directions can focus on the *(i)* refinement and investigation of the relevance and weight of each data attributes used for the learning process of SecRiskAI, *(ii)* investigation of reinforcement learning and immediate feedback of users to increase accuracy and usability of conversational agents like SecBot, *(iii)* proposing of new miners and visualizations to provide more accurate analysis for different scenarios and cyberattacks on the SecGrid, *(iv)* implementation of new features based on visualizations to allow a better understanding and customization of GL model for specific scenarios, and *(v)* design of ML techniques to combine different similarity measurements and new key metrics for the recommendation of protections using MENTOR.

Finally, the application of novel technologies and concepts has to be considered to evolve potential approaches to support cybersecurity. For example, cyber insurance approaches are a trending topic that BC can support to automate the process, ML/DL for automated risk assessment, and cybersecurity economic metrics to support cyber insurance underwriting. Also, incentives for information sharing have to be taken into account. Economic models and collaborative approaches have to be placed to move toward a more efficient cybersecurity ecosystem for governments, companies, and people.

Bibliography

[1] A. Charle, M. F. Franco, "Kirti - Source Code," 2020, https://gitlab.ifi.uzh.ch/franco/kirti.

[2] A. Kumar, T. Joon Lim, "Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-sampled Packet Traffic Analysis," Future of Information and Communication Conference (FICC 2019), San Francisco, USA, February 2019, pp. 847–867.

[3] A. Parmisano, S. Garcia, M. J. Erquiaga, "Aposemat IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic," January 2020, https://www.stratosphereips.org/datasets-iot23.

[4] A. Ross, T. Moore, "The Economics of Information Security," Journal of Science, Vol. 314, pp. 610–613, October 2006.

[5] A. Waldman, "Cybersecurity Investments Surge in 2021 as VCs Go All In," July 2021, https://searchsecurity.techtarget.com/feature/Cybersecurity-investments-surge-as-VCs-go-all-in.

[6] A. Abhishta, "The Blind Man and The Elephant: Measuring Economic Impacts of DDoS Attacks," Ph.D. dissertation, University of Twente, Netherlands, Dec. 2019.

[7] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," IEEE Access, Vol. 9, pp. 44 928–44 949, 2021.

[8] Accenture, "Ninth Annual Cost of Cybercrime Study," March 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.

[9] I. Aguirre and S. Alonso, "Improving the Automation of Security Information Management: A Collaborative Approach," IEEE Security Privacy, Vol. 10, No. 1, pp. 55–59, October 2012.

[10] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2020), Dublin, Ireland, 2020, pp. 1–5.

[11] M. Alharby and A. van Moorsel, "Blockchain-based Smart Contracts: A Systematic Mapping Study," International Conference on Computer Science and Information Technology (CoSIT), Geneva, Switzerland, March 2017.

[12] G. Alkawsi, A. K. Mahmood, and Y. Mohamed, "Factors Influencing the Adoption of Cloud Computing in SME: a Systematic Review," International Symposium on Mathematical Sciences and Computing Research (ISMSC), Ipoh, Malaysia, 2015, pp. 220–225.

[13] R. Anderson, "Why Cryptosystems Fail," 1st ACM Conference on Computer and Communications Security (CCS '93), Fairfax, USA, 1993, p. 215–227.

[14] R. Anderson, "Why Information Security is Hard - an Economic Perspective," 17th Annual Computer Security Applications Conference, New Orleans, USA, 2001, pp. 358–365.

[15] M. Anisetti, C. Ardagna, M. Cremonini, E. Damiani, J. Sessal, and L. Costa, "Security Threat Landscape," May 2020, https://sesar.di.unimi.it/security-threat-landscape/.

[16] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, "Understanding the Mirai Botnet," 26th USENIX Security Symposium (USENIX 2017), Vancouver, Canada, August 2017, pp. 1093–1110.

[17] I. M. Araújo, C. Natalino, A. L. Santana, and D. L. Cardoso, "Accelerating VNF-based Deep Packet Inspection with the use of GPUs," 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, July 2018, pp. 1–4.

[18] C. Ardagna, E. Damiani, M. Anisetti, and M. C. (Editors), "1st Year Report on Cybersecurity Threats," December 2019, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf.

[19] I. F. D. Arroyabe and J. C. F. de Arroyabe, "The Severity and Effects of Cyber-breaches in SMEs: a Machine Learning Approach," Enterprise Information Systems, pp. 1–27, 2021.

[20] J. v. d. Assen, "DDoSGrid 2.0: Integrating and Providing Visualizations for the European DDoS Clearing House," February 2021, Master Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[21] J. v. d. Assen, M. F. Franco, C. Killer, E. J. Scheid, and B. Stiller, "On collaborative threat modeling," Technical Report No. 2022.04, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, April 2022.

[22] AustCyber, "The Global Outlook for Cyber Security," 2019, https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter1.

[23] T. Aven and B. S. Krohn, "A New Perspective on How to Understand, Assess and Manage Risk and the Unforeseen," Reliability Engineering & System Safety, Vol. 121, pp. 1–10, January 2014.

[24] B. Aziz, Suhardi, and Kurnia, "A Systematic Literature Review of Cyber Insurance Challenges," International Conference on Information Technology Systems and Innovation (ICITSI 2020), Padang, Indonesia, October 2020, pp. 357–363.

[25] B. Filar, "Artemis: an Intelligent Assistant for Cyber Defense," 2017, https://www.elastic.co/blog/artemis-intelligent-assistant-cyber-defense.

[26] B. Rodrigues, M. Franco, C. Killer, E. J. Scheid, B. Stiller, On Trust, Blockchain, and Reputation Systems, ser. Optimization and Its Applications. Cham, Switzerland: Springer, 2022, No. 194, pp. 1–38, iSBN: 978-3-031-07534-6.

[27] BBC, "US Offers $ 10m Bounty for Colonial Pipeline Hackers," November 2021, https://www.bbc.com/news/technology-59176826.

[28] M. Benz and D. Chatterjee, "Calculated Risk? A Cybersecurity Evaluation Tool for SMEs," Business Horizons, Vol. 63, No. 4, pp. 531–540, August 2020.

[29] N. Berni, "SC4CyberInsurance: Automated Cyber-Insurance Contracts," January 2021, Master Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[30] R. Böhme, "Security Metrics and Security Investment Models," Advances in Information and Computer Security, I. Echizen, N. Kunihiro, and R. Sasaki, Eds. Berlin, Heidelberg: Springer, 2010, pp. 10–24.

[31] R. Böhme, S. Laube, and M. Riek, "A fundamental approach to cyber risk analysis," Variance, Vol. 12, No. 2, pp. 161–185, 2019.

[32] L. Boillat and J. v. d. Assen, "A Tool for Visualization and Analysis of Distributed Denial-of-Service (DDoS) Attacks," Communication Systems Group, Department of Informatics, Master Project, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, April 2020.

[33] L. Boillat, "DDoSGrid-Mining: Analyzing and Classifying DDoS Attack Traffic," Master Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, March 2021.

[34] L. Bondan, M. F. Franco, L. Marcuzzo, G. Venancio, R. L. Santos, R. J. Pfitscher, E. J. Scheid, B. Stiller, F. De Turck, E. P. Duarte, A. E. Schaeffer-Filho, C. R. P. d. Santos, and L. Z. Granville, "FENDE: Marketplace-Based Distribution, Execution, and Life Cycle Management of VNFs," IEEE Communications Magazine, Vol. 57, No. 1, pp. 13–19, January 2019.

[35] J. Brooke, "SUS: A Restropective," Journal of Usability Studies (JUS), Vol. 8, No. 2, pp. 29–40, February 2013.

[36] Bullguard, "New Study Reveals One In Three SMBs Use Free Consumer Cybersecurity And One In Five Use No Endpoint Security At All," February 2020, https://www.bullguard.com/press/press-releases/2020/new-study-reveals-one-in-three-smbs-use-free-consu.aspx.

[37] T. Bunk, D. Varshneya, V. Vlasov, and A. Nichol, "DIET: Lightweight Language Understanding for Dialogue Systems," May 2020, https://arxiv.org/abs/2004.09936.

[38] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 2014, https://ethereum.org/en/whitepaper/.

[39] C. Feng, Q. Wang, X. Xu, M. Franco, "SHINE - Source Code," 2021, https://gitlab.ifi.uzh.ch/franco/shine.

[40] C. Hesselman and T. van der Hout, "DDoS Clearing House for Europe," 2021, https://www.sidnlabs.nl/downloads/hHmYj5qY2q9lHYw9gB8LH/eb969909af2baebe3a3ec3e612ab0794/GA7_T3.2.pdf.

[41] C. Omlin, M. F. Franco, "SECAdvisor - Source Code," 2022, https://gitlab.ifi.uzh.ch/franco/secadvisor.

[42] C. Pugnetti, C. Casián, "Cyber risks and Swiss SMEs: an Investigation of Employee Attitudes and Behavioral Vulnerabilities," 2021, https://digitalcollection.zhaw.ch/bitstream/11475/21478/3/2021_Pugnetti-Casian_Cyber-Risks-and-Swiss-SMEs.pdf.

[43] Capgemini Invent, European Digital SME Alliance, and Executive Agency for Small and Medium-sized Enterprises (European Commission), Technopolis, "Skills for SMEs: Cybersecurity, Internet of things and Big Data for Small and Medium-sized Enterprise," December 2019, https://op.europa.eu/en/publication-detail/-/publication/82aa7f66-67fd-11ea-b735-01aa75ed71a1/language-en.

[44] A. Charle, "Kirti: Decentralized Reputation and SLA Enforcement for Cybersecurity," Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, September 2020.

[45] J. Clinch, "ITIL v3 and Information Security," 2009, technical Report.

[46] CMS Law, Tax, Future, "GDPR Enforcement Tracker," November 2021, https://www.enforcementtracker.com/.

[47] L. Coventry and D. Branley, "Cybersecurity in Healthcare: a Narrative Review of Trends, Threats and Ways Forward ," International Journal of Midlife Health and Beyond (MATURITAS), No. 113, pp. 48–52, April 2018.

[48] Cybersecurity Osservatorio, "Self Assessment Questionnaire," 2021, https://www.cybersecurityosservatorio.it/en/Services/survey.jsp.

[49] Cybersecurity Ventures, Herjavec Group, "The 2020-2021 Healthcare Cybersecurity Report," October 2021, https://www.herjavecgroup.com/2021-healthcare-cybersecurity-report-cybersecurity-ventures/.

[50] Cybertango, "The Cybersecurity Directory," 2022, https://www.cybertango.io/.

[51] D. Ben Peretz, "A Siri for Network Security: How Chatbots can Enhance Business Agility," 2020, https://www.infosecurity-magazine.com/opinions/network-chatbots-agility/.

[52] D. P. David, A. Mermoud, and S. Gillard, "Cyber-Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model," December 2021.

[53] A. Deljoo, T. van Engers, R. Koning, L. Gommans, and C. de Laat, "Towards Trustworthy Information Sharing by Creating Cyber Security Alliances," 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2018), New York, USA, August 2018, pp. 1506–1510.

[54] M. Dübendorfer, "Distributed Analysis of Cyberattacks in a Collaborative Setting," Communication Systems Group, Department of Informatics, March 2022, Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[55] E. Sula, M. F. Franco, B. Rodrigues, "ProtectDDoS - Source code," 2020, https://gitlab.ifi.uzh.ch/franco/ddosrecommendation.

[56] E. Sula, M. Franco, "The SecRiskAI - Source Code," 2021, https://gitlab.ifi.uzh.ch/franco/ml-risk-smes.

[57] Etherscan, "Ether Daily Price (USD) Chart," May 2022, https://etherscan.io/chart/etherprice.

[58] ETSI GS NFV-MAN, "Network Functions Virtualisation (NFV); Management and Orchestration," December 2014, white Paper. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf

[59] European Central Bank, "Financial Risk Map for 2020," July 2020, https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2020~a9164196cc.en.html.

[60] European Comission, "User Guide to the SME Definition," 2015, https://ec.europa.eu/regional_policy/sources/conferences/state-aid/sme/smedefinitionguide_en.pdf.

[61] European Commission, "The EU Cybersecurity Act," 2019, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[62] European Telecommunications Standards Institute (ETSI), "Cybersecurity for SMEs: Cybersecurity Standardization Essentials," 2021, eTSI TR 103 787-1, https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf.

[63] European Union Agency for Cybersecurity (ENISA) , "Threat Landscape," October 2020, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[64] European Union Agency for Cybersecurity (ENISA), "Economics of Security: Facing the Challenges," December 2012, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/EoSFinalreport.

[65] European Union Agency for Cybersecurity (ENISA), "Introduction to Return on Security Investment: Helping CERTs Assessing the Cost of (Lack of) Security," 2012, https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.

[66] European Union Agency for Cybersecurity (ENISA), "National Cyber Security Strategies: An Implementation Guide," December 2012, https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

[67] European Union Agency for Cybersecurity (ENISA), "Threat Taxonomy," September 2016, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[68] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Skills Framework," 2020, https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.

[69] European Union Agency for Cybersecurity (ENISA), "Highlights on the National Cybersecurity Strategies," October 2020, https://www.enisa.europa.eu/news/enisa-news/Highlights-on-the-National-Cybersecurity-Strategies.

[70] European Union Agency for Cybersecurity (ENISA), "Cybersecurity for SMEs: Challenges and Recommendations," June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

[71] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Guide for SMEs - 12 Steps to Securing your Business," June 2021, https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes.

[72] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Spending: An analysis of Investment Dynamics within the EU," November 2021, https://www.enisa.europa.eu/publications/nis-investments-2021.

[73] European Union Agency for Cybersecurity (ENISA), "Threat Landscape 2021," October 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[74] European Watch on Cybersecurity Privacy, "Cybersecurity Label," 2021, https://label.cyberwatching.eu/.

[75] M. Felici, N. Wainwright, S. Cavallini, and F. Bisogni, "What's New in the Economics of Cybersecurity?" IEEE Security and Privacy, Vol. 14, pp. 11–13, May 2016.

[76] C. Feng, Q. Wang, and X. Xu, "SHINE: a Collaborative System for Sharing Insights and Information of Economic Impacts of Cyberattacks," Master Project, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, May 2021.

[77] A. Fielder, S. König, E. Panaousis, S. Schauer, and S. Rass, "Risk Assessment Uncertainties in Cybersecurity Investments," Games, Vol. 9, No. 2, June 2018.

[78] Fortune Business Insights, "Cyber Security Market Size, Share COVID-19 Impact Analysis," 2022, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

[79] K. Fotiadou, T. Velivassaki, A. Voulkidis, K. Railis, P. Trakadas, and T. Zahariadis, "Incidents Information Sharing Platform for Distributed Attack Detection," IEEE Open Journal of the Communications Society, Vol. 1, pp. 593–605, April 2020.

[80] F. Fowley, C. Pahl, P. Jamshidi, D. Fang, and X. Liu, "A Classification and Comparison Framework for Cloud Service Brokerage Architectures," IEEE Transactions on Cloud Computing, Vol. 6, No. 2, pp. 358–371, 2018.

[81] M. Franco, N. Berni, E. J. Scheid, B. Rodrigues, C. Killer, and B. Stiller, "SaCI: a Blockchain-based Cyber Insurance Approach for the Deployment and Management of a Contract Coverage," Lecture Notes in Computer Science (LNCS), No. 13072. Virtually: Springer, September 2021, pp. 79–92.

[82] M. Franco, J. V. der Assen, L. Boillat, C. Killer, B. Rodrigues, E. Scheid, L. Granville, and B. Stiller, "DDoSGrid: a Platform for the Post-mortem Analysis and Visualization of DDoS Attacks," 20th IFIP Networking (Networking 2021). Espoo, Finland: IFIP, June 2021, pp. 1–3.

[83] M. Franco, L. Granville, and B. Stiller, "A Business-Driven Integrated Ecosystem for Cybersecurity Planning and Management," CONCORDIA Early Stage PhD Workshop (CON-PHD), Twente, Netherlands, June 2020, pp. 1–6.

[84] M. Franco, B. Rodrigues, C. Killer, E. J. Scheid, A. De Carli, A. Gassmann, D. Schoenbaechler, and B. Stiller, "WeTrace: a Privacy-preserving Tracing Approach," Journal of Communications and Networks, Vol. 1, No. 1, pp. 1–16, Oct 2021.

[85] M. Franco, B. Rodrigues, G. Parangi, and B. Stiller, "Cybersecurity Threats and Stakeholders: An Economic Analysis for Cybersecurity," CONCORDIA T4.3 Initial Report, Zürich, Switzerland, June 2019, https://files.ifi.uzh.ch/CSG/staff/franco/extern/publications/Report-on-Economics-Perspectives.pdf.

[86] M. Franco, B. Rodrigues, E. J. Scheid, A. Jacobs, C. Killer, L. Z. Granville, and B. Stiller, "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management," International Conference on Network and Service Management (CNSM 2020), Izmir, Turkey, November 2020, pp. 1–7.

[87] M. Franco, B. Rodrigues, and B. Stiller, "On the Recommendation of Protection Services," Technical Report No. 2019.06, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, August 2019.

[88] M. Franco, B. Rodrigues, and B. Stiller, "MENTOR: The Design and Evaluation of a Protection Services Recommender System," 15th International Conference on Network and Service Management (CNSM 2019). Halifax, Canada: IEEE, October 2019, pp. 1–7.

[89] M. Franco, E. Sula, B. Rodrigues, E. Scheid, and B. Stiller, "ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections," Economics of Grids, Clouds, Systems, and Services. Izola, Slovenia: Springer, September 2020.

[90] M. Franco, J. von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, and B. Stiller, "SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic," IEEE 46th Conference on Local Computer Networks (LCN 2021), Edmonton, Canada, October 2021, pp. 1–8.

[91] M. F. Franco, E. Scheid, L. Granville, and B. Stiller, "BRAIN: Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service," IFIP Networking (Networking 2019). Warsaw, Poland: IEEE, May 2019, pp. 1–9.

[92] M. F. Franco, E. Sula, A. Huertas, E. J. Scheid, , L. Z. Granville, and B. Stiller, "SecRiskAI: a Machine Learning-Based Approach for Cybersecurity Risk Prediction in Businesses," 24th IEEE International Conference on Business Informatics (CBI 2022). Amsterdan, Netherlands: IEEE, June 2022, pp. 1–10.

[93] M. F. Franco, F. M. Lacerda, and B. Stiller, "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," Journal of Business and Projects (Revista de Gestão e Projetos), Vol. 13, No. 3, pp. 1–25, nov 2022.

[94] Freiburg School of Management, "Swiss International Entrepreneurship Survey: Results of the Study on the Internationalization of Swiss SMEs," October 2019, https://www.heg-fr.ch/media/mgkmsc4s/sies-report-2019_en.pdf.

[95] C. J. Fung and B. McCormick, "VGuard: A Distributed Denial of Service Attack Mitigation Method using Network Function Virtualization," 11th International Conference on Network and Service Management (CNSM), Barcelona, Spain, November 2015, pp. 64–70.

[96] G. Dreo, C. Schmitt, A. van der Wess, N. Suri (Editors), "Roadmap for Education and Skills," 2021, https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf.

[97] G. Gallopeni, B. Rodrigues, M. Franco, and B. Stiller, "A Practical Analysis on Mirai Botnet Traffic," IFIP Networking Conference (Networking 2020), Paris, France, 2020, pp. 667–668.

[98] K. A. Garcia, R. Monroy, L. A. Trejo, C. Mex-Perera, and E. Aguirre, "Analyzing Log Files for Postmortem Intrusion Detection," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Vol. 42, No. 6, pp. 1690–1704, November 2012.

[99] P. R. Garvey and S. H. Patel, "Analytical Frameworks to Assess the Effectiveness and Economic-Returns of Cybersecurity Investments," IEEE Military Communications Conference, Baltimore, USA, October 2014, pp. 136–145.

[100] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?" Future Internet, Vol. 10, No. 2, February 2018.

[101] GDPR.EU Horizon 2020, "Complete guide to GDPR compliance," 2021, https://gdpr.eu/.

[102] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. Popescu, "A survey of cybersecurity risk management frameworks," International Workshop Soft Computing Applications, Arad, Romania, August 2020, pp. 240–272.

[103] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," ACM Transactions on Information and System Security, Vol. 5, No. 4, p. 438–457, November 2002.

[104] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," Journal of Information Security, Vol. 6, p. 24–30, January 2015.

[105] L. A. Gordon, M. P. Loeb, and L. Zhou, "Investing in Cybersecurity: Insights from the Gordon-Loeb Model," Journal of Information Security, Vol. 7, pp. 49–59, 2016.

[106] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating Cost–Benefit Analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," Journal of Cybersecurity, Vol. 6, No. 1, March 2020.

[107] GSMA, "Mobile Telecommunications Security Landscape," March 2021, https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf.

[108] N. Gupta Gourisetti, M. Mylrea, and H. Patangia, "Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework," IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC 2019), Las Vegas, USA, 2019, pp. 0206–0213.

[109] H. Aver, "Cybersecurity Economics," September 2020, https://www.kaspersky.com/blog/it-security-economics-2020-main/37205/.

[110] H. Kang, D. Hyun Ahn, G. Min Lee, J. Do Yoo, K. Ho Park, H. Kang Kim, "IoT Network Intrusion Dataset," September 2019, https://ieee-dataport.org/open-access/iot-network-intrusion-dataset.

[111] B. S. H. Kox, "Economic Aspects of Internet Security."

[112] H. R.K. Skeoch, "Expanding the Gordon-Loeb Model to Cyber-Insurance," Computers Security, p. 102533, 2021.

[113] U. Habiba and E. Hossain, "Auction Mechanisms for Virtualization in 5G Cellular Networks: Basics, Trends, and Open Challenges," IEEE Communications Surveys Tutorials, Vol. 20, No. 3, pp. 2264–2293, March 2018.

[114] R. Hallman, M. Major, J. Romero-Mariona., R. Phipps, E. Romero, and J. Miguel, "Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration," 5th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2020), Prague, Malta, May 2020, pp. 43–52.

[115] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," IEEE Communications Magazine, Vol. 53, No. 2, pp. 90–97, February 2015.

[116] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, H. Xue, M. Jonker, J. Ruiter, A. Sperotto, R. Rijswijk-Deij, G. Moura, A. Pras, and C. Laat, "A Responsible Internet to Increase Trust in the Digital World," Journal of Network and Systems Management, Vol. 28, pp. 882–922, October 2020.

[117] A. Hofmann, "Security Analysis of the Blockchain Agnostic Framework Prototype," Communication Systems Group, Department of Informatics, Zürich, Switzerland, December 2019, Independent Study, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[118] Y. Huang, J. Debnath, M. Iorga, A. Kumar, and B. Xie, "CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management," IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON 2019), New York, USA, October 2019, pp. 0697–0707.

[119] A. Huertas, J. Bauer, M. Demirci, J. Leupp, M. F. Franco, P. Sánchez, G. Bovet, G. M. Perez, and B. Stiller, "RITUAL: A Platform Quantifying the Trustworthiness of Supervised Machine Learning," 18th International Conference on Network and Service Management (CNSM) - Demo Papers. Thessaloniki, Greece: IEEE, September 2022, pp. 1–3.

[120] P. Huff, K. McClanahan, T. Le, and Q. Li, "A Recommender System for Tracking Vulnerabilities," 16th International Conference on Availability, Reliability and Security (ARES 2021), Vienna, Austria, August 2021, pp. 1–7.

[121] K. Hux, "Design and Implementation of a Traffic Sinkhole for Cyberattack Analysis," Communication Systems Group, Department of Informatics, March 2022, Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[122] IBM Security, "Cost of a Data Breach Report," 2022, https://www.ibm.com/security/data-breach.

[123] C. Inan, "A Visual Tool for the Analysis of Cybersecurity Investments," Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, August 2020.

[124] J. Bernard and M. Nicholson, "Reshaping the Cybersecurity Landscape," July 2020, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

[125] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, M. Fallon, "NIST SP 800-161r1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," May 2022, https://doi.org/10.6028/NIST.SP.800-161r1.

[126] J. Kontio, "A Software Process Engineering Framework," ser. Advances in Computers, M. V. Zelkowitz, Ed. Elsevier, 1998, Vol. 46, pp. 35–108.

[127] J. Muehlhausen, "The Difference between the Business Model, Framework and Architecture," 2012, https://customerthink.com/the_difference_between_the_business_model_framework_and_architecture/.

[128] J. N. Amaral, "About Computing Science Research Methodology," 2011, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.124.702.

[129] J. R. Reeder, P. F. McQuade, S. A. Schipma, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack," GreenbergTraurig Data, Privacy Cybersecurity, Vol. 1, pp. 1–25, August 2021.

[130] J. Willemson, "Extending the Gordon and Loeb Model for Information Security Investment," International Conference on Availability, Reliability and Security (ARES 2010), Krakow, Poland, 2010, pp. 258–261.

[131] JavaPipe, "DDoS Protection With IPtables: The Ultimate Guide," January 2020, https://javapipe.com/blog/iptables-ddos-protection/.

[132] V. R. Joseph, "Optimal Ratio for Data Splitting," Statistical Analysis and Data Mining, Vol. 15, pp. 531–538, August 2022.

[133] K. Jung, "Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk," North American Actuarial Journal, Vol. 25, No. 4, pp. 580–603, June 2021.

[134] D. Jurafsky and J. H. Martin, Speech and Language Processing, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, December 2021.

[135] A. M. Kanca and S. Sagiroglu, "Sharing Cyber Threat Intelligence and Collaboration," International Conference on Information Security and Cryptology (ISCTURKEY 2021), Ankara, Turkey, December 2021, pp. 167–172.

[136] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, pp. 11–27, 1981.

[137] Kaspersky, "IT Security Economics," Report, June 2019, https://go.kaspersky.com/rs/802-IJN-240/images/GL_Kaspersky_Report-IT-Security-Economics_report_2019.pdf.

[138] M. Kreitz, "Security by Design in Software Engineering," ACM Software Engineering Notes (SIGSOFT), Vol. 44, No. 3, pp. 1–23, Nov 2019.

[139] N. Kshetri, "The Economics of Cyber-Insurance," IT Professional, Vol. 20, No. 6, pp. 9–14, December 2018.

[140] N. Kshetri, "The Evolution of Cyber-insurance Industry and Market: An Institutional Analysis," Telecommunications Policy, Vol. 44, No. 8, pp. 1–14, 2020.

[141] N. Kshetri, "The Evolution of Cyber-insurance Industry and Market: An Institutional Analysis," Telecommunications Policy, Vol. 44, No. 8, p. 102007, September 2020.

[142] V. S. Kumar and V. L. Narasimhan, "Using Deep Learning For Assessing Cybersecurity Economic Risks In Virtual Power Plants," 7th International Conference on Electrical Energy Systems (ICEES), Chennai, India, February 2021, pp. 530–537.

[143] E. Künzler, "Real Cyber Value at Risk: An Approach to Estimate Economic Impacts of Cyberattacks on Businesses," January 2023, Master Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[144] L. A. Gordon, M. P. Loeb, L. Zhou, "Information Segmentation and Investing in Cybersecurity," Journal of Information Security, Vol. 12, pp. 115–136, January 2021.

[145] J. D. Lafferty., A. McCallum, and F. C. N. Pereira, "Conditional Random Fields: Probabilistic Models for Segmenting and Labeling Sequence Data," 18th International Conference on Machine Learning (ICML), San Francisco, USA, June 2001, pp. 282–289.

[146] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," Business Horizons, Vol. 64, No. 5, pp. 659–671, October 2021.

[147] T. Li, G. Convertino, R. K. Tayi, and S. Kazerooni, "What Data Should I Protect? Recommender and Planning Support for Data Security Analysts," 24th International Conference on Intelligent User Interfaces (IUI '19), California, USA, March 2019, p. 286–297.

[148] M. F. Franco, "BRAIN - Source Code," 2019, https://gitlab.ifi.uzh.ch/franco/brain-nfv-auction.

[149] M. F. Franco, B. Rodrigues, "MENTOR Engine - Source code," 2019, https://gitlab.ifi.uzh.ch/franco/recommendersystem.

[150] M. F. Franco, F. M. Lacerda, B. Stiller, "SECProject: a Framework for the Management of Cybersecurity Projects in Small and Medium-sized Enterprises," X International Symposium on Management, Project, Innovation and Sustainability (X SINGEP), São Paulo, Brazil, October 2022, pp. 1–16.

[151] M. Franco, B. Shaqiri, "SecBot Implementation," June 2020, https://gitlab.ifi.uzh.ch/franco/secbot.

[152] M. Franco, B. Stiller (Editors), "Deliverable D4.3: 3rd Year Report on Cybersecurity Threats," December 2021, https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D4.3.pdf.

[153] M. Franco, J. von der Assen, L. Boillat, B. Stiller, "SecGrid Project," February 2019, http://www.csg.uzh.ch/csg/en/research/SecGrid.

[154] M. Richards, N. Ford, Fundamentals of Software Architecture. O'Reilly, 2020.

[155] V. S. Mai, R. J. La, and A. Battou, "Optimal Cybersecurity Investments in Large Networks Using SIS Model: Algorithm Design," IEEE/ACM Transactions on Networking, Vol. 29, No. 6, pp. 2453–2466, December 2021.

[156] V. Matejka and J. A. H. Soto, "A framework for the definition and analysis of cyber insurance requirements," Master Project, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, September 2021.

[157] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communication Review, Vol. 34, No. 2, p. 39–53, Apr. 2004.

[158] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning," 2019.

[159] T. Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options," Workshop on Deterring CyberAttacks, Washington, DC, USA, April 2010, pp. 1–21.

[160] N. Berni, F. Imami, M. F. Franco, "SaCI - Source Code," 2021, https://gitlab.ifi.uzh.ch/franco/saci.

[161] N. Berni, F. Imami, M. Franco, "SaCI - Prototype and Source-Code," 2021, https://gitlab.ifi.uzh.ch/franco/saci.

[162] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009, https://bitcoin.org/bitcoin.pdf.

[163] M. Naldi and M. Flamini, "Calibration of the Gordon-Loeb Models for the Probability of Security Breaches," 19th International Conference on Computer Modelling Simulation (UKSim), Cambridge, UK, 2017, pp. 135–140.

[164] K. Nath, S. Dhar, and S. Basishtha, "Web 1.0 to Web 3.0 - Evolution of the Web and its Various Challenges," International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, India, February 2014, pp. 86–89.

[165] National Audit Office, "Investigation: WannaCry Cyber Attack and the NHS," 2018, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[166] National Institute of Standards and Technology (NIST), "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," 2014.

[167] National Institute of Standards and Technology (NIST), "Cybersecurity Framework Version 1.1," 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[168] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[169] National Institute of Standards and Technology (NIST), "Understanding the NIST Cybersecurity Framework," 2018, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework.

[170] National Institute of Standards and Technology (NIST), "Cybersecurity Spending: An analysis of Investment Dynamics within the EU," 2020, nIST Special Publication 800-53. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[171] Z. Neeman, "The Effectiveness of English Auctions," Games and Economic Behavior, Vol. 43, No. 2, pp. 214–238, May 2003.

[172] Network and Information Systems (NIS) Cooperation Group, "EU Coordinated Risk Assessment of 5G Networks Security," October 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

[173] C. Omlin, "A Gordon-Loeb-based Visual Tool for Cybersecurity Investments," Communication Systems Group, Department of Informatics, January 2022, Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[174] C. Omlin and O. Kamer, "SECAdvisor 2.0: Visualizations and Extensions for Cybersecurity Economics Analysis," Communication Systems Group, Department of Informatics, Master Project, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, January 2023.

[175] OWASP Foundation, "Open Web Application Security Project (OWASP)," 2001, https://owasp.org/.

[176] B. Y. Ozkan and M. Spruit, "Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda," International Journal of Standardization Research, Vol. 17, pp. 102–143, December 2019.

[177] S. Padovan, M. Nadig, and C. Birchler, "DDoSGrid 3.0: Enabling the Real-time Processing and Analysis of Cyber Attacks Traffic," Master Project, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, February 2022.

[178] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will Cyber-Insurance Improve Network Security? A Market Analysis," IEEE Conference on Computer Communications (INFOCOM 2014), Toronto, Canada, May 2014, pp. 235–243.

[179] S. M. Pappalardo, M. Niemiec, M. Bozhilova, N. Stoianov, A. Dziech, and B. Stiller, "Multi-Sector Assessment Framework - A New Approach to Analyse Cybersecurity Challenges and Opportunities," Multimedia Communications, Services, and Security. Krakow, Poland: Springer, Lecture Notes in Computer Science (LNCS), 2020, pp. 1–15.

[180] R. M. Parizi and A. Dehghantanha, "Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security," International Conference on Blockchain (ICBC 2018). Seattle, USA: Springer, June 2018, pp. 75–91.

[181] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails," Security and Privacy Protection in Information Processing Systems. Berlin, Heidelberg: Springer, 2013, pp. 366–378.

[182] Ponemon Institute, IBM Security, "Cyber Resilient Organization Report," July 2020, https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/.

[183] C. Pop, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Blockchain based Decentralized Applications: Technology Review and Development Guidelines," CoRR, Vol. abs/2003.07131, March 2020. [Online]. Available: https://arxiv.org/abs/2003.07131

[184] S. S. Portal, "Figures on SMEs: Companies and Jobs," 2021, https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/facts-and-figures/figures-smes/companies-and-jobs.html.

[185] Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th ed. PMI, 2021.

[186] PwC Germany, "IT Governance Framework," 2021, https://www.pwc.de/en/strategy-organisation-processes-systems/it-governance-framework.html.

[187] R. Bojanc, B. Jerman-Blažič, "An economic modelling approach to information security risk management," International Journal of Information Management, Vol. 28, No. 5, pp. 413–422, 2008.

[188] R. Mccrimmon and M. Matishak, "Cyberattack on Food Supply Followed Years of Warnings," May 2021, https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936.

[189] R. Poortinga, J. Ceron, J. Santanna, C. Hesselman, "European DDoS Clearing House Pilot," May 2019, https://github.com/orgs/ddos-clearing-house.

[190] R. S. Aguilar-Saven, "Business Process Modelling: Review and Framework," International Journal of Production Economics, Vol. 90, No. 2, pp. 129–149, 2004, production Planning and Control.

[191] A. M. Rahman, A. A. Mamun, and A. Islam, "Programming Challenges of Chatbot: Current and Future Prospective," IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, December 2017, pp. 75–78.

[192] A. Rajeevan, "Tokens, Gas and Gas limit in Ethereum," February 2019, https://arunrajeevan.medium.com/tokens-gas-and-gas-limit-in-ethereum-f07790f56d8f.

[193] Rasa Technologies, "Rasa: Open Source Conversational AI," December 2016, https://rasa.com/.

[194] P. Rathod and T. Hämäläinen, "A Novel Model for Cybersecurity Economics and Analysis," IEEE International Conference on Computer and Information Technology (CIT 2017), Helsinki, Finland, August 2017, pp. 274–279.

[195] M. Rea-Guaman, J. A. Calvo-Manzano, and T. S. Feliu, "A Prototype to Manage Cybersecurity in Small Companies," 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, June 2018, pp. 1–6.

[196] L. Ren and P. A. S. Ward, "Pooled Mining is Driving Blockchains Toward Centralized Systems," International Symposium on Reliable Distributed Systems Workshops (SRDSW 2019), Lyon, France, October 2019, pp. 43–48.

[197] B. Rodrigues, M. Franco, G. Paranghi, and B. Stiller, "SEConomy: A Framework for the Economic Assessment of Cybersecurity," 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019). Leeds, UK: Springer, September 2019, pp. 1–9.

[198] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. USA: Pearson, June 2021.

[199] S. Morgan, "2020 Official Annual Cybercrime Report," Herjavec Group, 2019, https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

[200] S. Morgan, "Cybercrime to Cost The World $10.5 Trillion Annually By 2025," 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

[201] S. Widup, A. Pinto, D. Hylender, G. Bassett, "2021 Verizon Data Breach Investigations Report," May 2021, Technical Report, https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report.

[202] Safeatlast, "Ransomware Statistics for Cybersecurity," January 2022, https://safeatlast.co/blog/ransomware-statistics/.

[203] P. M. Sanchez, J. M. J. Valero, A. H. Celdran, G. Bovet, M. G. Perez, and G. M. Perez, "A Survey on Device Behavior Fingerprinting: Data Sources, Techniques, Application Scenarios, and Datasets," IEEE Communications Surveys Tutorials, Vol. 23, No. 2, pp. 1048–1077, 2021.

[204] E. J. Scheid, M. Keller, M. Franco, and B. Stiller, "BUNKER: a Blockchain-based trUsted VNF pacKagE Repository," 16th Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019). Leeds, UK: Springer, September 2019, pp. 1–9.

[205] E. J. Scheid, B. Rodrigues, C. Killer, M. Franco, S. R. Niya, and B. Stiller, Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues, ser. IFIP AICT Festschrifts. Cham, Switzerland: Springer, Aug 2021, No. 1, pp. 1–29.

[206] E. J. Scheid, P. Widmer, B. Rodrigues, M. Franco, and B. Stiller, "A Controlled Natural Language to Support Intent-based Blockchain Selection," IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020). Toronto, Canada: IEEE, May 2020, pp. 1–9.

[207] E. J. Scheid, R. Hy, M. F. Franco, C. Killer, and B. Stiller, "On the Employment of Machine Learning in the Blockchain Selection Process," IEEE Transactions on Network and Service Management, Vol. 1, No. 1, pp. 1–12, December 2022.

[208] N. Sfondrini, G. Motta, and A. Longo, "Public Cloud Adoption in Multinational Companies: A Survey," IEEE International Conference on Services Computing (SCC 2018), 2018, pp. 177–184.

[209] K. Shah, A. Salunke, S. Dongare, and K. Antala, "Recommender Systems: An Overview of Different Approaches to Recommendations," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS 2017), Coimbatore, India, March 2017, pp. 1–4.

[210] B. Shaqiri, "Development and Refinement of a Chatbot for Cybersecurity Support," Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, February 2021.

[211] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," IEEE Access, Vol. 8, pp. 222 310–222 354, December 2020.

[212] I. M. Sholihah, H. Setiawan, and P. G. Nabila, "Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform," Sixth International Conference on Informatics and Computing (ICIC 2021), Jakarta, Indonesia, November 2021, pp. 1–6.

[213] A. Shostack, "Experiences Threat Modeling at Microsoft," 2008, https://adam.shostack.org/modseco8/Shostack-ModSeco8-Experiences-Threat-Modeling-At-Microsoft.pdf.

[214] A. Spain, "Cyber Risk Calculator (CERCA)," 2022, https://booklet.atosresearch.eu/assets/cerca.

[215] D. Stalder, "Machine-learning based Detection of Malicious DNS-over-HTTPS (DoH) Traffic Based on Packet Captures," Communication Systems Group, Department of Informatics, April 2022, Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[216] B. Stiller, M. Franco, C. Killer, S. R. Niya, B. Rodrigues, E. J. Scheid, R. Ribeiro, and E. Schiller (Editors), "Internet Economics Report XIV," Technical Report No. 2021.01, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, June 2021.

[217] A. Strielkina, O. Illiashenko, M. Zhydenko, and D. Uzun, "Cybersecurity of Healthcare IoT-based systems: Regulation and Case-Oriented Assessment," IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, UKraine, 2018, pp. 67–73.

[218] E. Sula, "ProtecDDoS: A Recommender System for Distributed Denial-of-Service Protection Services," Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, August 2019.

[219] E. Sula, "A Machine Learning-based Tool for Cybersecurity Risk Assessment," August 2021, Master Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[220] N. Szabo, "Formalizing and Securing Relationships on Public Networks," First Monday, Vol. 2, No. 9, September 1997.

[221] R. Tatman, "Rasa Reading Group: SecBot: Business-Driven Conversational Agent for Cybersecurity," March 2021, https://youtu.be/GbbI33aVZ20.

[222] S. Teufel, B. Teufel, M. Aldabbas, and M. Nguyen, "Cyber security canvas for smes," International Information Security Conference (ISSA 2020). Pretoria, South Africa: Springer, 2020, pp. 20–33.

[223] The AFCEA Cyber Committee, "The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment," 2013, https://www.afcea.org/committees/cyber/documents/cybereconfinal.pdf.

[224] The MITRE Corporation, "MITRE ATT&CK," 2015, https://attack.mitre.org/.

[225] C. Thyagarajan, S.Suresh, N. Sathish, and S. Suthir, "A Typical Analysis And Survey On Healthcare Cyber Security," International Journal of Scientific Technology Research, Vol. 9, No. 3, p. 1–5, March 2020.

[226] Tools Hero, "Business Framework," 2021, https://www.toolshero.com/tag/business-framework/.

[227] M. Tornow, "Design and implementation of a system to request, process and store information from protection services and cyberattacks," April 2020, Bachelor Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland.

[228] D. K. Tosh, S. Sengupta, S. Mukhopadhyay, C. A. Kamhoua, and K. A. Kwiat, "Game Theoretic Modeling to Enforce Security Information Sharing among Firms," IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, USA, November 2015, pp. 7–12.

[229] Z. Turk, B. G. de Soto, B. Mantha, A. Maciel, and A. Georgescu, "A Systemic Framework for Addressing Cybersecurity in Construction," Automation in Construction, Vol. 133, January 2022.

[230] M. S. U. Banerjee, A. Vashishtha, "Evaluation of the Capabilities of Wireshark as a Tool for Intrusion Detection," IEEE Transactions on Network and Service Management, Vol. 6, No. 7, pp. 1–5, September 2010.

[231] US Health Care Industry Cybersecurity Task Force, "Report On Improving Cybersecurity in the Health Care Industry," June 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[232] A. Vardalaki and V. Vlachos, "Emerging Malware Threats: The Case of Ransomware," Cybersecurity Issues in Emerging Technologies. Calgary, Alberta, Canada: CRC Press, 2021, pp. 1–18.

[233] Verizon, "2021 Data Breach Investigations Report," February 2021, https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf.

[234] B. Vignau, R. Khoury, S. Hallé, and A. Hamou-Lhadj, "ISO 27001 Risk Management and Compliance," Journal of Risk Management, Vol. 54, No. 1, pp. 1–24, 2021.

[235] B. Vignau, R. Khoury, S. Hallé, and A. Hamou-Lhadj, "The Evolution of IoT Malwares, from 2008 to 2019: Survey, Taxonomy, Process Simulator and Perspectives," Journal of Systems Architecture, Vol. 116, p. 102143, 2021.

[236] V. Vlasov, A. Drissner-Schmid, and A. Nichol, "Few-Shot Generalization Across Dialogue Tasks," November 2018, https://arxiv.org/abs/1811.11707.

[237] V. Vlasov, J. E. M. Mosig, and A. Nichol, "Dialogue Transformers," May 2020, https://arxiv.org/abs/1910.00486.

[238] J. von der Assen, M. F. Franco, C. Killer, E. J. Scheid, and B. Stiller, "CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling," IEEE International Conference on Cyber Security and Resilience (CSR 2022), Rhodes, Greece, July 2022, pp. 1–8.

[239] W. Sonnenreich, J. Albanese, B. Stout, "Return On Security Investment (ROSI): A Practical Quantitative Model," Journal of Research and Practice in Information Technology, pp. 239–252, 2005.

[240] S. M. Wagner and A. P. Schwab, "Setting the Stage for Successful Electronic Reverse Auctions," Journal of Purchasing and Supply Management, Vol. 10, No. 1, pp. 11–26, January 2004.

[241] J. Wargin, "Insurance Company Technology Trends Transforming the Industry in 2021," January 2021, https://www.duckcreek.com/blog/insurance-technology-trends/.

[242] Web3 Foundation, "Web 3.0 Technology Stack," May 2022, https://web3.foundation/about/.

[243] J. Webb and D. Hume, "Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, UK, March 2018, pp. 1–7.

[244] G. Wood, "Ethereum: a Secure Decentralised Generalised Transaction Ledger - Berlin Version 7251f10," 2020, https://ethereum.github.io/yellowpaper/paper.pdf.

[245] K. Wuyts, R. Scandariato, W. Joosen, M. Deng, and B. Preneel, "LINDDUN: A Privacy Threat Analysis Framework," 2019, https://www.linddun.org/.

[246] W. Xiong and R. Lagerström, "Threat Modeling–A Systematic Literature Review," Computers & Security, Vol. 84, pp. 53–69, 2019.

[247] Y. Baryshnikov, "IT Security Investment and Gordon-Loeb's 1/e rule," Berlin, Germany, June 2007, https://econinfosec.org/archive/weis2012/papers/Baryshnikov_WEIS2012.pdf.

[248] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafqat, "Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations," Future Generation Computer Systems, Vol. 95, pp. 754–763, 2019.

[249] YCharts, "Ethereum Average Gas Price," May 2022, https://ycharts.com/indicators/ethereum_average_gas_price.

[250] J. A. Zachman, "A Framework for Information Systems Architecture," IBM Systems Journal, Vol. 26, No. 3, pp. 276–292, 1987.

[251] M. E. Zadeh Nojoo Kambar, A. Esmaeilzadeh, and M. Heidari, "A Survey on Deep Learning Techniques for Joint Named Entities and Relation Extraction," IEEE World AI IoT Congress (AIIoT 2022), Seattle, USA, June 2022, pp. 218–224.

All links provided above were last accessed on August 12, 2022.

A Publications

This PhD thesis resulted in several scientific works published in selected venues. These works were all directly or indirectly related to the topic of this thesis. Further, master's and bachelor's theses were supervised and developed in the cybersecurity and network management context, whose individual outcomes in terms of proposed solutions and evaluations contributed toward the overall *CyberTEA* approach and results.

A.1 Contribution of Own Publications Within Chapters

The PhD thesis objectives outlined at the macro level are typically decomposed into several specific goals achieved by publications across the thesis period. Thus, it is relevant to highlight where those publications appear as core or additional elements in each chapter of this PhD thesis. Also, several students' thesis (*i.e.*, Master Thesis (MSc), Master Project (MAP), and Bachelor Thesis (BSc)) contributed to this PhD thesis by implementing solutions motivated, designed, and supervised by the author of this PhD thesis. Table A.1 lists own contributions in the PhD thesis' chapters.

A.2 List of Publications

This section lists publications made by the author during the PhD thesis period. In addition to the previously cited publications that contributed directly to the thesis, the author's research and collaboration within the Communication Systems Group (CSG) resulted in several publications from 2019 to 2022. All of these publications are related to cybersecurity or computer networks.

Table A.1: List of Publications per Chapter

Chapter	Related Publications				Student Thesis		
	Full Paper	Short Paper	Technical Report	Book Chapter	MSc	MAP	BSc
1. Introduction	-	[83, 197]	-	-	-	-	-
2. Theoretical Foundations	-	[197]	[85, 216]	[205]	[219]	-	-
3. State-of-the-Art	-	-	-	-	-	-	-
4. *CyberTEA* Approach	[81, 86, 88–92, 150]	[82]	[87]	-	[20, 29, 33, 143, 174, 219]	[32, 76]	[44, 173, 210, 218]
5. Evaluations	[81, 86, 88, 90–92]	-	-	-	[20, 29, 33, 219]	[76]	[44, 173, 210, 218]
6. Conclusions	-	-	-	-	-	-	-

Publication Title
[20] DDoSGrid 2.0: Integrating and Providing Visualizations for the European DDoS Clearing House
[29] SC4CyberInsurance: Automated Cyber-Insurance Contracts
[33] DDoSGrid-Mining: Analyzing and Classifying DDoS Attack Traffic
[32] A Tool for Visualization and Analysis of Distributed Denial-of-Service (DDoS) Attacks
[44] Kirti: Decentralized Reputation and SLA Enforcement for Cybersecurity
[76] SHINE: a Collaborative System for Sharing Insights and Information of Economic Impacts of Cyberattacks
[85] Cybersecurity Threats, Stakeholders, and SEConomy Framework - An Economic Analysis for Cybersecurity
[83] A Business-Driven Integrated Ecosystem for Cybersecurity Planning and Management
[88] MENTOR: The Design and Evaluation of a Protection Services Recommender System
[82] DDoSGrid: a Platform for the Post-mortem Analysis and Visualization of DDoS Attacks
[90] SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic
[91] BRAIN: Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service
[92] SecRiskAI: a Machine Learning-Based Approach for Cybersecurity Risk Prediction in Businesses
[87] On the Recommendation of Protection Services
[86] SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management
[89] ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections
[81] SaCI: a Blockchain-based Cyber Insurance Approach for the Deployment and Management of a Contract Coverage
[143] Real Cyber Value at Risk: An Approach to Estimate Economic Impacts of Cyberattacks on Businesses
[150] SECProject: a Framework for the Management of Cybersecurity Projects in Small and Medium-sized Enterprises
[173] A Gordon-Loeb-based Visual Tool for Cybersecurity Investments
[174] SECAdvisor 2.0: Visualizations and Extensions for Cybersecurity Economics Analysis
[197] SEConomy: A Framework for the Economic Assessment of Cybersecurity
[205] Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues
[210] Development and Refinement of a Chatbot for Cybersecurity Support
[216] Is it All About Money? An Analysis of Company Investments in Cybersecurity
[218] A Recommender System for Distributed Denial-of-Service Protection Services
[219] A Machine Learning-based Tool for Cybersecurity Risk Assessment

A.2.1 First Author Publications

The author of this thesis led the publications listed below, thus having him as the main contributor (*i.e.*, First Author).

2022

- *[Journal]* **M F. Franco**, F. M. Lacerda, B. Stiller: A Framework for the Planning and Management of Cybersecurity Projects in Small and Medium-sized Enterprises; UNINOVE, Journal of Business and Projects (Revista de Gestão e Projetos), Vol. 13, No. 3, December 2022, pp 1–25.
- *[Full Paper]* **M. F. Franco**, F. M. Lacerda , B. Stiller: **SECProject: a Framework for the Assessment and Management of Cybersecurity Projects in Small and Medium-sized Enterprises**; X International Symposium on Management, Project, Innovation and Sustainability (X SINGEP), São Paulo, Brazil, October 2022, pp. 1–16.
- *[Full Paper]* **M. F. Franco**, E. Sula, A. Huertas, E. J. Scheid, L. Z. Granville, B. Stiller: **SecRiskAI: a Machine Learning-based Approach for Cybersecurity Risk Prediction in Businesses**; 24th IEEE International Conference on Business Informatics, Amsterdam, Netherlands, June 2022, pp. 1–10.

2021

- *[Full Paper]* **M. Franco**, J. von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, B. Stiller: **SecGrid: A Visual System for the Analysis and ML-Based Classification of Cyberattack Traffic**; IEEE 46th Conference on Local Computer Networks (LCN 2021), Virtually, Edmonton, Canada, October 2021, pp. 1–8.

- *[Full Paper]* **M. Franco**, N. Berni, E. Scheid, B. Rodrigues, C. Killer, B. Stiller: **SaCI: a Blockchain-based Cyber Insurance Approach for the Deployment and Management of a Contract Coverage**; 18th International Conference on the Economics of Grids, Clouds, Systems and Services (GECON 2021), Virtually, September 2021, pp. 1–14.

- *[Journal]* **M. Franco**, B. Rodrigues, C. Killer, E. Scheid, A. De Carli, A. Gassmann, D. Schoenbaechler, B. Stiller: **WeTrace: a Privacy-preserving Tracing Approach**; KICKS and IEEE ComSoc, Journal of Communications and Networks (JCN), Special Issue on Communications and Networking Approaches for Combatting COVID-19, October 2021, pp. 1–16.

- *[Short Paper]* **M. Franco**, J. von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. Scheid, L. Granville, B. Stiller, B. Rodrigues, B. Stiller: **DDoSGrid: a Platform for the Post-mortem Analysis and Visualization of DDoS Attacks**; IFIP Networking 2021, Virtually, Espoo, Finland, June 21-24 2021, pp. 1–3.

2020

- *[Full Paper]* **M. Franco**, B. Rodrigues, E. Scheid, A. Jacobs, C. Killer, L. Granville, B. Stiller: **SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management**; 16th International Conference on Network and Service Management (CNSM 2020), Mini-Conference, Izmir, Turkey, November 2020, pp. 1-7.

- *[Workshop Paper]* **M. Franco**, L. Granville, B. Stiller: **Towards a Conversational Agent for Cybersecurity Planning and Management**; 2nd KuVS Fachgespräch "Machine Learning and Networking", Würzburg, Germany, October 2020, pp. 1–3.

- *[Full Paper]* **M. Franco**, E. Sula, B. Rodrigues, E. Scheid, B. Stiller: **ProtectDDoS: a Platform for Trustworthy Offering and Recommendation of Protections**; International Conference on Economics of Grids, Clouds, Software and Services (GECON 2020), Izola, Slovenia, September 2020, pp. 1-12.

- *[PhD Workshop]* **M. Franco**, L. Granville, B. Stiller: **A Business-Driven Integrated Ecosystem for Cybersecurity Planning and Management**; CONCORDIA Early Stage PhD Workshop (CON-PHD), Twente, Netherlands, June 2020, pp. 1–6.

2019

- *[Full Paper]* **M. Franco**, B. Rodrigues, B. Stiller: **MENTOR: The Design and Evaluation of a Protection Services Recommender System**; 15th International Conference on Network and Service Management (CNSM 2019), Mini-Conference, Halifax, Canada, October 2019, pp. 1-7.

- *[Full Paper]* **M. Franco**, M. Bucher, E. Scheid, L. Granville, B. Stiller: **GENEVIZ: A Visual Tool for Construction and Blockchain-based Validation of SFC**; 16th International Conference on Economics of Grids, Clouds, Systems, and Services (GECON 2019), Leeds, UK, September 2019, pp. 15-28.
- *[Technical Report]* **M. Franco**, B. Rodrigues, B. Stiller: **On the Recommendation of Protection Services**; Technical Report No. Ifi-2019.06, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, August 2019.
- *[Full Paper]* **M. Franco**, E. Scheid, L. Granville, B. Stiller: **BRAIN: Blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service**; IFIP Networking, Warshaw, Poland, May 2019, pp. 1-9.

A.2.2 Co-authorship Publications

Different successful collaborations were placed, having the author of this PhD thesis as one of the collaborators. All of these collaborations were related to the Network Management field and the topic of this thesis, resulting in the publications listed below.

2022

- *[Journal]* E. J. Scheid, R. Hy, **M. F. Franco**, C. Killer, B. Stiller: **On the Employment of Machine Learning in the Blockchain Selection Process**; IEEE Transactions on Network and Service Management, Vol. 1, No. 1, December 2022, pp. 1–12.
- *[Full Paper]* E. J. Scheid, **M. F. Franco**, F. Kuffer, N. Kubler, P. Kiechl, B. Stiller: **VeNiCE: Enabling Automatic VNF Management based on Smart Contract Events**; 47th IEEE Conference on Local Computer Networks (LCN 2022), Edmonton, Canada, September 2022, pp. 1–8.
- *[Demo]* A. Huertas, J. Bauer, M. Demirci, J. Leupp, **M. F. Franco**, P. Sánchez, G. Bovet, G. M. Perez, B. Stiller: **RITUAL: A Platform Quantifying the Trustworthiness of Supervised Machine Learning**; 18th International Conference on Network and Service Management (CNSM 2022), Thessaloniki, Greece, September 2022, pp. 1–3.
- *[Full Paper]* J. von der Assen, **M. F. Franco**, C. Killer, E. J. Scheid, B. Stiller: **CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling**; IEEE International Conference on Cyber Security and Resilience, Rhodes, Greece, July 2022, pp. 1–8.
- *[Book Chapter]* B. Rodrigues, M. Franco, C. Killer, E. J. Scheid, B. Stiller: **On Trust, Blockchain, and Reputation Systems**; Handbook on Blockchain, Series on Optimization and Its Applications, Springer, Cham, Switzerland, No. 194, 2022, ISBN 978-3-031-07534-6, pp. 299–337.
- *[Journal]* C. Killer, B. Rodrigues, E. J. Scheid, **M. F. Franco**, B. Stiller: **Blockchain-based Voting Considered Harmful?**; IEEE Transactions on Network and Service Management (TNSM), Vol. 1, No. 1, June 2022, pp. 1–16.
- *[Technical Report]* J. von der Assen, **M. F. Franco**, C. Killer, E. J. Scheid, B. Stiller: **On Collaborative Threat Modeling**; UZH, Technical Report No. 2022.04, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, April 2022.

- *[Tutorial]* A. Huertas, P. Sánchez, **M. Franco**, G. Bovet, G. Martínez, B. Stiller: **Theoretical and Practical Intelligent Behavioral Fingerprinting**; IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), Budapest, Hungary, April 2022.

2021

- *[Tutorial]* A. Huertas, P. M. Sánchez, **M. Franco**, G. Bovet, G. Martínez, B. Stiller: **Intelligent Behavioral Fingerprinting – From Theory to Practice**; 17th International Conference on Network and Service Management (CNSM 2021), Izmir, Turkey, October 2021.
- *[Full Paper]* E. J. Scheid, P. Kiechl, **M. Franco**, B. Rodrigues, C. Killer, B. Stiller: **Security and Standardization of a Notary-based Blockchain Interoperability API**; 3rd International Conference on Blockchain Computing and Applications (BCCA 2021), Tartu, Estonia, November 2021, pp. 1–7.
- *[Demo]* J. von der Assen, **M. Franco**, B. Rodrigues, B. Stiller: **Analysis and Classification of Cyberattack Traffic Using the SecGrid Platform**; IEEE 46th Conference on Local Computer Networks (LCN) - Demo Session, Edmond, Canada, October 2021, pp. 1–3.
- *[Short Paper]* L. Mueller, B. Rodrigues, E. Scheid, **M. Franco**, C. Killer, B. Stiller: **LaFlector: A Privacy-Preserving LiDAR-Based Approach for Accurate Indoor Tracking**; IEEE 46th Conference on Local Computer Networks (LCN 2021), Virtually, Edmonton, Canada, October 2021, pp. 1–4.
- *[Book Chapter]* E. Scheid, B. Rodrigues, C. Killer, **M. Franco**, S. Rafati, B. Stiller: **Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues**; Advancing Research in Information and Communication Technology, Springer, Cham, Switzerland, No. 1, August 2021, ISBN 978-3-030-81701-5, pp. 1–29.
- *[Short Paper]* R. Ribeiro, B. Rodrigues, C. Killer, L. Baumann, **M. Franco**, E. Scheid, B. Stiller: **ASIMOV: A Fully Passive WiFi Device Tracking**; IFIP Networking 2021, Virtually, Espoo, Finland, June 2021, pp. 1–3.
- *[Full Paper]* E. Scheid, A. Knecht, T. Strasser, C. Killer, **M. Franco**, B. Rodrigues, B. Stiller: **Edge2BC: a Practical Approach for Edge-to-Blockchain IoT Transactions**; IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021), Virtually, Darlinghurst, Australia, May 2021, pp. 1–9.
- *[Full Paper]* C. Killer, M. Knecht, C. Müller, B. Rodrigues, E. Scheid, **M. Franco**, B. Stiller: **Æternum: A Decentralized Voting System with Unconditional Privacy**; IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021), Virtually, Darlinghurst, Australia, May 2021, pp. 1–8.
- *[Tutorial]* C. Killer, B. Rodrigues, E. J. Scheid, **M. Franco**, B. Stiller: **Blockchain-based Remote Electronic Voting from Theory to Practice**; IFIP/IEEE International Symposium on Integrated Network Management (IM 2021), Bordeaux, France, May 2021.
- *[Full Paper]* B. Rodrigues, C. Halter, **M. Franco**, E. J. Scheid, C. Killer, B. Stiller: **BluePIL: a Bluetooth-based Passive Indoor Localization Method**; IFIP/IEEE International Symposium on Integrated Network Management (IM 2021), Bordeaux, France, May 2021, pp. 1–9.

2020

- *[Full Paper]* C. Killer, B. Rodrigues, E. J. Scheid, **M. Franco**, M. Eck, N. Zaugg, A. Schetlin, B. Stiller: Provotum: **A Blockchain-Based and End-to-End Verifiable Remote Electronic Voting System**; IEEE 45th Conference on Local Computer Networks (LCN 2020), Sidney, Australia, November 2020, pp. 1-12.
- *[Journal]* B. Rodrigues, E. Scheid, C. Killer, **M. Franco**, B. Stiller: **Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks**; Journal of Network and Systems Management, Springer Nature, August, 2020, pp. 1-37.
- *[Technical Report]* C. Killer, L. Thorbecke, B. Rodrigues, E. J. Scheid, **M. Franco**, B. Stiller: **Proverum: A Hybrid Public Verifiability for Decentralized Identity Management**; Technical Report No. 2020.03, Department of Informatics IfI, Universität Zürich UZH, Zürich, Switzerland, August 2020.
- *[Demo]* G. Gallopeni, B. Rodrigues, **M. Franco**, B. Stiller: **A Practical Analysis on Mirai Botnet Traffic**; IFIP Networking 2020, Paris, France, June 2020, pp. 1-3.
- *[Tutorial]* C. Killer, B. Rodrigues, E. Scheid, **M. Franco**, B. Stiller: **Practical Introduction to Blockchain-based Remote Electronic Voting**; IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), May 2020, Toronto, Canada.
- *[Full Paper]* E. J. Scheid, P. Widmer, B. Rodrigues, **M. Franco**, B. Stiller: **A Controlled Natural Language to Support Intent-based Blockchain Selection**; IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), May 2020, Toronto, Canada, pp. 1-9.
- *[Book Chapter]* B. Rodrigues, **M. Franco**, E. Scheid, Salil S. Kanhere, B. Stiller. **A Technology-driven Overview on Blockchain-based Academic Certificate Handling**, Blockchain Technology Applications in Education, IGI Global, November 2019, ISBN 9781522594789, pp. 197-223.
- *[Journal]* V. Garcia, G. Venacio, E. P. Duarte, T. Tavares, L. Marcuzzo, C. dos Santos, **M. Franco**, L. Bondan, L. Granville, A. Schaeffer-Filho, F. De Turck: **On the Design and Development of Emulation Platforms for NFV-based Infrastructures**; International Journal of Grid and Utility Computing, Vol. 11, No. 2, February 2020, pp. 230.

2019

- *[Full Paper]* B. Rodrigues, **M. Franco**, G. Parangi, B. Stiller: **SEConomy: A Framework for the Economic Assessment of Cybersecurity**; 16th International Conference on Economics of Grids, Clouds, Systems, and Services (GECON 2019), Leeds, UK, September 2019, pp. 154-166.
- *[Short Paper]* E. Scheid, M. Keller, **M. Franco**, B. Stiller: **BUNKER: a Blockchain-based trUsted VNF packagE Repository**; 16th International Conference on Economics of Grids, Clouds, Systems, and Services (GECON 2019), Leeds, UK, September 2019, pp. 188-196.
- *[Journal]* R. Pfitscher, A. Jacobs, L. Zembruzki, R. dos Santos, E. Scheid, **M. Franco**, A. Schaeffer-Filho, L. Granville: Guiltiness: **A Practical Approach for Quantifying Virtual Network Functions Performance**; Computer Networks (COMNET), June 2019, pp. 14-31.

- *[Journal]* G. Venancio, V. Garcia, L. Marcuzzo, T. Tavares, **M. Franco**, L. Bondan, A. Schaeffer-Filho, C. Raniery, L. Granville, E. Procopio: **Beyond VNFM: Filling the Gaps of the ETSI VNF Manager to Fully Support VNF Lifecycle Operations**; International Journal of Network Management (IJNM), April 2019, pp. 1-16.
- *[Journal]* L. Bondan, **M. F. Franco**, L. Marcuzzo, G. Venancio, R. L. Santos, R. J. Pfitscher, E. J. Scheid, B. Stiller, F. De Turck, E. P. Duarte, A. E. Schaeffer-Filho, C. R. P. Santos, and L. Z. Granville:;**FENDE: Marketplace-Based Distribution, Execution, and Life Cycle Management of VNFs**; IEEE Communications Magazine, Vol. 57, No. 1, January 2019, pp. 1389-1406.

B

Cyber Insurance Market and Its Stakeholders

An in-depth literature review and investigation of the cyber insurance market was conducted to understand the main stakeholders and the steps required to consider, when designing cyber insurance models and underwriting contracts. Interviewees with cyber insurance underwriters working in Switzerland were conducted to validate the main steps mapped. These steps were critical in order to understand better the field and its importance to map within the *CyberTEA* approach. Figure B.1 shows the steps and elements of the cyber insurance market, while Figure B.2 shows its main stakeholders and interactions. These artifacts are part of the work conducted in [156] under the supervision of the author of this PhD thesis.

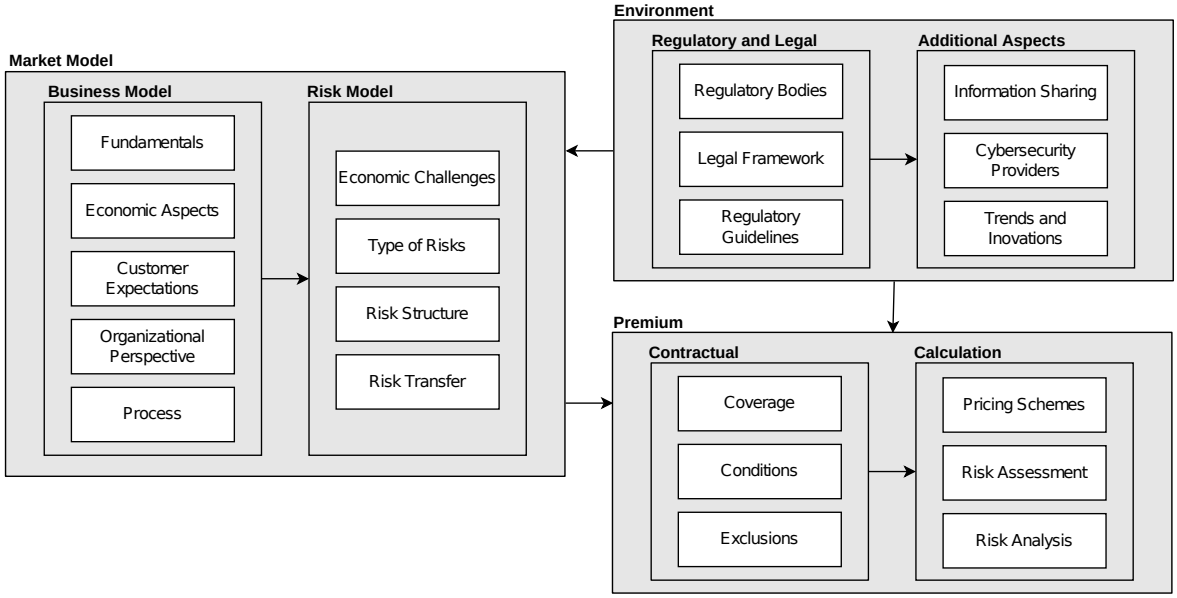


Figure B.1: Main Steps and Elements of the Cyber Insurance Market, based on [156]

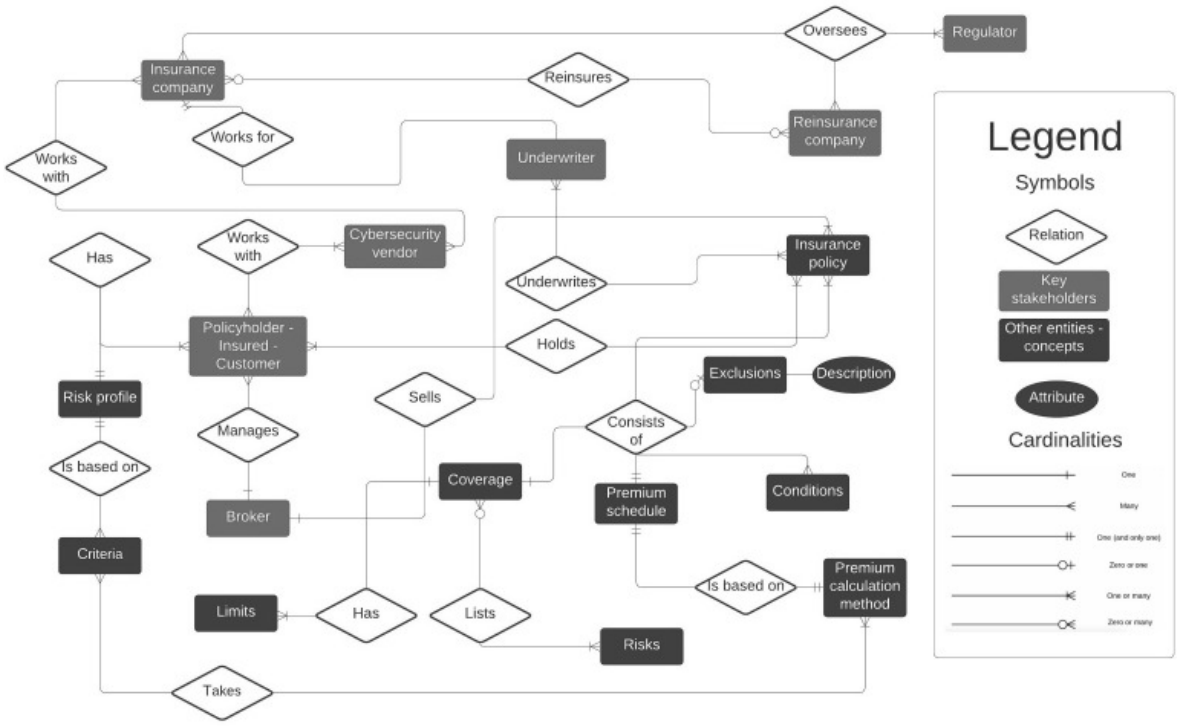


Figure B.2: Relationship of the Stakeholders of the Cyber Insurance Market [156]

C

Example of the Bank Sector Stakeholders

Figure C.1 shows the possible stakeholders that are involved in the Financial cyber security domain and the interaction among them. The actors are categorized into four main categories: exploiters, victims, security providers, and regulators. Note that the stakeholders identified and listed below are not exhaustive but provide an overview of what to expect for the financial and other sectors.

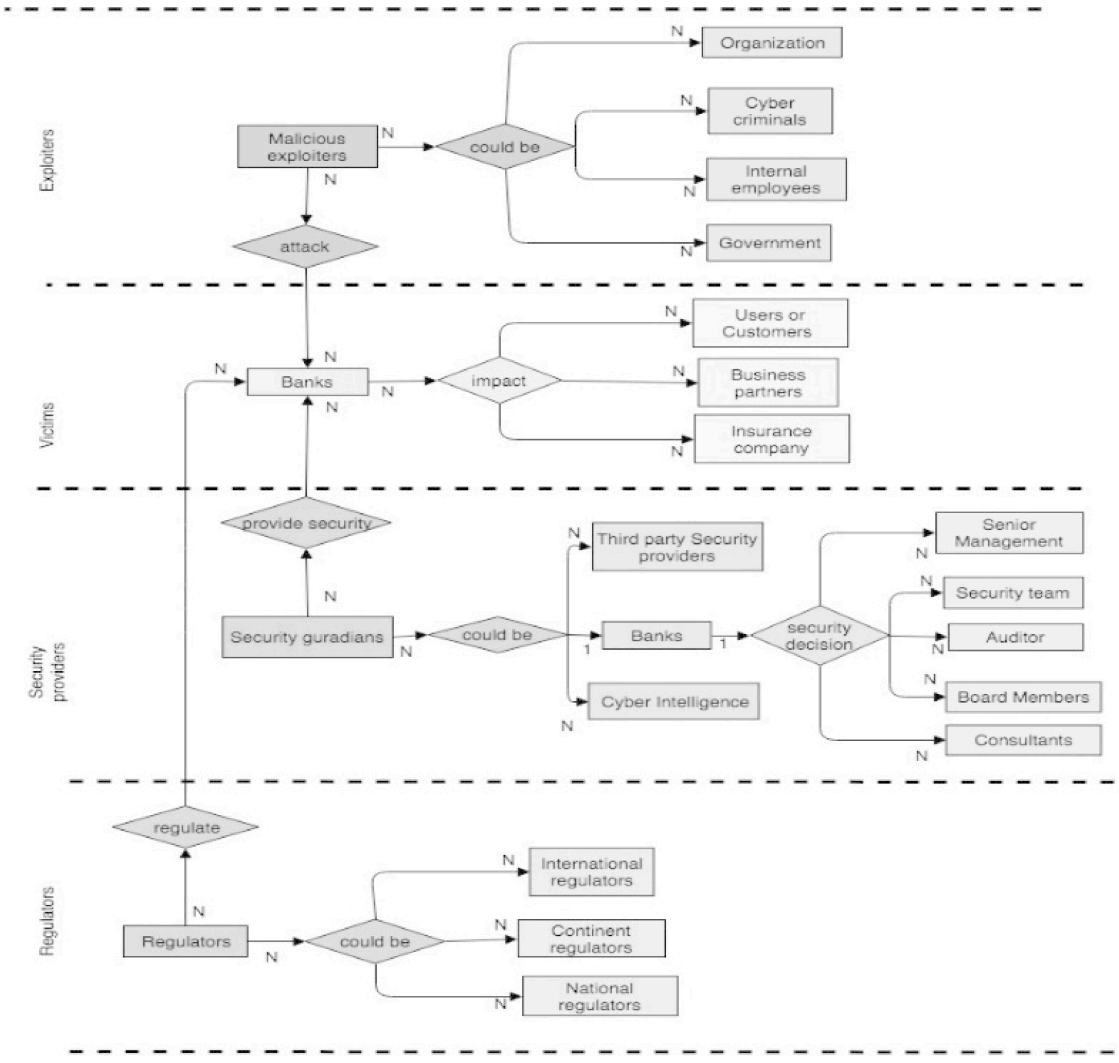


Figure C.1: Example of Relationship of the Stakeholders of the Bank Sector [85]

D

Usability Questionnaire of SecGrid's Evaluation

This appendix describes the different tasks and questions that SecGrid's usability evaluation participants had to answer. This evaluation was conducted in work developed in [20] under the supervision of the author of this PhD thesis. The experiment was conducted as follows. Using a predefined dataset, the participants had to solve the following tasks:

T1 **How many packets were present in the attack?**
This requires the user to look at the metrics displayed outside of the visualizations. The answer can be found on both the *datasets* and *dashboard* page. The correct answer is 1640892.

T2 **How many hosts participated in the attack?**
This information can be derived from the total number of source IP addresses metric. The correct answer is 2678.

T3 **From which country were most packets sent, considering only the 100 hosts that sent the most packets?**
This investigates whether the user can derive information on a DDoS attack on the network layer. The user must look at the "Top 100 sources by traffic" visualization, where a world map is used to plot the countries. The correct answer is China.

T4 **Which destination port received the largest number of segments?**
This requires the user to look at the "Traffic by ports (top 20)" visualization. In addition to that, it was assessed whether the user could derive information from the transport layer. The correct answer is port 80.

T5 **There were only packets directed to ports in the well-known port range (1 to 1024), correct?**
This requires that the Scatterplot chart is correctly interpreted. This interpretation is supported by that visualization's optional, interactive logarithmic scaling. Alternatively, this answer can also be inferred

from simply looking at the metric that defines the number of targeted destination ports. Since this number is larger than 1024, the correct answer is "No".

T6 **Which of the following attack vectors describes the attack in dataset "Dataset 1" best?**

(a) UDP-Flooding
(b) ARP-Flooding
(c) ICMP-Flooding
(d) XML-RPC Code Injection
(e) SYN-Flooding
(f) HTTP-Flooding

This question requires the user to use and combine all the previous clues to detect the pattern that indicates the attack type. Only " SYN-Flooding " is correct among the six presented DDoS attack types.

After these initial six tasks and questions, the participants were instructed to clear the current dashboard, open a new dataset and navigate back to the dashboard page. With this new dataset, the participant had to solve the following tasks:

T7 **Regarding the HTTP traffic in this dataset, do you consider this traffic as being part of the attack?** With this, two different elements were verified. First, whether the user understands the visual clues might indicate that a piece of data is just noise. Additionally, it was possible to see whether the user can derive information from the application layer. The correct answer is "no" since only 0.16% of all packets contained HTTP traffic.

T8 **Looking at the metrics, which of the following attack vectors describes the attack in dataset "Dataset 2" best?**

(a) UDP-Flooding
(b) ARP-Flooding
(c) ICMP-Flooding
(d) XML-RPC Code Injection
(e) SYN-Flooding
(f) HTTP-Flooding

This question can be answered by looking at the metrics. Since 99.58% of all packets carry ICMP messages, the user can assume that ICMP-Flooding is likely the appropriate answer.

The next part of the evaluation consisted of establishing the perceived usability of a SUS questionnaire. For that, the following ten questions were asked to each participant. The participant expressed his/her approval on a Likert scale:

S1 I think that I would like to use this system frequently.

S2 I found the system unnecessarily complex.

S3 I thought the system was easy to use.

S4 I think that I would need the support of a technical person to be able to use this system.

S5 I found the various functions in this system were well integrated.

S6 I thought there was too much inconsistency in this system.

S7 I would imagine that most people would learn to use this system very quickly.

S8 I found the system very cumbersome to use.

S9 I felt very confident using the system.

S10 I needed to learn many things before I could get going with this system.

Finally, the participant could provide any feedback. With that, suggestions and feature requests were collected to be used as possible future work for SecGrid. Additionally, this unstructured channel allowed the user to report eventual system errors.

E

Optimal Investment Calculation using GL

This appendix shows examples of calculations performed by the SECAdvisor in the background until finding the optimal investment, as demonstrated in Section 4.6. These background calculations are shown in Figure E.1, in which *v* means the vulnerability, *Li* the potential loss of the segment, *alpha* the productivity coefficient, and *z* the amount invested in cybersecurity. Then, the $S(z, v)$ is calculated according to the Equation 4.5. The expected loss is the product of $S(z, v) \times Li$. Finally, the economic benefits are calculated based on how much an investment *z* reduces the expected loss. For example, in the second row, the expected loss is US$ 84,415 with an investment of US$ 72,000. Then, in the third row, the investment is increased to US$ 1,000, becoming equal to US$ 73,000. The expected loss was reduced to US$ 83,333. Therefore, by investing US$ 1,000 more, it was possible to reduce US$ 1082, thus, resulting in an economic benefit equal to US$ 82. The amount of *z* increases until the economic benefits are not worthy anymore, which means that the amount invested *z* is higher than the reduction in the economic loss. All rows highlighted in white have an economic benefit, while the dark gray ones do not provide any economic benefit anymore. The unique row in light gray is the optimal investment, since it is the last value of *z* that provides an economic benefit.

v	Li	alpha	z	S(z, v)	Expected Loss	Benefits
0.26	5000000	0.001	70000	0.01733333	86,666.67	
0.26	5000000	0.001	72000	0.01688312	84,415.58	-251.082251
0.26	5000000	0.001	73000	0.01666667	83,333.33	-82.2510823
0.26	5000000	0.001	74000	0.0164557	82,278.48	-54.8523207
0.26	5000000	0.001	74500	0.0163522	81,761.01	-17.4747234
0.26	5000000	0.001	75600	0.01612903	80,645.16	-15.844999
0.26	5000000	0.001	75622	0.01612463	80,623.15	-15.8513192
0.26	5000000	0.001	75623	0.01612443	80,622.15	-0.00632214
0.26	5000000	0.001	75624	0.01612423	80,621.15	2.28844E-05
0.26	5000000	0.001	27000	0.040625	203,125.00	73879.845
0.26	5000000	0.001	27500	0.04	200,000.00	71254.845
0.26	5000000	0.001	28000	0.03939394	196,969.70	-5155.30303
0.26	5000000	0.001	30000	0.03714286	185,714.29	-11785.7143
0.26	5000000	0.001	40000	0.02888889	144,444.44	-40525.2525

Figure E.1: Example of Values Checked During GL Calculation by SECAdvisor until Find the Optimal Investment

Acronyms

ALE Annual Loss Expectancy

API Application Programming Interfaces

ARO Annual Rate of Occurrence

ARP Address Resolution Protocol

ASIC Application-Specific Integrated Circuits

B2B Business-to-Business

B2C Business-to-Customer

BC Blockchain

BGP Border Gateway Protocol

BL Business Layer

CEO Chief Executive Officer

CI Cyber Insurance

CIA Confidentiality, Integrity, and Availability

CISO Chief Information Security Officer

CRF Conditional Random Fields

CSA Cybersecurity Advisor

CSF Cybersecurity Framework

CSG Communication Systems Group

CSRF Cross-Site-Request-Forgery

CVSS Common Vulnerability Security System

DDoS Distributed Denial-of-Service

DIET Dual Intent and Entity Transformer

DL Decision Layer

DL Deep Learning

Domain Name System DNS

DoS Denial-of-Service

DT Decision Tree

EBIS Expected Benefit of Investment in Information Security

ECDSA Elliptic Curve Digital Signature Algorithm

ELK Elastic Stack

ENBIS Expected Net Benefit of Investment in Information Security

ENISA European Network and Information Security Agency

ETH Ether

ETSI European Telecommunications Standards Institute

EU European Union

EVM Ethereum Virtual Machine

GDPR General Data Protection Regulation

GL Gordon-Loeb

HTTP Hypertext Transfer Protocol

IaaS Infrastructure-as-a-Service

ICT Information and Communication Technology

InP Infrastructure Providers

IoT Internet-of-Things

IP Internet Protocol

IPFS InterPlanetary File System

IRR Internal Rate of Return

ISO International Organization for Standardization

IT Information Technology

ITIL Information Technology Infrastructure Library

JSON JavaScript Object Notation

K-NN K-Nearest Neighbors

KPI Key Performance Indicator

LAN Local Area Network

LTSM Long Short-Term Memory

MCC Multi-Class Classification

ML Machine Learning

MLP Multi-Layer Perceptron

MNE Multi-National Enterprises

NFV Network Functions Virtualization

NHS National Health System

NIST National Institute of Standards and Technology

NPL Natural Language Processing

NPV Net Present Value

ODM Object Data Modeling

OS Operating System

OSI Open Systems Interconnection

PCAP Packet Capture

PD Profile Descriptor

PMI Project Management Institute

RF Random Forest

RMF Risk Management Framework

RML Risk Management Layer

ROSI Return On Security Investment

RQ Research Question

SC Smart Contract

SIEM Security Information and Event Management

SL Supplementary Layer

SLA Service Level Agreement

SLE Single Loss Exposure

SME Small- and Medium-sized Enterprise

SoC System on a Chip

SP Security Provider

SQL Structured Query Language

SSL Secure Sockets Layers

SuL Supervised Learning

SUS System Usability Scale

SVM Support Vector Machine

TCP Transmission Control Protocol

UDP User Datagram Protocol

US United States

US$ United States Dollar

VNF Virtual Network Function

VNFaaS VNF-as-a-Service

WAF Web Application Firewall

XSS Cross-Site Scripting

Glossary

Approach A set of methodologies, frameworks, and solutions that are used together to achieve a commom objective.

Blockchain A decentralized append-only immutable ledger with read and write access open to any interested party.

Budget The total sum of money allocated for the particular purpose of a project for a specific period of time (*e.g.*, yearly, monthly, or during the project duration).

Business-to-Business This is a business model in which the transactions happens only between businesses, such as one involving a manufacturer and wholesaler, or a wholesaler and a retailer.

Business-to-Customer This is a business model in which the transactions happens between a business and the final individual consumer.

Cryptocurrency A currency in its digital representation, with a certain supply, typically exchange rates to fiat currency, and technically based on modern encryption mechanisms in combination with communication protocols and distributed systems.

Cyber Insurance It is an agreement in which an insurance company offers protection in case a cyberattack victimizes an organization (*i.e.*, insured). Different cyberattacks and potential losses can be included (or excluded) from a contract based on the coverage agreement.

Cyber Risk The risk of direct or indirect impacts (*e.g.*, financial loss, disruption or damage to the reputation of an organization) resulting from the failure of companies information technology systems due to a malicious attacker

Cyber Threat Any circumstance or event with the potential to cause of an incident that may result in a breach of information security or compromise business operations.

Cybersecurity Economics The intersection between cybersecurity and economics that investigates cyberattacks, strategies, and protections with an economic optic, thus focusing, above technical aspects, to understand, measure, and reduce the potential effects of cyberattacks in companies' financial health.

Cybersecurity Planning The activities that involves the specification of cybersecurity policies, procedures, controls, and solutions required to protect a company against cyber threats and risk.

Cybersecurity Strategy A set of high-level plans and actions about how an organization will secure its assets and minimize cybersecurity risks. This should be adaptable to the current and emerging threat landscape, thus evolving according to the business.

De Facto Standard It is a standard adopted widely by industry and its customers, even though a formal standards organization does not endorse it.

De Jure Standard It is a standard endorsed by a formal standards organization (*i.e.*, standard according to the law). This standard is ratified through official procedures and receives a stamp of approval.

Decentralization The characteristic of a system to be controlled by many stakeholders, such that no central point of control – neither physically nor logically – exists to overlook all interactions, communications, or decisions.

Decision The act of reasoning between alternatives with different outcomes and, given a set of pre-defined requirements, selecting one.

Framework A layered structure that indicates what kind of softwares can or should be built to satisfy a particular methodology.

Gas The internal pricing to run a transaction or a contract in the Ethereum BC.

Immutability A property which guarantees that the content previously persisted into a database remains unaltered and that it cannot be deleted any circumstances.

Methodology Connects a set of ideas, principles and rules in a harmonious manner to facilitate handling of situations

Micro Enterprise The smaller type of SME, which employs from 1 to 9 people.

Security Providers Companies that offers cybersecurity solution as products for their customers.

Small- and Medium-sized Enterprise Any commercial enterprise, regardless of its legal structure and activity,that employs fewer than 250 people.

Smart Contract A computerized transaction protocol that executes the terms of a contract agreed between the parties involved.

Solution A set of pieces of code, interfaces, and APIs developed with specific features to satisfy different components mapped in the proposed framework.

List of Algorithms

List of Figures

List of Listings

List of Tables

Curriculum Vitae

Personal Details

Name	Muriel Figueredo Franco
Date of Birth	January 9, 1991
Place of Birth	Pelotas, Rio Grande do Sul (RS), Brazil

Education

September 18 – February 23	Doctoral Program at the University of Zurich UZH Department of Informatics (IfI), Communication Systems Group (CSG)
April 20 – December 21	Master of Business Administration (MBA), Project Management Federal University of São Paulo (USP/ESALQ)
March 15 – April 17	Master of Science (MSc), Computer Science Federal University of Rio Grande do Sul (UFRGS)
March 10 – December 14	Bachelor of Science (BSc), Computer Science Federal University of Pelotas (UFPEL)

Professional Experience

September 18 – March 23	Research and Teaching Assistant at Communication Systems Group (CSG) University of Zurich UZH
May 18 – August 18	Substitute Professor at Federal Institute of Rio Grande do Sul (IFSul) Internet Systems bachelor degree
May 17 – January 20	Project Managerand Developer at GT-FENDE Brazilian Research Network (RNP)
December 17 – September 18	Full-Stack Developer Brazilian Computer Society (SBC)
March 15 – March 17	Graduate Student Researcher at Computer Networks Group Federal University of Rio Grande do Sul (UFRGS)
December 10 – December 14	Undergraduate Student Researcher at Laboratory of Comfort and Energy Efficiency Federal University of Pelotas (UFPEL)