University of Padova

Department of Mathematics "Tullio Levi-Civita"

Master Thesis in Cybersecurity

Enhancing Cybersecurity for SMEs: A Structured Framework for IT Security Assessment

Supervisor

Prof. Nicola Laurenti

University of Padova

Master Candidate

Alessandro Cusinato

Student ID

2044733

Academic Year

2023-2024

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

Abstract

The digital landscape is rapidly evolving, driven by technological advancements, global competition and government initiatives promoting digitization and Industry 4.0. This evolution has democratized access to sophisticated digital and IT tools, bringing unprecedented opportunities to small and medium-sized enterprises (SMEs). However, this technological empowerment is not without its challenges. As SMEs embrace these new capabilities, they simultaneously expose themselves to an array of cybersecurity threats. The complexity of these threats often demands costly solutions and requires personnel with specialized skills, ongoing training, and continuous education. For many SMEs, this creates a paradox: the very technological advancements that offer competitive advantages also present significant cybersecurity risks that can strain their limited resources. This paper introduces an IT security assessment framework tailored specifically for SMEs, acknowledging their unique challenges and resource constraints. The framework aims to enhance the cybersecurity posture of SMEs in a practical and cost-effective manner through the following key features: a systematic approach, to simplify the analysis and reduce the economic effort, an evaluation method, in order to allow comparison between different levels, and a categorization system, to identify and prioritize IT security risks. By providing SMEs with a structured approach to cybersecurity, this framework empowers them to make informed decisions about their security investments, balancing risk mitigation with resource allocation. This approach not only helps protect SMEs from evolving cyber threats but also enables them to leverage technological advancements confidently, fostering innovation and growth in an increasingly digital business environment.

Contents

Listing of figures

Listing of acronyms

CVE . . . . . - Common Vulnerabilities and Exposures

CVSS . . . . . - Common Vulnerability Scoring System

DKIM . . . . . - DomainKeys Identified Mail

DMARC . . . . . - Domain-based Message Authentication, Reporting, and Conformance

EDR . . . . . - Endpoint Detection and Response

EPSS . . . . . - Exploit Prediction Scoring System

FTP . . . . . - File Transfer Protocol

HTTPS . . . . . - Hypertext Transfer Protocol Secure

IAAS . . . . . - Infrastructure As A Service

ICMP . . . . . - Internet Control Message Protocol

IDS . . . . . - Intrusion Detection System

IP . . . . . - Internet Protocol

IPS . . . . . - Intrusion Prevention System

ISCSI . . . . . - Internet Small Computer Systems Interface

NetBIOS . . . . . - Network Basic Input/Output System

PAAS . . . . . - Platform As A Service

SAAS . . . . . - Software As A Service

SMB . . . . . - Server Message Block

SME . . . . . - Small and Medium-sized Enterprises

SNMP . . . . . - Simple Network Management Protocol

SPF . . . . . - Sender Policy Framework

SFTP . . . . . - SSH File Transfer Protocol

SSL . . . . . - Secure Sockets Layer

TCP . . . . . - Transmission Control Protocol

TLS . . . . . - Transport Layer Security

UDP . . . . . - User Datagram Protocol

UTM . . . . . - Unified Threat Management

VLAN . . . . . - Virtual Local Area Network

VPN . . . . . - Virtual Private Network

XDR . . . . . - Extended Detection and Response

1 Introduction

1.1 Background and Motivation

At the end of my studies, I decided to undertake an internship to find a context in which I could actively and consistently apply the concepts I had learned in my years of study. I interned at Solunet S.r.l., a technology solutions provider specializing in IT consulting and support for small and medium-sized businesses. Starting as a retailer of physical and digital IT solutions for enterprises, the company has evolved over time to become a Managed Security Service Partner (MSSP). That means a provider which offers a variety of IT services such as network management, cybersecurity, data backup and software updates. In recent years it has also complemented its monitoring activities with a parallel activity of consulting on both, operational and cybersecurity fields. This change has led to a process of specialization of technicians, who have moved from installation and configuration interventions to active monitoring processes. Cybersecurity has become part of the company's assets and it has therefore found the incentive to develop new products geared towards it. One of these services is the so-called IT Assessment. This service consists basically on evaluating the infrastructure of a company considering all possible points of interest, from hardware quality to software reliability and internal network organization. An IT assessment is a common practice when starting a collaboration with a new company, but it's also a powerful tool for a company that is planning to expand and need a solid foundation to build a new, more modern infrastructure. From the point of view of the

customer it increase awareness and from the point of view of an MSSP it means a crucial starting point to structure and propose an appropriate work plan. The idea for this thesis stems from the fact that during the months that I worked for Solunet, I practiced and studied the assessment method and noticed that there was potential for growth and improvement.
The first step to start developing this project was to analyze the critical issues of the assessment currently distributed by the company. First of all I've noticed that there was not a real structured procedure common to all practitioners and for all the targets. Each technician varied his or her approach to suit the size, existing technologies and available resources of the observed subject. Moreover different technicians had different backgrounds and specializations, so in the absence of precise guidelines they diverted the assessment to their points of interest, perhaps bypassing others. This kind of approach is quite limiting for different reasons. The lack of an all-encompassing action plan makes it difficult to standardize the intervention and thus to train new staff on this practice. At the same time the evaluations gain a certain subjectivity that makes them inconsistent, especially when comparing different companies or understanding the evolution of a company over time. It could sound as a lack of organization but it is strictly correlated with the extreme variability in the technologies and equipment adopted by the kinds of companies with Solunet has to deal with. Indeed, the Small-Medium Enterprise (SME) environment is certainly another highly critical aspect.
Dealing with SMEs means interacting with extremely disparate realities which are difficult to approach in many ways. In general the IT infrastructure was established in the early years of the company, often integrated by necessity and aiming at cost containment more than functionality. These companies often relies on low cost freelancers, or sometimes times even on simple "friends who knows", in the early stages of their development process. Then sometimes the growth from a micro to a small or medium size, forces the company to contact a specialist, which have to face a starting point that is limited, unorganized and fractionated.
Finally, even if we to leave out the difficulties in standardizing assessment and relationship with SMEs, we must still consider the difficulty of presenting understandable results. Sometimes SMEs lack the budget or the awareness necessary to include an IT team or even just an IT technician in the company's organization. These circumstances present an additional challenge for a consultant which has to present the IT assessment to the customer. It must ensure that all identified weaknesses and the remediation plan are communicated clearly and effectively. These are a calling card for future collaboration but above all they often represent a significant expense for a company. There is therefore a need to make the seriousness of the situation and the validity of the solutions proposed to an unskilled public.

To address these specific challenges, I have chosen to concentrate my efforts on developing an objective and structured framework. This framework includes an easily understandable evaluation scale for categorizing weaknesses and outlining key steps in the remediation plan. The goal is to create a simple work plan that not only facilitates theoretical understanding but can also be implemented effectively in a practical work environment, particularly within the complex context of SMEs.

1.2 Problem Statement

In order to overcome the challenges that this framework presented to me, it was necessary to divide the problem into steps[3]. After all, creating a framework from scratch is a challenge in itself, so breaking it down into sub-problems is definitely a useful strategy to direct efforts and put ideas in order[4].
The first step involves the analysis of the context I want to consider, that of small and medium-sized enterprises. That means to understand its peculiarities, both in terms of threats and needs, and figuring out how to overstep its limitations. Indeed, the size of firms is often not just a question of scale. The limitations, both in terms of personnel and resources, result in particular problems not attributable to large companies. Their size makes them a perfect target for certain types of attacks, if not an unattractive customer for the biggest player on cybersecurity tools. Much research has been done on the subject, including in cybersecurity, which seems to be a weak point of SMEs[5] [6] [7] [1] .
The second step is up to structure an efficient and noninvasive data collection system. This process needs to be scalable, adapting regardless of the business size, and well-organized for easy repeatability and for staff training [8]. The main goal is to be able to not stop or compromise the company's operations but at the same time find out all the weaknesses and vulnerabilities in the target. The framework must cover a wide area of topics, but also need to be sufficiently deep to identify small problems and vulnerabilities. This type of approach can then be extended to other types of network investigation, which may deepen the cybersecurity level or the IT awareness of personnel.
The following step is certainly the most difficult to keep objective but also the most important in the work context in which I found myself working. Given the data, a technician must propose an evaluation that is as objective and quantifiable as possible. The final perspective must be comparable to other similar situations, comparable between different steps of the remediation plan and possibly understandable by any audience, even with unskilled or only partially

informed personnel. All of this possibly made in different forms, be they numerical, graphic or whatever, in order to meet the needs despite the situation[9] [10].
Finally, this classification will need to be extended and supplemented with an evaluation system for restorative interventions. A company will need to be able to understand which interventions have priority, based both on their urgency and on the effectiveness of the individual intervention. In fact it should not be forgotten that often the real aim of an assessment is not simply awareness, but rather the subsequent improvement plan.

1.3 Thesis Structure

The structure of this work will more or less follow the steps presented in the previous paragraph. In the first part there will be a brief summary of the main concepts that have emerged from an initial bibliographical research. As expected, the needs of my company is part of a larger context of research that involved university researchers but especially the major players of companies providing computer services. The objective of this first part is to insert the thesis within a certain categorization of works but also and above all to take inspiration from research that came before mine and have led to interesting results.
After this first part will come the main body of my research, that is the creation of the theoretical framework. This will include a part on understanding the needs of SMEs and on categorising problems into thematic groups to facilitate their framing and understanding. This will be followed by a reflection on the process of data collection and analysis, which also requires an effort to weigh up the value of each thematic group within the overall assessment. The theoretical framework will also include the methodology for presenting the results and creating an objective and acceptable measurement scale.
Once the theory is framed, a presentation of a possible implementation of the data collection process will follow. I considered this step essential in my work, especially to emphasize the immediate applicability of the concepts presented and its feasibility with tools available to all. Also for this I will try, where possible, to present open source alternative tools to show how to approach this type of solution even with limited resources.

2
Literature Review

As for security, cybersecurity has now reached a point where people start to realize that preserving the integrity of private networks has its positive resonance not only for them, but also for the whole society. For this reason, the literature on computer security today is not only lead by private researches by big tech companies, but it also involves the academic world and, over the past few years, the political debate. As awareness grows, it brings the necessity to extend security legislation and include cybersecurity as a constitutive paradigm. Various initiatives have been developed in the form of guidelines and frameworks[11]. Examples are the UK's Cyber Essentials[12], the SME Guide from the Center for Cyber Security Belgium[13], the Center for Internet Security Controls in the USA[14] or the Finnish Cyber Security Certificate. All these are still far behind private initiatives [15][16] [17], which have lead the cybersecurity panorama for years, but they are without any doubt a first step in the right direction.
Among these, however, I did not find any solution that matched my needs, at least not completely. So, always in the idea of breaking down bigger problems into smaller ones, I took a step back. Leaving aside for a moment the frameworks already created, I have searched in various publications some contextual information to frame the context and the core problems.

2.1 Small and Medium Enterprises

The global digital transition, which was accelerated by the COVID-19 pandemic, forced all institutions, including small businesses, to increasingly depend on Information and Commu-

nication Technology (ICT) for their daily operations and service delivery. The proliferation of ICT in enterprises enables them to develop new business models and enhance their operational and commercial activities. Nevertheless, this practice also introduces new cybersecurity risks and vulnerabilities. While large organizations typically have the resources and an established cybersecurity program to mitigate these risks, SMEs often face a different scenario.

In Italy, but in general following an EU definition, a company is referred to be a small-medium business if it employs at most 250 people and generates less than 43 million dollars in annual revenue. Small businesses play a crucial role in fostering community development, providing local employment, and serving local markets. In northeastern Italy, for example, the economic landscape is not dominated by large companies or multinational corporations, but rather consists of a vast network of SMEs. According to 2021 Eurostat data, Lombardy and Veneto are the regions with the highest concentration of SMEs, which make up more than 99.5 percent of the total business landscape in those areas. [18] This is because not all economic sectors benefit from large-scale production but also because of historical and cultural reasons. The socio-economic context of this part of the country has grown in this way and thanks to this situation it owes its dynamism and resilience. All this to say that it is difficult to think that this situation is close to disappearing, but it is a phenomenon that must be understood, accepted and managed accordingly. This leads to the need to focus specifically on SMEs.

In addition, it's important to recognize that most start-ups begin as SMEs, for obvious reasons. This companies, particularly in their early stages, share with SMEs many of the peculiarities and vulnerabilities. This means that creating a more SME-friendly economic environment also means protecting this sector of the economy. A sector that involves companies that drive technological innovation and development during their formative stages, when they are most fragile. Of course, this cannot be generalized for every small or micro enterprise, which in fact are usually small family-owned and low value-added companies. But this highlights the importance of developing solutions that are scalable and financially viable, even for smaller companies.

Moreover, it must be considered also that in a globalized and specialized world, only very few companies control an entire production process on their own. The interconnected nature of businesses means that the security of one company often depends on the security of its partners and vice versa. Weak security practices among SMEs can create obstacles for them in forming partnerships with larger companies, as they may become the weakest link in the supply chain. It is common for less organized companies to become targets for cyberattacks that exploit their vulnerabilities to infiltrate their partnerns' networks, which are more developed and

well-protected. By adopting strong security practices, SMEs can build trust within their business ecosystems, opening up new opportunities for collaboration.
Now that the importance of SMEs in the socio-economic context has been established let's concentrate on their specific features. From an engineering perspective, deals with SMEs means having to address three major constraints: limited resources, a shortage of skilled personnel, and a lack of research and development.
Resource constraints are a common issue on small activities and can take place under various conditions. For low value-added productions, slim profit margins mean that even when profits are substantial the funds available for innovation and security remain limited. Other times the profits can be substantial but the awareness of the staff is limited. This is a scenario which I have encountered frequently in my work experience. It involves entrepreneurs who are unaware of the importance of IT as a fundamental element of a modern and efficient business. In these cases, limited knowledge makes it difficult to convince the manager of the real economic benefit of IT development. Even more difficult if we consider the next step, that's the cybersecurity. Otherwise, in the case of a start-up for example, there are budget and awareness but usually the resources are entirely allocated on developing their product, with the goal to quick enter and dominate a niche market. The conquest of a market could lead to a fast growth and so to greater financial resources in a next future. This makes some entrepreneurs to not invest in security as part of a calculated risk to expedite reaching that goal.
The second constrain is the widespread technological illiteracy. This does not mean, of course, that every employee should have a background in computer science. It means, however, that a minimum knowledge is necessary for all, not only to increase their operativity, but also because the lack of preparation leads to problems at various levels. I have already said how low risk awareness could impact the invested resources, because a good number of workers and entrepreneurs are opposed to expenditure or regulations they consider unnecessary. Related to this is also the physiological shortage of qualified personnel, which surely depends on the fact that this kind of specialized workers are difficult to find and therefore very expensive. This shortage results in the recruitment of staff not properly trained and in an almost total absence of cybersecurity protocols and mandatory implementation of best practices. If we then omit the specialized personnel, SMEs also represent situations in which it is often not common to organize training courses for employees who therefore generally have a level of awareness absolutely insufficient. And this is a threat from another point of view because an unprepared user is by itself an easily exploitable vulnerability.
Lastly, I've noticed that the cybersecurity research landscape for SMEs remains notably under-

developed. A critical gap exists in statistical data concerning the most prevalent threats these businesses encounter and their overall security readiness and awareness. Comprehensive bibliographic reviews of cybersecurity literature reveal that, despite a substantial corpus of published work, particularly in the realm of standardization, there is a marked scarcity of research specifically tailored to address the unique needs and challenges faced by SMEs.[19] [20]

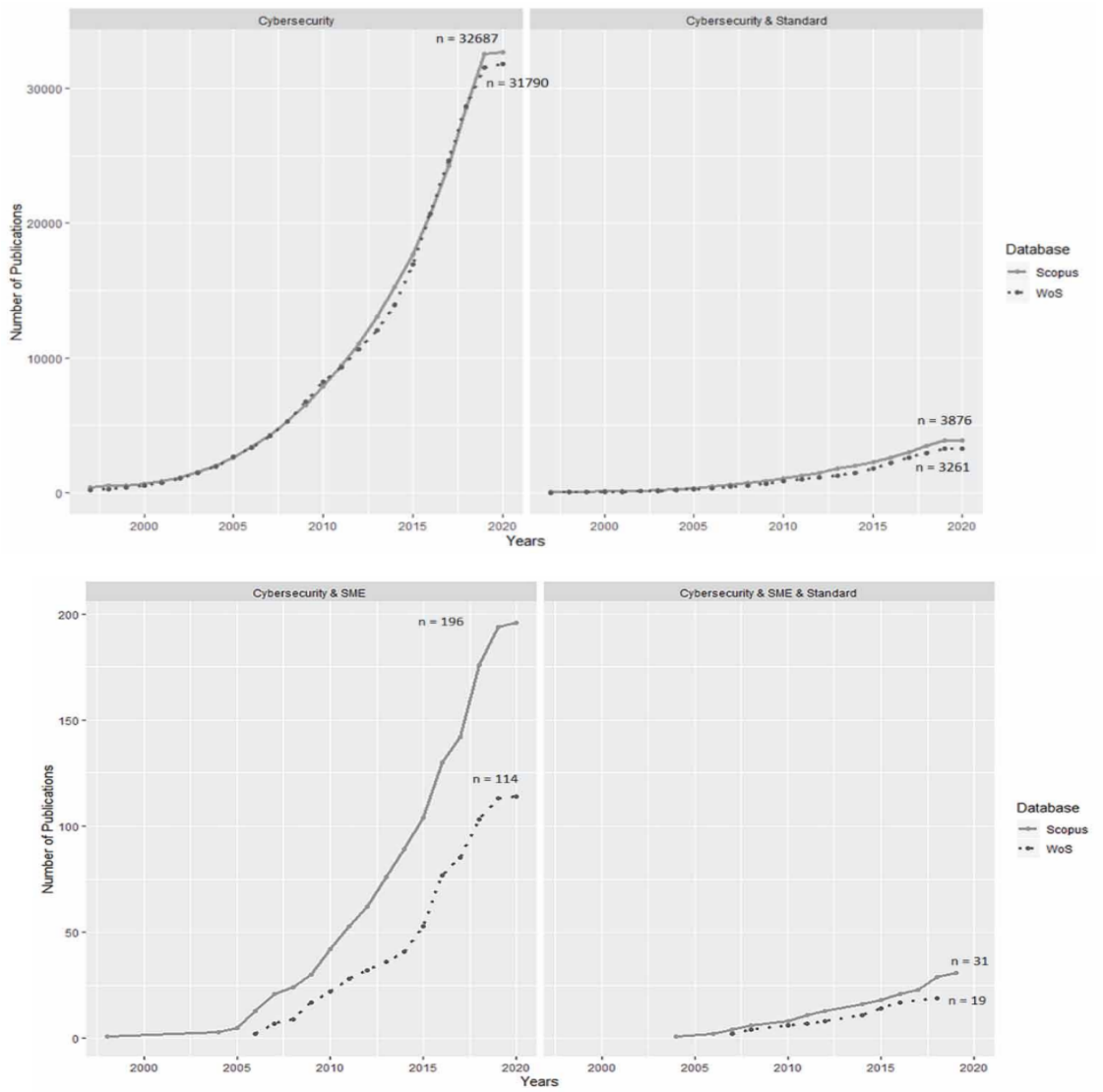


Figure 2.1: The graphs show that the literature in recent years has been much more focused on large companies than all SMEs. Figure taken from "Cybersecurity Standardisation for SMEs: Stakeholder perspectives and a research agenda", International Journal of Standardization Research Volume 17, 2019

This situation could find an explanation on simple economics. Major players in this sector understandably prioritize corporations with substantial budgets that benefit from economies of scale, resulting in lower management overheads. For example, consider a Remote Monitoring and Management (RMM) systems. This tool typically comprise a central controller, a limited number of probes, and numerous agents installed across machines. The bulk of the implementation effort lies in setting up and configuring the probes and the centralized controller, with minimal additional effort required to manage 10 or 100 nodes. This implies that the cost differences between SMEs and large enterprises are minimal, making the pricing often prohibitive for smaller businesses. This pattern extends to other cybersecurity solutions, including endpoint protection software, switch and access point controllers, and vulnerability detection systems. The market's orientation towards larger clients is further evidenced by entry-level packages from major providers, which often starting at a minimum of 1000-1500 nodes, effectively excluding SMEs as a viable target market. It is not a coincidence that the role of an MSSP is also to condense into a single controller the needs of different companies to achieve a volume of users sustainable from an economic point of view. This industry-wide trend exacerbates the cybersecurity challenges faced by smaller businesses, leaving them vulnerable incapable to sustain some solutions by itself.

2.2 Common Threats

At this point, the focus shifts to the quantity and type of threats that SMEs must face when it develop its own network. Many people assume that large organizations are more vulnerable to cyberattacks than small businesses due to the scale of their operations, but this isn't necessarily the case. According to the Verizon Data Breach Investigations Report (DBIR)[21], there was only a relatively small difference in the number of data breaches experienced by large and small organizations in 2021. Furthermore, large firms tend to detect breaches more quickly than small organizations in over half of the cases, primarily because they have more robust and well established security measures in place. A compilation of statistics by Maddie Shepherd shows that 43% of cyberattacks target SMEs, underscoring their vulnerability in the digital world. Even more concerning is that 60% of small businesses are forced to close within six months of a cyberattack, illustrating the severe consequences of such incidents. Additionally, 47% of small businesses lack the knowledge needed to protect themselves from cyberthreats, pointing to a critical need for better education and preparation. Moreover, the combined impact of human error and system failures, which account for 52% of data breaches, underscores

the importance of addressing both technological and human factors to develop comprehensive cybersecurity strategies. [22] [23]
It should be considered that SMEs are not only a favorite target for cybercrime, but their peculiarities make them suitable for some particular types of attacks that maybe would be ineffective in other contexts. This does not suggest that there are cyberthreats from which SMEs could not defend themselves, neither that big companies become immune when reaches a certain size. It underlines the fact that usually attackers need to invest time and resources into their activities, making some attacks, which are particularly sophisticated and costly, not economically viable. SMEs are rarely targeted by DDoS campaigns or infiltration. Instead, smaller companies are more likely to be affected by large-scale attacks designed to strike as many targets as possible in search of a vulnerable entry point. Common threats to SMEs include phishing campaigns, exploits on outdated firmware and brute-force password attempts. A 2022 survey indicates that malware (18%), phishing (17%), and data breaches (16%) are the most common attacks on small enterprises [24]. An other independent research states that in 2024, 82% of ransomware attacks targeted businesses with 1000 or fewer employees and that the majority of malicious emails, including spam, phishing, and email malware, are targeted at companies with fewer than 250 employees [25].
When assessing the security of a small firm, priority should be given to areas where the company is most vulnerable and most likely to be attacked.

2.3 Assessment Frameworks

The assessment process falls under the wider category of production process analysis. Within this framework, there are various subsets of assessments that differ based on their objectives, execution methods, and target areas. A key step for research is to determine which of the existing methods is most suitable for IT analysis in the context of SMEs. A first example is the vulnerability assessment. Both vulnerability assessments and penetration tests are examples of target-oriented approaches. In a vulnerability assessment the focus is more on identifying specific weaknesses that make an organization or asset susceptible to exploitation by particular threats. Meanwhile, penetration testing is more concerned with identifying potential scenarios that could exploit these vulnerabilities and negatively impact organizational operations, assets, individuals or even the entire society. Both of these examples focus on a specific objective and explore it in depth, but they have limitations, especially regarding scalability, standardization and comprehensiveness. Their effectiveness varies significantly depending on the chosen tar-

get and its size, and they often do not adequately consider the broader context. Additionally, both typically require a subsequent operation of analysis and recommendations based on the collected data, which can vary widely depending on the results of the initial assessment.
A different approach is the so called "checklist-based" evaluation. This kind of approach utilizes a list of activities, functions or properties to structure the assessment process as a checklist. The elements are subsequently taken from the list and the security state of the evaluated system is confronted with them. In this case, the pros and cons are exactly the opposite of what we saw earlier. Main strengths of this kind of approach are scalability and adaptability to different contexts. Matter of fact this type of analysis is used on application for quality or legislative standards, which must be transversal to the context and size of a company. On the other hand, weaknesses are definitely in the design and in the depth of the analysis. Creating a sufficiently comprehensive checklist, which is at the same time effective and simply implementable, is an operation that requires time, research and experimentation. Not to mention that it is then necessary to update it with the progress of the standards or of the technologies employed. Moreover, such an analysis may often be limited in very uncommon situations and It tends to be much more transversal and much less in depth. The most famous example of checklist assessment are the ones to achieve compliance with the GDPR (General Data Protection Regulation) or the NIST (National Institute of Standards and Technology) frameworks. The ISO standards (27017 for Cloud Security, 27001 for Information Security Management System and so on) are also very widespread, especially to become part of the supply chain of major international players in almost every manufactural sector. And these are just some examples
Both methodologies find their place in the context of SMEs and it is necessary to consider their pros and cons to outline the structure of a framework as effective as possible in the context in which this work is focused on.
But beyond one method or another, what emerges is that there are some fundamental points that make a framework effective and complete. First, the steps that it must have at least:

Criteria: the framework provides a set of criteria against which SMEs can evaluate their security posture. These criteria cover various fields, such as risk management, security controls, incident response and compliance.

Levels: the framework outlines a structured evaluation scale that categorizes different levels of security maturity. Each level represents a set of specific security practices and controls that SMEs are expected to implement. By identifying their current level, SMEs can determine the necessary actions and improvements required to advance to higher levels of security as quick as possible.

Best Practices: the framework provides a detailed set of best practices and recommendations for implementing robust security controls, policies, and procedures. By following these best practices, SMEs can enhance their security posture and ensure that their cybersecurity measures are effective and up to date.

Final Roadmap: based on the outcomes of the assessment, the framework assists SMEs in creating a strategic roadmap for advancing their cybersecurity maturity. It serves as a practical guide to follow, helping them systematically progress towards a more secure and resilient cybersecurity posture.

State that, from the review could be deduced also that not only in the steps there is a certain repetitiveness, but also in some crucial targets that cannot be ignored:

Technological Aspect: this involves a comprehensive review of the various technologies currently employed within the organization. It includes an evaluation of how these technologies are maintained and monitored on an ongoing basis. This aspect covers not only the initial deployment of technology but also how well it is supported over time, including regular updates, patches and performance improvements.

Human Aspect: this perspective focuses on the level of awareness and competency among staff regarding technology and cybersecurity. It assesses how well employees are informed about current practices, threats and necessary procedures. This includes evaluating training programs and the effectiveness of communications.

Innovation Aspect: this aspect evaluates the organization's capacity to embrace and invest in new technologies and innovations. It examines how well the company adapts to evolving technological trends and its commitment to continuous improvement and development. The focus is on how proactive the company is in fostering innovation and integrating new solutions into its operations.

Based on these insights gained from the study of the scientific literature on the main topic, it is now possible to start structuring the theoretical form of my analysis framework.

3

THEORETICAL FRAMEWORK

To clearly define an IT assessment, it is essential first to outline its objectives and the methods to achieve them. In the business context I experienced, the primary objective of an IT assessment was to establish a foundation for collaboration between my company and a new customer. For a company like Solunet, which distributes hardware and software, provides services, and manages IT infrastructure projects, this assessment is almost a mandatory step. It is not possible to manage a network without knowing it in detail and without having a general overview of the company it belongs to. And being the first form of collaboration, it also assumes the role of an introduction. From the customer's perspective, in fact, an IT assessment is like an examination, a way to gauge the professionalism and capability of a company that will become a crucial component of proper business operations. An effective assessment illuminates three crucial dimensions about the company that makes it: knowledge, efficiency, and vision. Knowledge is exemplified through a comprehensive usage of information theory, encompassing software execution, communication protocols, security measures, telecommunications and data protection strategies. Efficiency manifests in the execution of the assessment process, unfolding transparently under the client's watchful eye. This approach optimally leverages both technical tools and human expertise, demonstrating a methodology that maximizes resources and minimizes disruption. And lastly vision is reflected in the assessment's focus, which must go beyond mere documentation of existing infrastructure. It lays the foundation for future initiatives and provides a benchmark for evaluating the success of completed projects. This forward-thinking perspective ensures that the assessment not only captures the current state but also guides fu-

ture growth and development. These are the objectives that the assessment must achieve to be effective from the point of view of both the supplier's and the customer's desire. But, if one wants to consider its efficiency in technical terms, we must add new variables to the equation. Firstly, an IT assessment requires operators with a various and deep skill set, comprehensive of software, hardware, and personal expertise. Such versatile professionals, capable of adapting to various needs and contexts, are hard to find and challenging to train. Typically this versatility could come only from extensive field experience. On the other hand, the context of SMEs is characterized by all the main obstacles we presented in previous section. Companies have a shortage of trained personnel and limited budgets which are, often, even delayed in time. This usually leads to infrastructures that are designed with efficiency as primary focus, forgetting essential security considerations. This oversight is critical and demands a new approach to the IT assessment process. Planning for efficiency rarely aligns with development towards security, because the faster is a process and the more difficult it becomes to control it. Based on this assumption, it is unthinkable to develop an IT assessment that does not consider cybersecurity as an integral part of the functioning of the entire structure. From all these points it follows that the process of IT assessment must be thought from its fragilities, to define the development criteria necessary to fix them. The formulation of my IT assessment will therefore take as the cornerstones of the project three fundamental paradigms: modularity, security and clarity.

Modularity

Modularity is the criterion that defines a complex process as the sum of simpler ones. These simpler processes allow us not only to adapt to different dimensions and contexts but also to offer a greater level of depth. I have applied this principle many times in my attempt to define the problem, but now we need to implement it within the solution. Instead of carrying out a monolithic project that in the name of replicability sacrifices time and resources in unnecessary analysis, a modular assessment could offer a separate set of services. These services needs to be independent of each other in execution but linked in purpose and conclusions, able to better concentrate time and resources. This allows the staff involved in each module to specialize in a more restricted field of competence, increasing their skills and simplifying the training process of new technicians. Making the process as independent as possible from the people who carry it out is a key factor in achieving a certain objectivity. Even for the customers modularity is advantageous because it allows them to request each module separately. Obviously this contradicts one of the key points of IT assessment, that is to be broad and comprehensive. But at the same time this practice allows to meet those customers who have limited budgets, or those who

entrust part of the infrastructure to other players and only need a specific service. Moreover, at the end of a development or improvement project, the application of only a dedicated module could be a form of evaluation of the quality of the work. That's extremely useful to keep up to date the knowledge about an infrastructure but at the same time is cheaper and faster than a new comprehensive assessment.

Security

Security is the second criterion on which is structured my attempt to define IT assessment. As said before, it becomes fundamental to consider the planning from the point of view not only of the functionality of an infrastructure but also from that of its protection. Always referring to the three cornerstones of security, availability, confidentiality and integrity, the IT assessment must aim to integrate cybersecurity among the essential features for the functioning of a network. The message that must transpire is that an insecure infrastructure cannot support and guarantee the work of a company, without exceptions. Scurity, in the IT field as on other fields, must be implemented from the first stages of the growth process. A solid foundation not only provides protection regardless of the company's size, but also ensures easier scalability in case of future growth. Many times, during my internship I had to deal with companies that did not want to deviate from their initial choices and found themselves having to reinvent their infrastructure from scratch to reach the status that their position in the market imposed.

Clarity

I decided to include clarity among the fundamental criteria to adapt my work to the context in which I decided to develop it. This does not mean having to create a trivial or discounted evaluation system just because it can be understood by low-skilled people. On the contrary, it means being able to give to the evaluation a shape that is both objective and technical but also clear and understandable. The evaluation criterion must be able to highlight the differences between before and after an intervention but also between two companies that may have different peculiarities and needs. It must be able to give different weights to different interventions and to provide a global vision of the infrastructure that transcends the single devices. It must also reflect some specific characteristics of cybersecurity. It must be considered that just as a chain is said to be as strong as its weakest link, also an IT infrastructure can be assessed very negatively despite having some specific excellencies. An almost perfect system with a breach could prove weaker than a mediocre but homogeneous system in every cybersecurity aspects.

In other words, it can be said that the evaluation, to be consistent, will have to weigh the weakness rather than the strength. All these concepts must be included into a solution in a form of numerical and/or graphic presentation of the final result.

3.1 Assessment Modules

With the objective of modularizing the assessment process established, the focus should now shift to a pragmatic analysis of the most effective way to implement this division. Following the principle of security, a useful starting point could be the three pillars of cybersecurity: availability, confidentiality and integrity (ACI). This type of subdivision would certainly be an effective way to highlight the importance of safety and evaluation, also because the three concepts are well defined and simple to present. However, from a practical perspective, this subdivision loses some effectiveness. First of all they were designed for security only while my work tries to be more comprehensive. After that it must be considered that from the point of view of real implementations this subdivision is not always respected. Integrity and confidentiality are often interrelated and customers rarely approach an assessment by addressing these two aspects separately. There are certainly solutions more similar to one or the other but it is rare that a such specific solutions are created. If you create a VPN you try to make the data stream hidden that difficult to tamper with, and same for backups or for communications. This does not alter the fact that the ACI subdivision cannot be taken up in the presentation of results, but as far as the structure of the analysis is concerned, the division must be different. It took shape a little bit at a time by evaluating the series of interventions and analyses that I intended to insert, trying to balance both, coherence of the concepts and amount of work needed. The final subdivision includes three macro-modules: operational analysis, security analysis, and personnel analysis. Each one of these modules are them divided again into sub-modules I will present in next sections.

3.1.1 Operational Assessment

The operational assessment is the process that takes its cue from what was the IT assessment previously offered by the company. Its main purpose is to assess if a company's IT infrastructure can support its production needs. This aim, however, by its nature, poses some issues for what concerns adaptability. The efficiency of a structure depends both on the capacity of the infrastructure itself but also on the needs it must meet. Having an overabundant structure is a

positive note, but it does not guarantee anything more than a structure that is simply adequate. At the same time, it is also necessary to consider the future planning of a company. A company that aims for rapid expansion must consider not only the sustainability of the currently active network but also the needs and challenges that will arise from the increase in personnel or from the acquisition of new locations. With these premises established, it comes that in first instance the operational assessment must take into consideration two crucial factors: the current necessities of the company and the future plans. Once the premises have been defined, then the object of the analysis must be determined. Following the criterion of modularity, the analysis of the capacity of an infrastructure can be divided into two macro categories, the analysis of the effectiveness of individual components and the analysis of the process to control and manage these components. The first instance will consider:

Hardware component(HC): hardware components are the starting point for building an infrastructure. In this first section I will consider only the computing units, therefore servers and clients, while the network hardware will be treated separately. The aspects that I will evaluate will be related to the computing power and storage capacity of devices, which I will compare with what are the needs of the company. Regarding the computational power I will have to take into account also the typology, because CPU and GPU respond to different needs and they cannot always be superimposed. On the other hand, for everything else I will give importance to redundancy, which is useful both not to stress too much the hardware and to take over in case of failures and malfunctions. The third point is only optional because it aims to evaluate what IoT devices are, whether they are sensors, controllers or other. These are often an integral part of a company's structure, especially if it works on manufacturing, and as such cannot be excluded from the assessment.

Software component(SC): the software component investigates the efficiency and effectiveness of the software used by the company. Production and management software are treated separately because they have a different impact on the production process. In production, the software is often integrated into the machines that governs and it is therefore difficult to maintain or update and many times impossible to replace. The difficulty of use it become secondary because the workers of a certain machine develop by habit a certain efficiency in repetitive processes, regardless of their complexity. It follows that the evaluation will give more weight to the maintenance and updating possibilities in production software, while for management software it will focus more on its usability. These are generally much less repetitive and more articulated because they have to accommodate different customers and bureaucracy. Virtualization software is treated separately as it serves as the basis for any other software, including operating systems, and therefore its impact on operations is by far the most impactful. Regarding the

virtualization software will be considered the stability and the ease of use as well as the integration with other solutions (hyperconvergence).

Network component(NC): the network components are treated separately for two reasons. First of all, they are devices where it is very difficult to separate software and hardware. Switches and firewalls, but also access points and routers, are equipped with custom-made operating systems, so replacing them is not only difficult but often counterproductive. On the other hand they have an incredible impact on the productivity of the company regardless of its client and server capabilities since they manage communication between all nodes. In this case the values that will be taken into account are the troughtput, i.e. the data flow that these devices can handle, as well as their modernity and integration with centralized controllers. In these cases a real added value is the redundancy of some nodes, the so called "high availability", which consists in splitting some nerve points so that to the failure of one, follows the immediate replacement of its twin device. I have included in this section the analysis of access control to storage over network. This is firstly because its operation is related to the communication protocols used more than to the nodes that allow it to function. Then also because this analysis very often results in an active directory analysis, which does not make sense to exist unless in a network context. For this point configuration of services and best practices are considered to come to an evaluation. Best paractices could comprehend some simple task as to establish consistent naming for groups, users and computers or to clean Up unused AD Objects. Others are more difficult to set up and include to limit administrative access, to use Group Policies strategically or to enforce strong password policies.

Resource supply(RS): resource supply considers the provision of everything that is essential at a physical level to support the infrastructure. This is all about power supply and connectivity. Regarding connectivity, two different forms of distribution should be considered: the one that allows the internal network to connect to the external one and the one that allows it to be distributed internally between the various nodes. The evaluation will then take into account separately the stability and the availability of external connectivity, and then the stability and capillarity of internal connectivity. For the internal network, a certain priority is given to wireless distribution because it is more complex to spread and has also more issues, depending on electromagnetic noise and physical obstacles. With regard to the energy supply, what is evaluated is the presence and quality of Uninterruptible Power Supplies (UPS). These devices are used to support the infrastructure in the event of an electrical failure, but also preserve its integrity. In fact, even being unable to sustain production for a long period of time, they can allow a gradual and soft shutdown of the core devices and are also able to protect these from voltage surges or short interruptions.

The second instance considers the monitoring and management process of the infrastructure,

which include also its ability to resist and respond to an issue, both it is caused by an accident or an attack. It shall consist of:

Monitoring(MO): monitoring of an IT infrastructure can take place on various levels. At packet traffic level, monitoring could be useful for managing the data flow, recognizing abnormal flows or redirecting traffic, preserving the operability of the entire network. This can happen at the firewall or switch level, especially if their have a centralized controller, as their operating systems often include components for data collection and analysis. Otherwise, another solution is to use one or more nodes as a probe, which is also often used in the context of Remote Monitoring and Management (RMM) software. RMM is a type of software used to remotely control IT devices. It allows IT administrators to proactively run commands, change configurations and collect information without having to be physically present on-site. Often such systems are also able to exploit a protocol called Simple Network Management Protocol (SNMP), which allows to extract information from the nodes of the network without affecting excessively on the performance. Due to its effectiveness I decided to include a specific entry for this protocol in the evaluation. As a last point I considered the implementation of a system for log collection and log analysis. This system not only provides information in real time but also allows to keep an history record. Generally this is a very sophisticated structure, even very expensive, but it proves to be fundamental in context of disaster recovery and forensic analysis after a cyber crime.

Incident response(IR): By incidence response is meant a structured process for identifying, managing, and mitigating accidents or attacks which aims to break down an organization's IT systems. This is a term that is often associated more with cybersecurity than with business continuity. In this case I decided to insert it to emphasize the importance of having not only an efficient but also a robust infrastructure, especially considering the large number of SMEs that do not survive the damage caused by cyber attacks. For these reasons two points of the evaluation recall backups, analyzing their effectiveness in data recovery from two different points of view. The first point concerns the time coverage of backups, which should be either close enough to the present, to lose as few data as possible in case of restore, and also sufficiently far, to ensure with some probability that the system can be returned to the state before it was compromised. It should be considered in fact that many cyber attacks include a period of study in which a system is compromised despite continuing to operate. The secondo point considered about backup is their capacity to quickly restore the informations. The data recovery period is a production downtime and as such can be measured in terms of the downtime costs for the company. The third point of the evaluation will be on system's ability to replace services. In this case, the redundancy is evaluated, both in terms of hardware resources for a possible migration of virtual machines and from the point of view of nodes in high availability. To cloud services are given a certain importance because they generally rep-

resent an excellent solution in terms of continuity and reliability, especially for SMEs. This is because they are the expression of much larger companies able to provide greater guarantees and security.

All these appraisals, like I said before, will go then weighted to the necessities of the company and to the longevity of the infrastructures, always considering the future expansion of a company. Slight fluctuations may then be included in the evaluation, resulting from the reputation of the tools used and the reliability of the brands, but given their limited objectivity they are not considered as an indispensable element of the evaluation.

3.1.2 Security Assessment

In the context of security analysis, a widespread process in the IT field is vulnerability assessment. Vulnerability assessment is a commonly used term to outline a process that aims to research and evaluate vulnerabilities in the company's software. This process usually includes the use of software to scan operating systems and applications in search of known vulnerabilities or versions not fixed yet. In its most refined version, it evolves into vulnerability management when in addition to vulnerability detection it also proposes a structured remediation plan. In my work experience, however, I noticed that this approach to vulnerability was extremely sterile, both from the point of view of a company that requires it and from that one of a company that provides support. Neither of these entities usually has the possibility or the capability to intervene directly in the remediation of a CVE. They only can operate a software update, where possible, or a hardware replacement. In the context of SMEs, unfortunately, both these solutions may be impracticable, due to the costs involved or to problems of compatibility with implemented software. It is therefore necessary to approach this kind of network weakness with a different point of view, the point of view of someone that is incapable to solve a problem and must proceed mitigating its effects. Now I want to emphasize that this framework is not an attempt to deviate from what are the best solutions and best practices, but a process of acceptance of their limits. While research aims for the ideal scenario, engineering must optimize with the resources at hand. Consequently, my assessment extends beyond a simple vulnerability assessment, adopting a more comprehensive approach. It focuses not only on vulnerabilities but expands the vision to include the two inseparable aspects: the weaknesses of an infrastructure and the security measures implemented to mitigate these weaknesses. From this perspective, the security assessment will initially consider:

Software update(SU): a well-structured and continuous update policy is the main tool that a company can adopt in an attempt to limit the amount of software vulnerabilities. Based on this assumption a vulnerability scan often leads as a first result to a list of updates and security patches not yet performed. In this first evaluation I thought it was necessary to separate the updates related to the operating systems from those of the application software. This is not only for an order reason but also because often companies do not have a policy of management of applications, so they find themselves, after a scan, in front of an endless list of unwanted software. These software could then be uninstalled or replaced, which is much more easyier if compared on change the operating systems. Beyond this, in both evaluations I tried to give some weight to the percentage of nodes updated and then some weight to the evaluation of the CVE, both according to the CVSS scale and EPSS scale. This decision stems from the fact that even CVE not yet exploitable must be considered in the whole view of the security of the system, although it does not obtain a high EPSS value. As last factor to evaluatre I decided to give higher importance to all those software that can not be updated. This may be due to a number of factors, such as the fact that the software is no longer supported or that an update could lead to compatibility issues. In this case the vulnerability cannot be fixed but the node can be isolated from the system, or monitored. In this case I will therefore give importance not to the severity of the vulnerability but to the accessibility of the compromised node. So considering its connections with the external network and with other fundamental nodes of the infrastructure.

Known vulnerabilities(KV): this section is designed to group together a whole series of results from a set of standard controls that add up to the CVE scanning work. There are a number of extremely common vulnerabilities that relate to the wrong configuration of the software more than the software itself. As a matter of order I thought to divide the analysis between the vulnerabilities reachable from the external network and those reachable from the internal network. In both cases, a certain importance is given to vulnerabilities related to the injection of malicious code, be it SQL, Javascript or other. This is because they represent a type of vulnerability extremely easy to patch but at the same time devastating in terms of danger. With regard to external scanning, the presence of unknown exposed services or even open doors is then evaluated, and the possibility of finding sensitive information from these channels or from the company's public channels. On the other hand, in the internal scan, it is given importance to insecure communication protocols, which would allow an infiltrator to obtain information by sniffing traffic, and on the use of illegitimate software. I decided to include in this section the evaluation of the logging system because it is the most powerful tool for investigating known vulnerabilities, outside the assessment process.

The second fundamental issue concerns the countermeasures put in place to respond to these vulnerabilities. This, as already mentioned, is important because of the limited resources of

SMEs in which for economic reasons or backwardness it is not always possible to eliminate vulnerabilities. So there are:

Perimetral security(PS) Perimetral security is the first layer of protection against attacks from outside. For the evaluation it is therefore natural that the first element that is considered is the firewall. Of course, firewalls, especially the new generation ones, contain a wide range of security services in their software. For that reason I decided to consider the overall traffic handling function and the Unified Threat Management (UTM) separately. First of all the framework will evaluate the segmentation of the network, assigning higher ratings according to the specificity and capillarity of the division. In this case, greater importance is also given to the internal network access policies, that means to the firewall control interface and to the VPN service. Later on, the UTM will be evaluated, obviously in proportion to their invasiveness and effectiveness, from the simple traffic filter to the most sophisticated IDS/IPS. Subsequently, an element of evaluation will be the mail system. Despite of it is a less sophisticated service, the mail service is still the main risk for a company from the point of view of external threats. This because it often delegates to human judgment part of the control process. For that reason the final rating depends on the number of layers of checks added to the mail before it is delivered to the user. The human component certainly retains its importance but replacing it as much as possible with automation makes it possible to compensate for the generally low level of digital awareness in SMEs.

Network security(NS): in the section of network security, will be taken into account all those countermeasures that operate at the level of interconnection between nodes. The first consideration concerns the lowest level of communication, that reguards which connections are allowed and which are not. To highlight this, the segmentation configuration, usually via VLANs, and the switch configuration are evaluated. Often, in fact, the lack of traffic monitoring or the wrong configuration of trunks between the various switches can compromise the isolation of internal subnets. The second point concerns access to storage space through the internal network, which is very often due to an active directory evaluation, as already mentioned for the operational assessment. The last point is optional and concerns an analysis of the digital signature process, whether it relates to documents, scripts or other. The reason I've included it in network security is because it's more about the ability multiple nodes to recognize each other rather than the security of a single node. Which made it more similar to the world of network rather than endpoint.

Endpoint security(ES): endpoint security is difficult to assess because it involves, more than others, all the main actors of cybersecurity. In order to create an assessment as much simple as possible I tried to group the endpoint security into three subsets: security software, backup software, corporate policies. Security software evaluates the effectiveness of endpoint protection, evaluating systems that implement behavioral analysis

or AI over and above the simple decentralized antivirus, which in its individual is increasingly ineffective and anachronistic. The backup system on the other hand allows me to evaluate both the response capacity of the node to an attack, and the information security from a side channel. In fact, it is often not considered that the backup is itself a copy of the currently active node and keeping unencrypted or unprotected backups is comparable to leaving crucial information accessible to everybody. The last point addresses the importance of some standardization on the use of the endpoint, in order to make it more manageable and prevent risky behavior by inexperienced users. The policies of apps allowed or forbidden, the reliability of company software and best practices like screensaver are considered for the final evaluation.

Ultimately it seems essential to evaluate all corporate policies related to access, whether it is intended as physical or virtual:

Access protocols(AP): access protocols are divided into virtual and physical. Password policies are given greater importance, especially as identity theft is a much more common threat than physical intrusion into company systems. In particular, for passwords, two elements are considered. First of all, I give a certain weight to how the password itself is formed, considering the expiration date and the complexity of each one. Secondly, the password management is considered, so whether it is transcribed on a sheet, file or password manager and if there are leaks of passwords in known database breaches. The last element of evaluation concerns the policies of physical access to the infrastructure, thus also considering the surveillance and the appointment of responsible persons.

3.1.3 Personnel Assessment

The last module to complete the idea of IT assessment, despite being the analysis of a telecommunications infrastructure, must concern the human component. In the world of IT, in fact, a component of risk also derives from the improper use of a device and not necessarily only from the vulnerabilities inherent in it. Considering the human component, there are several interactions that must be taken into account to obtain a complete evaluation. In the first place, we need to consider qualified personnel or, at the very least, those who control and manage the infrastructure. While this may seem obvious, the qualification of staff is a crucial factor in the SME world. Certified and highly qualified managers can usually aspire to particularly lucrative positions in companies against which especially small companies cannot compete. In addition to this, often such entities do not even have a human resources department capable of effectively assessing a candidate's abilities. The second fundamental factor concerns protocols and

restrictions imposed on personnel to limit the use of infrastructure to what are security practices. Finally, we must consider the human factor of unskilled personnel. In this case it becomes extremely challenging to maintain a schematic and objective assessment, since investigating the habits and abilities of a large group of people is likely to become excessively burdensome and beyond the actual needs of an analysis of this nature. In these cases the most sensible approach is to use tests, simulations that can push employees into controlled risk situations to observe their reactions. A classic example is phishing campaigns. To these tests can be added another analysis very widespread in the cybersecurity field and that goes instead to test the confidentiality of the company's information through the information made public by its staff. This analysis is called OSINT (Open-Source Intelligence) and usually aims to search public sources or easily accessible to try to obtain information. The sum of all these different processes goes to constitute the modules linked to the personnel that could be so embedded:

Designed personnel(DP): the evaluation of the designated staff is certainly a very difficult analysis to carry out objectively. First of all, because it is a situation in which some technicians are judging the work of personnel who, on paper, should have a qualification equal to that of those who are judging them. In addition, the work of skilled personnel often depends not only on the staff themselves but also on the limitations imposed by management. For these reasons, the evaluation tries to concentrate all these variables on a scale which considers the qualifications of the operators but also the budget and the company's guidelines. This analysis is carried out in parallel between the company's internal staff and external support staff, if any. This is because in these two situations there were, in my opinion, two distinctions to be made. In the first case, it is necessary to consider also the vision of the operator and his future projects, being an integral part of the growth of the company. This is a factor which cannot be demanded by external personnel, for which a crucial element that need to be considered is the timeliness of intervention.

Personnel awareness(PA): worker awareness is another key element to consider because it involves all that sector of staff who are not necessarily technically prepared in the IT context. This assessment takes into account two separate aspects: on the one hand, the current awareness of the workers and, on the other, the company's efforts to increase and maintain it. In the first evaluation scale I will try to probe the knowledge of employees on crucial aspects of their relationship with technology, as updating policies, controlled use of software and awareness in web browsing and using mail services. The company's effort is considered in the form of quality and consistency of the training process for the staff, and for the creation of guidelines. These guidelines should cover, at least, the process of adding or removing a user, controlling their access privileges and classifying sensitive data.

Protocols(PR): In a context of control and standardization of IT infrastructure, protocols are the main tool for increasing the level of security and efficiency for what concern the human factor. Focusing on evaluating unskilled personnel, I decided to include in this evaluation the two most effective protocols for limiting what are the main threats to SMEs, identity theft and client compromise. For the first case, the password policy is considered. Which is more complex as it may seem because a password to be effective must balance two opposing factors. In fact, the simpler a password is and the easier it will be to steal it, but at the same time the more difficult it is and the more the user will struggle to memorize it and end up saving it in some unencrypted file or writing it on a post it. An effective password must be complex but not difficult, must be changed frequently and must not be shared or reused. After that the evaluation considers the policies on the use of corporate assets, whether they are hardware or software, trying to limit the use to the work environment and reliable and controlled tools. Asset inventory and software inventory may seem simple countermeasures but in this context they are extremely underestimated but equally indispensable.

Other common analysis that could be incorporated on personnel assessment are also the most popular behavioural analysis on cybersecurity context:

Mail security(MS): as previously anticipated, e-mails are the main weak point of business networks, especially in SMEs. Automated security implementations have been covered in previous assessments, this section focuses only on the human factor of mail security. In this case the most effective tool is surely phishing campaigns. This tool aims to test your workers in channels such as email or company number to test their propensity to disseminate sensitive data without having carried out due controls. Often these analyses use email addresses very similar to those used by users, famous company templates or daily messages to confuse the victims. The successful implementation of a phishing campaign guarantees both a survey of your security and a method to train your employees.

OSINT(OS): Open Source Intelligence, is the practice of gathering and analyzing publicly available information to generate valuable insights. This method relies on a wide array of accessible sources, including websites, social media, government records, academic papers, and traditional media. It operates entirely within the public domain, making it a legal and widely used tool across various sectors. From the cybersecurity point of view this allows to understand the starting point of an external attacker, operating as an individual outside the company willing to collect as much information as possible.

The principle of modularity highlighted in this paragraphs is certainly combined with the need for specialization and efficient subdivision of the analysis process but also offers many facilities

from an exhibition point of view. In fact, when all three or even just a part of them is completed, they offer the possibility to mix the results and then to embrace the exhibition method more in line with the needs of the moment. This reflects both the desire for clarity of the framework and its aim to embrace an evaluation system that cannot disregard the idea of security.

3.2 Assessment Evaluation

The last step that remains to be done regarding the theoretical definition of our method of analysis is that of the representation of the evaluation. Initially I expressed clarity as one of the fundamental paradigms of my framework because the exposure of the results had always seemed to me one of the haziest and worst defined parts of IT assessment. That not depend just on IT cultural background of the people to whom it was exposed. Certainly, it should be considered the human component of the manager or the IT technician who may struggle to understand all the concepts presented. But, at the same time, it must be recognized that evaluations are often extremely linked to the technician who prepares the report. In the same way, demanding a purely mathematical and objective analysis is certainly an exaggerated goal. There is no structure that can guarantee 100% safety or operability,and therefore there is no point of comparison. As with many other branches of science, computer science has long accepted the fact that in the presence of huge quantities of variables the best choice is probability or approximation. A good result would be to develop a numerical representation and/or a graphic representation capable of expressing just some fundamental aspects. Working to reach a shape that is immediately recognizable, regardless of the preparation of the interlocutor.

3.2.1 Evaluation type

Starting taking as example the vulnerability assessment evaluation system, already widespread and well established, different scales are considered. The most common vulnerability scoring system Is the so called Common Vulnerability Scoring System (CVSS)[9] and it is a gravity-oriented evaluation system. This means that the more a vulnerability can be harmful to a network, the more it will be evaluated. So, for example a vulnerability that can be exploited simply to suspend a service will be evaluated much less than one that allows, for example, to obtain complete control of a machine. The great weakness of this rating scale is to consider only the danger but not the risk. In the current IT context, in fact, criminal groups and hackers usually specialize in some types of attacks, leaving out others, less profitable or less probable. In this

context it's normal to think that it's riskier to maintain a vulnerability with a medium severity, but that is sought by many, rather than a very serious one but little considered. This is why the Exploit Prediction Scoring System (EPSS)[26] was created. A risk-based scale that also considers the probability that a certain vulnerability will be exploited. It is a complex scale to structure, employing machine learning strategies to process large amounts of data from all around the world. In fact, it collects data from all the main databases of cyber-attacks and crosses the data to identify patterns and recurrences. In this way it provides a more comprehensive assessment, especially from the point of view of the order of priority in the remediation plan. Both these assessment scales, CVSS and EPSS, can be extremely exhaustive in certain contexts. The CVSS offers a fundamental descriptiveness to understand the weakness of a piece of code or to describe the occasion for an attack. Two environments far from the world of SMEs, closer to development companies, which have to deal with those CVE, or to attackers and researchers. EPSS, on the other hand, is already starting to look at the risk side, but in my opinion, it still offers a more problem-oriented perspective than a solution one. This is limiting because often, especially in the context of SMEs, this problem may not be solved. It often happens that there are compatibility problems, which prevent updates and the subsequent repair of CVE. This can happen for both enterprise software and hardware. If a node is carried whit a management software if it is embedded into a production machine, it is unthinkable that it should be replaced. This does not mean that there are no solutions to these kinds of problems, but it means that you cannot get rid of the problem itself. For this reason, a problem-oriented assessment risks to assess more the dangers of the risks, even if it is weighted as in the case of EPSS. Each problem has only one final solution but many different ways to get around it. The only way to take this perspective is to abandon the problem-oriented solutions and to shift towards a solution-oriented approach. Coming back to the focus of the IT assessment project, that is exactly on the development and the adoption of new solutions. This idea, originated in the context of vulnerability analysis, is so reasonable that can be applied to the entire IT assessment process. While it may lack mathematical rigor, a solution-oriented approach effectively bridges the needs of SMEs with the capabilities of supporting companies. This diverts the idea of assessment more towards a check-list based evaluation.

3.2.2 Solution-oriented Evaluation

A solution-oriented evaluation in its simplest form could be structured very trivially as a simple vector of binary solutions. In fact, the solution to a specific problem may or may not be present. This is, of course, wanting to intend problems in their most isolated sense. So for example, if I call p_1 the Value of Presence of a specific solution, which get 1 value for the presence and 0 for the non-presence, our final evaluation form could be seen as the vector

$$V = (p_1, p_2, \cdots, p_n)$$

This form is pretty unfair for three main reasons: different problems could have the same solution, different solution could be correlated and different solution could have a different weight on the overall security evaluation. Now let us consider some possible strategies to overcome these limitations.
First of all, it may be useful to group together all those problems that have the same solution. In practice, this means that although data collection is extensive and proceeds node by node, solutions must group together problems that are common to several nodes. For example, an update delay affects several nodes at the same time, and this means that there will be multiple problems that nevertheless have a common solution: an update plan. This goes to change our representation from single Value of Presence to macro representations:

$$P_1 = (p_1, p_2, p_3, \cdots) \quad , \quad P_2 = (p_6, p_7, p_8, \cdots)$$

$$V = (P_1, P_2, \cdots, P_n)$$

The second factor to consider concerns the correlation between the various solutions. In fact, they are not only often logically correlated but they may also be consequential. Take as example the upgrade plan for OSs, that may be pursued in parallel with the upgrade plan for individual software. In the same way if think that a solution could be to implement a specific firewall rule I already assume that a firewall is present. For these reasons, another improvement may be to group Values into thematic groups. This not only logically reorganizes the proposed solutions but also makes the result conceptually more understandable to a layman. The modules presented on previous paragraph could be an example of thematic sets which groups solutions

with some affinities.

$$P_A = P_1 + P_2 + P_3 + \cdots \quad , \quad P_B = P_6 + P_7 + P_8 + \cdots$$

$$V = (P_A, P_B, \cdots, P_n)$$

The last necessary step concerns the weight to be given to each solution. In fact, even if someone wants to focus in a binary view of solution and non-solution, he cannot ignore the fact that some elements are more fundamental than others. This attribution of value is certainly the least objective step, as it depends almost more on my personal experience than on a mathematical assessment of the risk. Looking to the future, this will certainly remain the point to work on to aim for greater mathematical rigor. In the next paragraph, I will present my evaluation scale and I will try to justify the choice; meanwhile, our final evaluation vector will have become of the type:

$$W_A = w_1P_1 + w_2P_2 + \cdots \quad , \quad W_B = w_6P_6 + w_7P_7 + \cdots$$

$$V = (W_A, W_B, \cdots, W_n)$$

3.2.3 Tabular representation

The tabular representation I developed in my research is nothing more than a synthesis of the concepts expressed so far. Starting from the division into modules and linking to the idea of solution-oriented vector, I thought the best idea was to consider the three assessments separately, using three vectors of size equal to the number of sub-modules for each assessment. What results are three solution vectors, expressed as V_o, V_s and V_p (recall acronyms in 3.1):

$$V_o = (HC, SC, NC, RS, IR, MO)$$

$$V_s = (SU, KV, PS, NS, ES, AP)$$

$$V_p = (DP, PA, PR, MS, OS)$$

Each component of each vector expresses a value between 1 and 5, which in turn indicates the rounded average of the individual sections that make up each module. The choice of rounding derives primarily from the discrete nature of the assessment, that considers solutions that

are present or not, but also reflects the reality of safety. If we admit that a chain is as strong as its weakest link, the partial implementation of a security measure little differs from the non-implementation of the same. For the same reason the choice to round down results to the nearest integer. I've chosen the range 1 to 5 depending on the fact that I considered it a scale greater enough to express the values I need to show in my analysis. Certainly, a greater number of intervals would allow each point to be expressed more punctually, but at the same time it risks to increase the difficulty of the evaluation. A period of testing can certainly fine tune this value to reach a reasonable balance for the view of a cost-benefit analysis. There is no denying that a future development of this evaluation model is possible. I think that one of the goals of my research is also to be the starting point for more objective and more effective evaluation systems in the future. Similarly, a future improvement could be on solving the one that i think as the main issue of this type of assessment. That's, unfortunately, the inability to distinguish qualitatively two solutions that are substantially similar. For example, in a solution-oriented rating like this, two firewalls that offer the same services would be considered equal. That's happen even if one comes from a larger and more structured company, with good support, larger development team, an history of reliability, and the other comes from a new start-up. Obviously none of these factors guarantees with certainty the superiority of one brand over another, and thinking of adding to the rating scale all these additional variables would certainly make it unmanageable. This does not compromise the purpose of the assessment but, especially from the commercial point of view, this is a lack that could not be ignored. This problem could be overcome by creating a fluctuation between the values of the solutions, perhaps inserting decimals to emphasize the good or bad reputation of one of the implemented brands. This could be a possible solution, but I decided not to include it in this first version of the framework. It might find some space in the graphic representation that I will present later. Now, given a general idea of the vector shape, and the reasons behind that, I must assign a meaning to each value of the vector. By combining each number or range of numbers with a solution of its own, it is possible to create some evaluation tables. These tables serve as a blueprint for the entire assessment process and as templates for standardising the assessment. They can certainly be revised and modified because they derive almost more from my experience than from mathematical objectivity. Nevertheless, they represent an extremely effective and efficient starting point to give a first real understanding of what is the theoretical framework developed so far. Below are the assessment tables:

	OPERATIONAL ASSESSMENT					
	VALUE	1	2	3	4	5
HARDWARE COMPONENT	CPU / MEMORY	SERVER: enough to work	SERVER: enough to grow	CLIENT: enough to grow	modernity	type(CPU instead of GPU...)
	Evaluation of computational power of the company	The company could work but failures and malfunctions are frequent	Computational power is enough to sustain future projects	Redoundancy on client devices	Hardware component is relatively recent, that means it has an higher probability to be supported for many years	The type of devices reflects the best solution for the company's business
	STORAGE	SERVER: enough to work	SERVER: enough to grow	CLIENT: enough to grow	modernity	redoundancy
	Evaluation of hardware used for information storage	The company could work but there is few free storage and few redoundancy	Storage capacity is enough to sustain future projects	Redoundancy on client devices	Hardware component is relatively recent, that means it has less probability to fail	Crucial informations are stored on more than one support
	ALTERNATIVE HARDWARE		usability	reparability	modernity	redoundancy
	Evaluation on particular computing devices such as IoT systems, drones, microcontrollers		The tools are easy to use, not requiring too much training	Devices are easy to maintain, repair, and upgrade	Hardware component is relatively recent, that means it has an higher probability to be supported for many years	Easy to get new devices
SOFTWARE COMPONENT	PRODUCTION SW	usability		reparability		reputation
	Analysis of software needed for the production process	Evaluation of software that considers its effectiveness, difficulty of use, and possible alternatives		Softwares are easy to maintain, repair, and upgrade		The reputation of a software include the updates frequence, CVE patching and widespread
	MANAGEMENT SW	usability			reparability	reputation
	Analysis of software needed to manage personnel and bureaucracy	Evaluation of software that considers its effectiveness, difficulty of use, and possible alternatives			Softwares are easy to maintain, repair, and upgrade	The reputation of a software include the updates frequence, CVE patching and widespread
	OPTIONAL: VIRTUALIZATION	usability			reputation	hyperconvergence
	Analysis of software needed to manage virtual machines and containers	Evaluation of software that considers its effectiveness, difficulty of use, and possible alternatives			The reputation of a software include the updates frequence, CVE patching and widespread	Implementation of hyperconvergence
NETWORK COMPONENT	FIREWALL	troughtput			modernity	high availability
	This section considers the firewall as a tool for network traffic management	Comparing the data throughput of the device with the need of the business, in the case of the firewall also considers the ability to support the necessary vpn connections			It is essential to limit access to the management interface as much as possible	Implementation of High Availability
	SWITCH	troughtput			centralized control	high availability
	Countermeasures to prevent risky behavior on the Web can take various forms based on the different types of protocols that can be controlled	Comparing the data throughput of the device with the need of the business			Consider the ability to scan even encrypted traffic	Implementation of High Availability on core switch
	STORAGE ACCESS		domain	access hierarchy	controlled share	best practices
	This section consider the software limitate access to sensible information that are shared on the network		To implement an internal domain is the most functional and easy way to have a centralized control on devices and users	It is important to create different rights besed on different needs and a hierarchy based on the role in the company	Shared folders must be controlled and organized to preserve at the same time the availability for the employes and the protection of sensible data	Best practice could be to implement hereditary on folders, not share profiles and passwords, organize access on groups and not on individials, exploit GPOs
RESOURCES SUPPLY	CONNECTIVITY	troughtput			stability	backup connectivity
	Evaluation of connectivity provision	Comparing the data throughput of the device with the need of the business			Consider the fact that usally fiber connection is more stable than cable connection that is usually more stable than wireless connection	Implementation of a backup connectivity
	WIRELESS DISTRIBUTION		troughtput	coverage		
	Evaluation of wireless coverage		Comparing the data throughput of the device to the need of the business	Comparing the wireless coverage with the need of the business (result of wireless assessment)		
	ENERGY SUPPLY		UPS	UPS for all fundamentals	strong UPS	modern UPS
	Evaluation of energy provision		Use of alternative energy support	Use of alternative energy support for all crucial devices	Use of an alte energy support with enough capacity to sustain the entire business	Use of modern solutions ensure low risk
INCIDENT RESPONSE	BACKUP TYPE		all fundamentals backup	short retention	long retention	redoundancy
	The first point to consider in evaluating a backup is whether it occurs frequently enough and is maintained long enough		All of the company's core assets have at least one backup	Backups are close enough that not too much crucial information is lost between the current state and the most recent backup	Presence of a backup old enough to ensure a clean restore point (more than 30 days)	Implementation of backup copy
	BACKUP RECOVERY		one day	half day	less than 1 hour	high availability
	The second point to consider for a backup is how quickly it can guarantee a restoration of files		Comparison of speed of recovery with business needs			
	MOBILITY		redoundancy		cloud technology	
	The weakness of a network could be connected also with its physical infrastructure		Possibility to quickly replace elements that have become unusable, considering also the possibility of moving VMs in a cluster		Implementation of cloud services	
MONITORING	MONITORING		traffic monitor	snmp monitoring	rmm	
	Assessment of the company's ability to keep the infrastructure monitored		Implementation of softwares to monitoring packet traffic or devices state	Implementation of softwares to monitoring network elements through snmp protocol	Implementation of softwares for remote monitoring and management	
	LOG SOFTWARE		personal accounts	logging software / SIEM		
	Implementation of logging systems		Use of personal accounts for personal accountability monitoring	Use of software to collect and analyze data from all the possible sources on the network		
	PHYSICAL SECURITY		dedicated location	simple access controll	surveillance	badge/personal identification
	Implementation of procedures to control physical access to the infrastructure		To have dedicated location for IT crucial devices make it easier to control them, to repair them and also to protect them	Security based on physical keys and dedicated staff	Security based on monitoring, with people or cameras	Implementation of more secure technologies as badges or biometrical identification

Figure 3.1: Evaluation criteria table for the Operational Assessment

	SECURITY ASSESSMENT					
	VALUE	1	2	3	4	5
SOFTWARE UPDATE	UPDATE OS		high risk	high severity	66% updated nodes	all nodes updated
	Evaluation of critical issues present on device operating systems		Presence of CVE with an high score on EPSS scale	Presence of CVE with an high score on CVSS scale	A high number of devices are up to date	Good update policy
	UPDATE SW		high risk	high severity	66% updated nodes	all nodes updated
	Evaluation of critical issues present on the software employed by the devices		Presence of CVE with an high score on EPSS scale	Presence of CVE with an high score on CVSS scale	A high number of devices are up to date	Good update policy
	DISMISS OS / SW	exposed	interconnected	crucial	not replacable	no dismissed OS
	Evaluation of the critical issues present on those devices that for various reasons (lack of support, hardware too old, ...) do not have the possibility to be updated	The unsupported element is exposed outside the network	The no longer supported element is not isolated from the rest of the network	Without such a device, the company's business is compromised	The element cannot be replaced with a safer alternative	No dismissed OS
KNOWN VULNERABILITIES	INTERNAL SERVICES		not legitimate software	no weak protocols	no injection vulnerabilities	
	Some services known to be risky from an insider threat perspective are used within the network		the usage of not legitimate software could lead to problems due to the untrusthness of it	Trasmission services as NETBIOS, SMB v1 or SNMP v1-v2 could spread over the network crucial information unencrypted	There are no vulnerabilities related to failure to sanitize data entry	
	EXTERNAL SERVICES		no sensible ports exposed	no informations exposed	no injection vulnerabilities	
	Services exposed to the Internet have known vulnerabilities		Exposed ports that should not be, although not vulnerable, may prove risky in the long run	Security-sensitive information could be unknowingly made public (on the company's website, in social profiles, on online photos, ...)	There are no vulnerabilities related to failure to sanitize data entry	
PERIMETRAL SECURITY	FIREWALL		dedicated LAN rules	dedicated protocol rules	bound IP access	strong VPN
	This section considers the firewall as a tool for network segmentation and filtering traffic between subnets		Segmenting the network into different subnets with specific access rules helps control interactions and isolate crucial nodes	An additional step forward involves limiting the flow of data to known and used protocols	It is essential to limit access to the management interface as much as possible	Strong communication protocols
	WEB TRAFFIC		web filtering	proxy	SSL inspection	IDS/IPS
	Countermeasures to prevent risky behavior on the Web can take various forms based on the different types of protocols that can be controlled		Consider the ability to restrict access to unwanted sites or, even better, limit it to only those that are necessary	Consider the ability to scan unencrypted traffic	Consider the ability to scan even encrypted traffic	Service analysis of network traffic as a whole with the ability to automate countermeasures
	MAIL		DKIM / DMARC / email encryption		anti spam	advanced email security
	The most common but also most effective attacks often originate from email traffic, as it is the main form of exchange with external		DKIM and SPF help to demonstrate legitimacy, DMARC tells mail servers what to do when DKIM or SPF fail, cryptography could be necessary on some context		An anti-spam service help on prevent undesired mail traffic analysing the overall behaviour on the company and outside it	Advanced mail security considers also all these countermeasures that are not connected with mail traffic but that are correlated with it, as for example sandbox analysis, redirection prevention
NETWORK SECURITY	SEGMENTATION		managed switches	VLANs	secured trunks	monitored traffic
	This section considers in detail the ability to maintain the division between subnets across the entire network and not only considering the flow through the firewall		Consider the ability to control the traffic in a structured way	Consider the logical division on different subnets which must not share packets between them	Consider the fact that sometimes trunks between switches are set to allow all the traffic, letting a man-in-the-middle attack to sniff all the traffic	Implementation of policies or software that are able to collect data from the network and alert in case of suspicious behaviour
	STORAGE ACCESS		domain	access hierarchy	controlled share	best practices
	This section consider the software limitate access to sensible information that are shared on the network		To implement an internal domain is the most functional and easy way to have a centralized control on devices and users	It is important to create different rights besed on different needs and a hierarchy based on the role in the company	Shared folders must be controlled and organized to preserve at the same time the availability for the employes and the protection of sensible data	Best practice could be to implement hereditary on folders, not share profiles and passwords, organize access on groups and not on individials, exploit GPOs
	OPTIONAL: SIGNING		sign software / sign usage		signing security	
	Implementation of digital signature for documents or scripts	Evaluation of the signature application process considering whether and how that process is used			Evaluation of the algorithm used for digital signature	
ENDPOINT SECURITY	ENDPOINT PROTECTION		USB protection	antivirus	behavioural analysis	
	Consider the countermeasures implemented to avoid software compromise		To prevent internal intrusion of malicious software	Consider the implementation of a software able to detect and delete malicious code executed on the device	Consider the implementation of a software that is able to analyze the overall behaviour to detect also malicious exploitation of allowed software	
	BACKUP POLICY		scheduled backup	long retention policy / encrypted backup / multiple backups		
	Consider the countermeasures implemented to recover devices after an incident		Consider the implementation of some kind of backup on crucial devices	The backup must have long retention policies (average intrusion time is over 30 days) and could be more secure implementing encryption and multiple copies		
	APP CONTROLL		screensaver	only trusted software(CVE)	app denied	app allowed
	Countermeasures to prevent the usage of unsecure apps		The endpoints are suppose to be blocked when an employee leave, even for shot breaks	The software used by the company enjoys a certain reputation	The usage of certain applications is denied inside the company	Employees only can use the software approved by the company
ACCESS PROTOCOLS	PASSWORD SECURITY		no breached password		no transcription of password	password manager
	Assessment of password complexity and theft risk		Passwords already leaked in some data breach are not used		there are no post-it or text files unencrypted that contains the crucial passwords	the company use a third software to encrypt and protect the passwords
	PASSWORD POLICY		expiration date	password evaluation(strong, easy to remember, no shared)		
	The password policy must be the first and most important protocol on a company to prevent any kind of intrusion		Every strong password could be cracked with enough computational power and enough time so a password with no expiration date is inherently weak	A good password must be strong (long, with letters, numbers, special characters) but also in some way easy to remember (implementing words or simil words) because too difficult password leads people to write them down on paper sheets and text files compromising their efficacy		
	PHYSICAL SECURITY		dedicated location	simple access controll	sourveillance	badge/personal identification
	The weakness of a network could be connected also with its physical infrastructure		To have dedicated location for IT crucial devices make it easier to control them, to repair them and also to protect them	Security based on physical keys and dedicated staff	Security based on monitoring, with people or cameras	Implementation of more secure technologies as badges or biometrical identification

Figure 3.2: Evaluation criteria table for the Security Assessment

	PERSONNEL ASSESSMENT					
	VALUE	1	2	3	4	5
DESIGNED PERSONNEL	IT MANAGER	skills		budget	experience on the company	vision / developement plan
	IT manager is the figure in charge of IT infrastructure maintenance and development	Assessment of the IT manager's skills, taking into consideration educational qualifications, certifications, previous work experience		Evaluation of the budget allocated for IT is one of the elements to be considered in development and improvement	Experience in the company ensures a better overall view of needs and wants	Considerations on abilities and improvement proposals
	EXTERNAL SUPPORT	skills		budget	experience on the company	timely intervention
	Evaluation of external support related to the IT infrastructure	Assessment of the capabilities of external support in relation to the situation presents in the company and the reputation of the support		Evaluation of the budget allocated for IT is one of the elements to be considered in development and improvement	Experience in the company ensures a better overall view of needs and wants	Key evaluation criterions for external interventions are timing and cost
PERSONNEL AWARENESS	WORKERS		update awareness	web awareness	software awareness	password awareness
	IT awareness of the employees		Awareness of the importance of keeping software updated and the procedures to do so	Awareness of the dangers of the web and how to avoid them	Awareness of the use of the company's main software	Awareness of the importance of a password and best practices
	USER PROTOCOL		enrollment procedure	access control	log collection	data protection
	Protocols governing the creation and management of IT infrastructure users		Procedures for onboarding and offboarding users	Role-based access control implementation	Logging and monitoring of user activities	Guidelines for data retention and secure disposal
PROTOCOLS	PASSWORD POLICY		no expiration date	password evaluation(strong, easy to remember, no shared)		
	The password policy must be the first and most important protocol on a company to prevent any kind of intrusion		Every strong password could be cracked with enough computational power and enough time so a password with no expiration date is inherently weak	A good password must be strong (long, with letters, numbers, special characters) but also in some way easy to remember (implementing words or simil words) because too difficult password leads people to write them down on paper sheets and text files compromising their efficacy		
	ASSET PROTOCOL		only company hardware	asset inventory	only trusted software(CVE)	app control
	Protocols governing the use of company IT material		Employees do not use company software outside of the devices provided by the company itself	An inventory is present that tracks the use of company assets	The software used by the company enjoys a certain reputation	Employees only can use the software approved by the company
MAIL SECURITY	PHISHING AWARENESS	evaluation over phishing campain				
	A phishing campaign test assesses an organization's susceptibility to fraudulent email or communication attempts	The assessment considers employees' ability to recognize, avoid, and report suspicious emails				
OSINT	OSINT	evaluation over osint				
	OSINT refers to the collection and analysis of publicly available information from sources like social media, websites, and other open platforms to gather intelligence or insights.	The process searches and analyzes all publicly available information about a company, highlighting its critical points				

Figure 3.3: Evaluation criteria table for the Personnel Assessment

3.2.4 OSP or ACI

As emphasized above I realized that the classification of the framework proceeded by embracing the construction of the process more than the desire for knowledge of the client. Certainly the modularity of services is an important element in terms of sales, but if I have to consider the idea of asking for a check in terms of standardization, it is easier than the request goes towards a different display form. Embracing this idea I was interested about the possibility of combining the data extracted from the three analyses to create an exhibition form closer to the requests of customers, who are very often affectionate to ACI. The ACI triad (Availability, Confidentiality and Integrity) is a cornerstone model in cybersecurity that provides a comprehensive yet straightforward framework for understanding and addressing information security challenges. This paradigm is highly effective for structuring cybersecurity presentations due to its all-encompassing nature and accessibility to both technical and non-technical audiences. By focusing on these three key principles, presenters can cover the essential aspects of data protection: keeping information private (Confidentiality), ensuring its accuracy and trustworthiness

(Integrity), and guaranteeing access for authorized users when needed (Availability). This approach allows for a balanced discussion of security measures, facilitates risk assessment, and helps in prioritizing security efforts. In the following representation a redistribution of the table entries is shown to readjust them to the ACI subdivision. To highlight the origin items have been highlighted with colors based on if they are derived from operational assessment (red), security assessment (green), personnel assessment or attributable to a combination of several assessments (blue).

	AVAILABILITY					
	VALUE	1	2	3	4	5
HARDWARE COMPONENT	CPU / MEMORY	SERVER enough to work	SERVER enough to grow	CLIENT enough to grow	modernity	type
	STORAGE	SERVER enough to work	SERVER enough to grow	CLIENT enough to grow	modernity	redoundancy
	ALTERNATIVE HARDWARE		usability	reparability	modernity	redoundancy
SOFTWARE COMPONENT	PRODUCTION SW	usability			reparability	update frequence
	MANAGEMENT SW	usability			reparability	update frequence
	OPTIONAL: VIRTUALIZATION	usability			reputation	hyperconvergence
NETWORK COMPONENT	FIREWALL	troughtput			modernity	high availability
	SWITCH	troughtput			centralized control	high availability
RESOURSES SUPPLY	CONNECTIVITY	troughtput			stability	backup connectivity
	WIRELESS DISTRIBUTION	troughtput			coverage	
	ENERGY SUPPLY		UPS	UPS for all fundamentals	strong UPS	modern UPS
INCIDENT RESPONSE	BACKUP TYPE		all fundamentals backup	short retention	long retention	redoundancy
	BACKUP RECOVERY		one day	half day	less than 1 hour	high availability
	MOBILITY		redoundancy	virtualization		cloud technology
	CONFIDENTIALITY					
	VALUE	1	2	3	4	5
CRYPTOGRAPHY	OVER COMMUNICATION		SNMP encryption	email/messages encryption	remote access app	VPN security
	OVER STORAGE		storage encryption		backup encryption	
PERIMETRAL SECURITY	FIREWALL		dedicated LAN rules	dedicated protocol rules	bound IP access	strong VPN
	WEB TRAFFIC		web filtering	proxy	SSL inspection	IDS/IPS
	MAIL		DKIM / DMARC / email encryption		anti spam	advanced email security
NETWORK SECURITY	SEGMENTATION		managed switches	VLANs	secured trunks	monitored traffic
	STORAGE ACCESS		domain	access hierarchy	controlled share	best practices
ACCESS PROTOCOLS	PASSWORD SECURITY		no breached password		no transcription of password	password manager
	PASSWORD POLICY		expiration date	password evaluation(strong, easy to remember, no shared)		
	ASSET PROTOCOL		only company hardware	asset inventory	only trusted software	app control
KNOWN VULNERABILITIES	INTERNAL SERVICES		not legitimate software	no weak protocols	no injection vulnerabilities	
	EXTERNAL SERVICES		no senisible port exposed	no informations exposed	no injection vulnerabilities	
OSINT	OSINT	evaluation over osint				
MAIL SECURITY	PHISHING AWARENESS	evaluation over phishing campain				
	INTEGRITY					
	VALUE	1	2	3	4	5
SOFTWARE UPDATE	UPDATE OS		high risk	high severity	66% updated nodes	all nodes updated
	UPDATE SW		high risk	high severity	66% updated nodes	all nodes updated
	DISMISS OS / SW	exposed	interconnected / not replaceable		crucial	no dismissed OS
ENDPOINT SECURITY	ENDPOINT PROTECTION		encrypted storage	antivirus	network analysis	behavioural analysis
	BACKUP POLICY		scheduled backup	long retention policy / encrypted backup / multiple backups		
NETWORK SECURITY	OPTIONAL: SIGNING		sign software / sign usage		signing security	
MONITORING	MONITORING		virtualization	domain	snmp monitoring	rmm
	LOG SOFTWARE		personal accounts	logging over access	logging software / SIEM	
	PHYSICAL SECURITY		dedicated location	simple access controll	sourveillance	badge/personal identification
ACCESS PROTOCOLS	PASSWORD SECURITY		no breached password		no transcription of password	password manager
	PASSWORD POLICY		expiration date	password evaluation(strong, easy to remember, no shared)		
	ASSET PROTOCOL		only company hardware	asset inventory	only trusted software	app control
PERSONNEL AWARENESS	WORKERS		update awareness	web awareness	software awareness	password awareness
	USER PROTOCOL		enrollment procedure	access control	log collection	data protection

Figure 3.4: Reorganised ACI classification criteria table.

3.2.5 Numerical representation

The idea of a numerical representation comes from the desire to condense the multiple values from the vectorial representation into a single meaningful number. Obviously it leads to lose some information, but it can still represent some crucial points. Already by itself, the vector has the ability to show quite clearly strengths and weaknesses of an infrastructure. For example, a security assessment that returns

$$V_s = (3, 3, 5, 4, 1, 3)$$

represents a solid and well protected network, with unprotected endpoints, so overall a strong infrastructure against external attacks but weak against internal threats. Starting from this kind of representation the most obvious idea of overall evaluation could be simply to take the average of the values, or their sum. Such representation would certainly effectively show the distance between a good and a bad infrastructure but would not consider the variability of these values. Especially in the area of security it is impossible not to consider the fact that even one particularly deficient could have negative consequences on the entire infrastructure. Always referring to the metaphor of the chain, two infrastructures like the following

$$V1_s = (3, 3, 3, 3, 3, 3)$$

$$V2_s = (5, 5, 5, 1, 1, 1)$$

show an equal sum and average, but while one represents fair coverage in almost all sectors, the other represents excellence but also extremely risky gaps. In order to address this issue the evaluation must consider also the variability in the form of variance or, even better, standard deviation. Since a high standard deviation represents a deficit for our network, it would be reasonable to consider it as a negative value. Since I wanted to work exclusively with positive factors, again for the sake of simplicity, I preferred to replace the negative value of the standard deviation by another factor, i.e.

$$\sigma_{pos} = \sigma_{max} - \sigma$$

where σ_{max} indicates the maximum possible standard deviation. This value is calculated trivially considering that the vector of maximum standard deviation is always the vector with half minimum values and half maximum. Given n as number of values, M as maximum value, m

as minimum and μ as vector average, we obtain

$$\mu = \frac{M \cdot \lfloor \frac{n}{2} \rfloor + m \cdot \lceil \frac{n}{2} \rceil}{n}$$

$$\sigma_{max} = \frac{\lfloor \frac{n}{2} \rfloor \cdot (M - \mu)^2 + \lceil \frac{n}{2} \rceil \cdot (m - \mu)^2}{n}$$

After that I considered as necessary to provide a multiplicative factor n_{std} to balance the standard deviation in relation to vector average, a value that was intended to be combined to. Given that the evaluation become

$$E = V_{avg} + n_{std} \cdot \sigma_{pos}$$

Having defined the contribution of variability, I wanted to add another factor to highlight another aspect. In fact, regarding the solutions adopted by a company, we can observe that with the growth of complexity and cost for a solution, there is also a proportional reduction of the gains in terms of effectiveness. This is not to say that the most expensive solutions are not worth the cost, but rather to emphasize how the simplest and most basic implementations, even if small, represent a huge advance compared to their absence. The progress from a simple firewall to a firewall with an IPS system, however effective, is not comparable to the transition from not having a firewall to having one. In this sense, the last steps represent the intention to achieve a certain standard, while the former represent the foundations of a secure and efficient infrastructure. To highlight also mathematically this point I thought that a good method could be to value more the first steps compared to the last ones. One way to do this, what I finally decided to do, is to apply a root to the evaluations before calculating the average. This, following the trend of the root function, will penalize the higher numbers proportionally to the exponent n_{exp}. Taking note of the latter consideration, the numerical representation of the assessment should appear as follows:

$$V_{sqrt} = \sum_{x=1}^{6} \frac{\sqrt[n_{exp}]{V_x}}{n}$$

$$E = V_{sqrt} + n_{std} \cdot \sigma_{pos}$$

A number that could be normalized as a number between 0 and 100 computing the maximum and the minimum value for each type of vector. With $n_{std} = 0.2$ and $n_{exp} = 1.5$, we get for example

$$V = (5, 4, 2, 2, 1, 1) \rightarrow V_{avg} = 2.5 \quad \sigma_{std} = 1.5 \; E = 32$$

$$V = (3, 2, 2, 2, 2, 2) \rightarrow V_{avg} = 2.16 \quad \sigma_{std} = 0.37 \quad E = 32$$

$$V = (5, 5, 5, 5, 2, 5) \rightarrow V_{avg} = 4.5 \quad \sigma_{std} = 1.11 \quad E = 83$$

$$V = (4, 4, 4, 4, 5, 5) \rightarrow V_{avg} = 4.33 \quad \sigma_{std} = 0.47 \quad E = 84$$

As desired a higher variability penalize the evaluation and this gap is greater for low values than for greater ones. Obviously I cannot be sure this is the best combination for n_{std} and n_{exp} values, but the estimation could be improved with experiments and trials over time. For now this numerical representation is enough for the first attempt of framework I'm trying to structure.

3.2.6 Graphical representation

For the graphical representation of my evaluation, the starting point was certainly the Gartner quadrant. The Gartner Quadrant, known as the Gartner Magic Quadrant, is a graphical representation tool developed by the consulting firm Gartner to present the competitive positioning of companies in a given technology sector. It works through a two-dimensional matrix that evaluates companies according to two main criteria: the "vision" on the horizontal axis and the "ability to execute" on the vertical one. Its strength lies in making immediate and almost trivial the result of an extremely detailed and complex market analysis. In the case of the framework under consideration, the need becomes to represent not only two evaluation criteria but at least five or six sub-modules that coexist within the same assessment. To satisfy this need my choice has therefore moved from what is a simple Cartesian plan to another type of graph, the radar chart. I found this to be the most reasonable type of chart for multiple reasons. The first is certainly the possibility of representing a greater number of criteria at the same time, allowing in the case of assessments to show the entire vector of solutions. The second reason follows what is the paradigm of evaluation oriented to solutions because it allows to represent in the same graph two evaluations simultaneously. In this way it is possible to show the evolution of an infrastructure from before to after an intervention, or to present new implementations with a view on expanding the graph in one direction instead of the other. To conclude, the graph

tends to penalize concave figures because of its representation based on the area of a polygon, and therefore follows the idea that a uniform distribution of solutions is preferable to a polarization. In addition to this, wanting to find out other positives, we can also add a way to represent the quality of a solution. As mentioned in paragraph 3.2.3, the lack of representation of solution trustworthiness is one of the main issues of tabular representation. Contrarily the graphical representation being less formal and mathematically defined, could leave space for intermediate values. Values as 3 or 4 could be transformed into 3.5 or 4.5 to underline that the proposed solution does not offer anything more than the previous one from a quantitative point of view but that certainly offers guarantees of a higher quality. Some Examples of such representation may include the following:

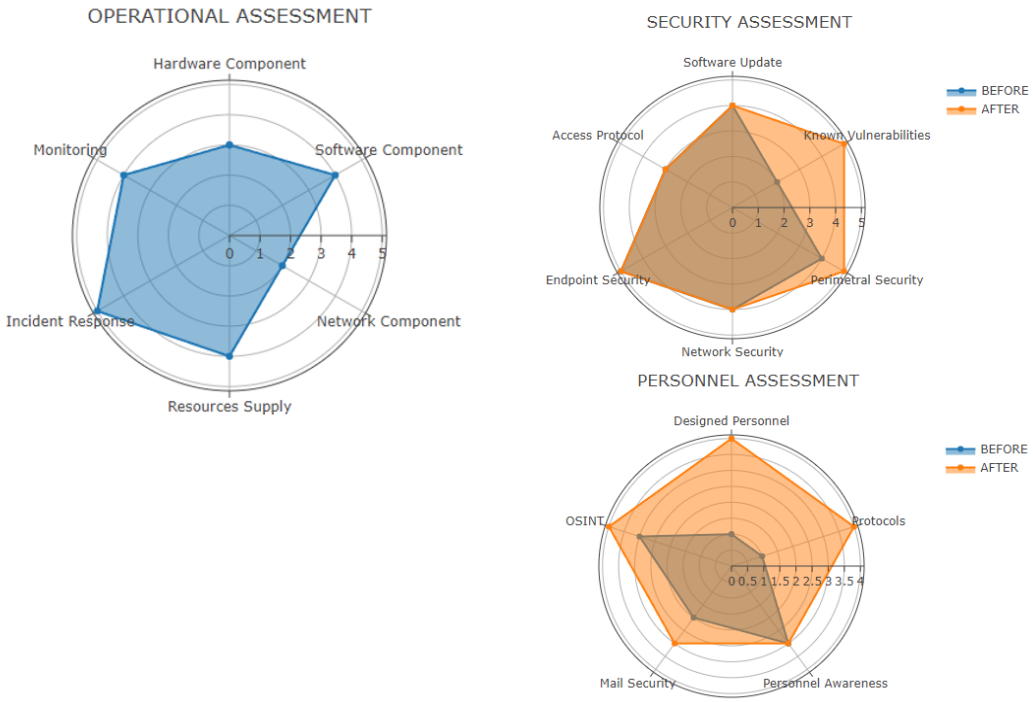


Figure 3.5: Example of implementation of graphical evaluation. On the left is the result of an operational assessment in which the hardware and network components are significantly sacrificed compared to the rest. On the right, two graphic representations of a remediation plan, in which the current condition is shown in blue and the prospect of improvement in orange.

4

Comparing Alternatives

Since the beginning of my experience in Solunet I had the opportunity to test and evaluate the validity of this solution but unfortunately I could not do it enough times to be able to group effective statistics. To try to evaluate frameworks I thought I would compare it with some of the most popular alternatives. As stated at the beginning of my thesis, it is really rare to find in literature frameworks with the same focus for which I have structured mine. There are a number of alternatives, obviously different in detail but similar in many respects and from which I can obtain interesting terms of comparison.

4.0.1 Cyber Essential (UK)

Cyber Essentials[27] is a UK government-backed certification scheme designed to help organizations protect themselves from a wide range of common cyber attacks. It provides guidance and sets out basic security measures particularly for SMEs. It is presented as a list of recommendations for self-assessment, which can then be tested by certified personnel. It focuses on 5 main points: Firewalls, Secure Configuration, Security Update Measurement, User Access Control, Malware Protection.
It is a relatively simple assessment process. It takes into account a few points and tries to concentrate on its main function more than to observe every possible flaw. In this sense it could be described as a partial assessment, an attempt not to ensure the result but rather to allow anyone to start the process. It is not by chance that the first part presents itself as a self-assessment.

In its implementing rules, it focuses heavily on the redistribution of responsibilities. In all guidelines, it tries to create a clear separation between what is the responsibility of the employee, of the company or of the software used. It makes a deep reflection on the implications of using corporate material outside the company's perimeter and on smartworking. It even takes into account the differences between software services presented as IaaS, PaaS and SaaS.
From a comparative point of view, the Cyber Essential, like my framework, seeks to approach the limits of SMEs by reducing the complexity of the process. In its case, however, the balance is perhaps too much on the side of simplicity, obviously hoping to reach as many audiences as possible. The factors considered are few, the division is approximate and even if partially effective (it declares that in this way organizations can protect themselves from 80% of common cyber threats) not suitable for an exhaustive research as that objective of this thesis.

4.0.2 Cyber security guide for SME (Belgium)

As in the previous case, also in the Cyber security guide for SME[28], developed in Belgium, what is presented is essentially a list of points to be considered. Compared to the Cyber Essential it develops in many more points (12) and considers a wider spectrum of considerations. The following are the titles of the modules:

- Involving top management
- Publish a corporate security policy and a code of conduct
- Raise staff awareness of cyber risks
- Manage your key ICT assets
- Update all programs
- Install antivirus protection
- Backup all information
- Manage access to your computers and networks
- Secure workstations and mobile devices
- Secure servers and network components
- Secure remote access
- Have a business continuity and an incident handling plan

In this case the guidelines are more developed, also including business continuity and incident response. In addition, each point is presented with a gradation, although relatively simple. For each module, two perspectives are presented, one as ”basic protection” and the other as ”advanced protection”. This is fundamental because it allows companies to approach a problem gradually, without demanding the maximum result in the first instance.
Here too, however, some shortcomings are evident. The assessment is completely out of line with the needs of the company and instead only considers absolute entities. The division into two levels is surely not enough for the great diversity on SMEs. From an operational point of view it also develops even less than the Cyber Essential, presenting only generic guidelines and no testing methodology.

4.0.3 CIS Controls

The Center for Internet Security has introduced a further refined rating standard. This classification groups 20 different thematic groups, which comprehensively cover almost every aspect of a company's IT infrastructure, including personnel.

Figure 4.1: The 20 modules that form the core of the CIS.

In addition to the modules, it also introduces a methodology for approaching the assessment process. It divides each analysis into three phases: know, protect and prepare. The three ways describe the need to keep an inventory, to consider cybersecurity as a fundamental paradigm and finally to be prepared in case of accidents[29]. The guide is very detailed and also provides further documentation with a series of tests and procedures to ensure compliance with each module. Compared to the previous framework, this not only expands the number of modules

but also deepens each one by defining sub-categories and a system of graded evaluation. Most scores, in fact, are expressed as a percentage of achievement within the infrastructure and for each test, appropriate tools for data collection are also presented[2].
The CIS approach is certainly the one that most closely resembles the framework presented in this thesis. Its definition is exhaustive, the practical implementation clear and detailed. However, there are two main weaknesses of this framework. First, this framework, like the previous ones, does not take into account the needs and priorities of the infrastructures it analyses, coming to set standards rather than priorities. This is obviously consistent with its role, which is to define a standard and not to present a development plan. Its second weakness is that each module and subcategory are presented with the same value despite having a different impact on the risks of the firm. Modules are difficult to group into sub-services, which I was interested in developing in my framework, and in general little space is left for the evaluation of staff. However, the emphasis on policy-making practices must be appreciated.

4.0.4 National Institution for Standard and Technology

Despite being the most dated of the frameworks presented I thought it is important to also report on NIST for some of its peculiarities. In the implementation of Celia Paulsen and Patricia Toth[7], in particular, a reflection on the peculiarities of small and medium-sized enterprises and their fragility is presented. It emphasizes the importance of remediation more than other frameworks and it is the only one that seems to really accept the limitations of SMEs. It extends the research phases to five: identify, protect, detect, respond and recover. This is important because it does not only focus on what is the best scenario (protect and recover) but accepts the possibility of having to go down a compromise (detect and response). It thus embraces the philosophy that a problem in SMEs cannot always be solved but can be circumvented or mitigated.
From the implementation point of view, it is very similar to CIS, although it is less detailed in each module. It is also quite inadequate from the point of view of practical guidelines. In some ways it almost resembles more a guide to creating a consistent framework than the definition of a new specific one.

Control Category	Cyber Essentials (UK)	The Centre For Cyber Security Belgium SME Guide (Belgium)	Center for Internet Security (CIS) (Europe)	NIST Small Business Information Security (USA)	OSP
Management commitment and policies		X		X	X
Asset Management		X	X	X	X
Patch Management	X	X	X	X	X
Access Control	X	X	X	X	X
Secure Computers, Servers and Network Configuration	X	X	X	X	X
Log Management			X	X	X
Email and Web Security			X	X	X
Malware Protection	X	X	X	X	X
Network and Communications Security	X	X	X	X	X
Back-up and Recovery Management		X	X	X	X
Data Protection and Encryption			X	X	X
Awareness and Training		X	X	X	X
Secure Development			X		
Incident and Continuity Management		X	X	X	X
Human Resource Security			X	X	X
Improvement and Compliance				X	
Supplier Relationships					

Figure 4.2: Comparative table presented by Ozkan and Spruit in 2021[1]. It highlights the macro topics considered in the frameworks just presented. The framework presented in this thesis was added as last column.

4.0.5 Emer-Untherhofer-Rauch Framework

This framework was proposed in 2021 by four researchers from the Free University of Bolzano. It focuses on the evolution towards Industry 4.0 and the technologies that this paradigm brings with it. From the point of view of the assessment approach, this framework is divided into four levels numbered 0 to 3: prerequisites, security management and maintenance, fault management, network management and maintenance. It is evident that this solution, unlike the others, was born not as a standardization but as a solution for companies, especially because the first point is focused on the study of the customer. In "prerequisites" the peculiarities and needs of the case are analysed and studied in order to calibrate the following modules. In the other modules, you will learn more about all other aspects of IT infrastructure.
Its industry 4.0 orientation is evident from the fact that the evaluation is entirely structured on the evaluation of individual technologies and how they are implemented. In practice, the proposed framework first defines a list of technologies that a customer needs, then defines a "maturity" scale to judge its implementation, and then groups these technologies into thematic modules.
The strengths of the framework are certainly the attention to the specific case, therefore its

adaptability, and the great rigor with which it allows to classify and evaluate each applied technology. Although it may seem less intuitive than the previous one, it appears much easier to implement since it is oriented towards individual technologies, but at the same time it does not lose the possibility of grouping evaluations among them. It also develops a method of representation very similar to the radar chart presented on my work, the spider chart. Which is quite similar but only placing emphasis on the value of each single evaluation without attaching particular importance to the area described.

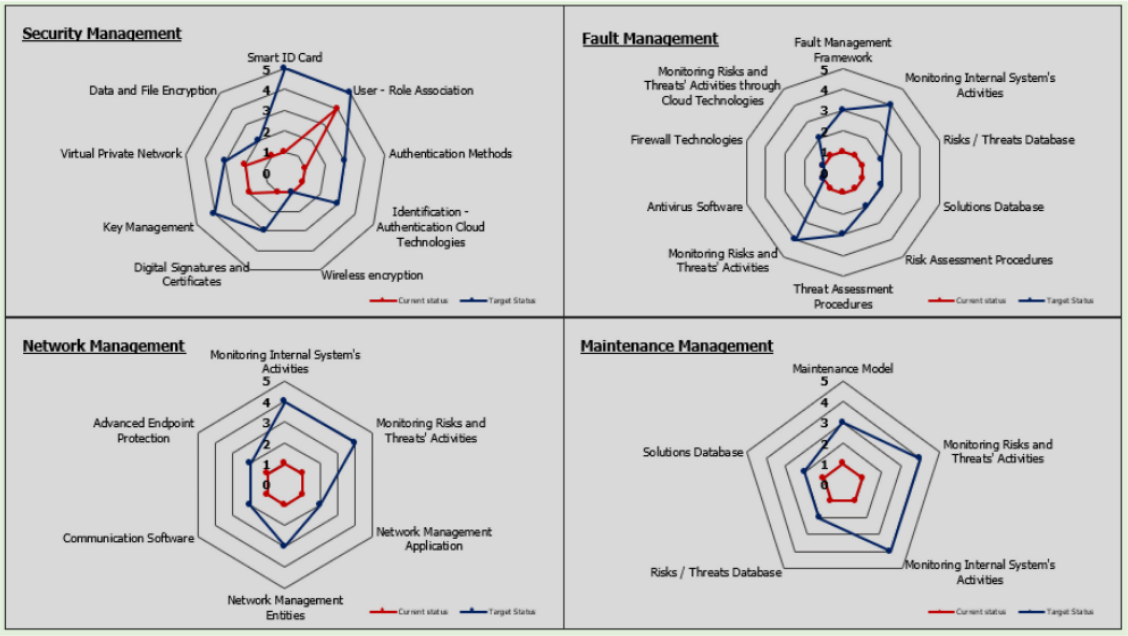


Figure 4.3: Spider chart visualization of the cybersecurity gaps between current and target levels of cybersecurity for security, fault, network and maintenance management areas[2].

The result makes it extremely understandable on which technologies to invest and on which instead it has reached an acceptable level, but although it is well suited according to the remediation plan, it says very little about the current state of the company. Each technology has the same weight despite different impacts on the company and there is no correlation between solutions that interact with each other or compensate for each other's shortcomings. It should also be pointed out that the personnel factor is totally neglected[2].

4.0.6 Final thoughts

It is clear that starting from different premises and objectives leads to different implementations. It is equally clear that intrinsic differences make it very difficult to carry out a comparison which is in some way objective. It follows that is not possible to see my work as an improvement of these previous frameworks. It embraces certain concepts but does not propose itself as a new improved version but only as a new declination to solve a different problem in a different context. From the analysis of the frameworks it is understood that no previously proposed solution presents all the characteristics I was looking for. Instead theoretical framework presented in the previous chapter is built in a way that overcome their shortcomings. This does not mean that it is perfect, nor it is complete. But it only means that it reflects, at least in form, all my expectations. The three modules consider equally the efficiency, safety and skills of the staff, adapting the evaluations of sub-modules to the impact on the company. For some evaluations a degree of maturity is expressed, for others one of consequentiality, for still others the evaluation is weighted with the needs of the company.
The only point which has not yet been explored is how this theory can be applied in practice. This means not only showing a method for collecting data. It means to structure a work plan that is as modular and efficient as possible, respecting both the need to divide large analyses into simpler and replicable processes but also to combine in the smallest number of interventions the greater number of data collected.

5

FRAMEWORK IMPLEMENTATION

The theoretical definition of objectives and form is just a first step before the development of an action plan. In this section I will try to present a set of tools which can be combined to extract all the information needed to arrive at the assessment described above. It is important to underline how this is not the only way, nor the best way. Everything is structured using the software and hardware tools provided to me by the company, without the desire to advertise them or claim that they are the best solution. I thought it was important to specify this in the name of the universality of the framework, which is set up with the desire to make it applicable in as many contexts as possible. Another important premise to make is that performing an assessment of this nature means having full access to a client's infrastructure, with all the risks it carries. It may seem a paradox but the path taken to protect your company involves lowering your defenses against an external organization. The company carrying out an assessment has the chance to interrupt the work of a company, to steal private information or intellectual property, to compromise defenses in the perspective of a future attack. This means that from a practical point of view the first step of the implementation concerns the safety, both on bureaucracy and practice, of the customer. The risks of the procedure must be presented and all preventive measures must be guarantee. This may include advice to work towards changing the credentials and access provided to operators at the end of the assessment process.

Having made the necessary preconditions, I now present some of the steps that may be useful during an assessment and the data that each of them allows to collect. For greater clarity I decided to divide the phases of the analysis following the order in which they are administered

to the customer. This led me to distinguish the assessment in three basic phases: direct data collection, automatic data collection and internal solution analysis. The first describes the data collection phase that takes place physically in the company requesting the assessment and which therefore consists of a direct data collection by the operator on site. The second describes some tools capable of collecting and parsing data in a semi-autonomous way once installed within the infrastructure. Finally, the third phase deletes the main configurations to be investigated in the tools already implemented by the company. I have finally grouped in a last category (which for convenience I called "other") those analyses related mainly to personnel assessment and that do not fall into the categorization just explained.

5.1 Direct Data Collection

5.1.1 Inspection

Each assessment begins with an inspection of the company to be analysed. In general, in most cases the analyses can be done remotely by simply inserting a device into the network that can act as a bridge for technicians to access the network. On the other hand, the presence is important to judge all those aspects of functionality and safety related to the structure that hosts the company. Security of the CED and the distribution cabinets, positioning the video surveillance, unsupervised access, are all features that can be deduced from the floor plan but that require a site inspection to confirm. On the contrary, there are analyses that must be carried out on site, such as the analysis of the wireless network. It requires sampling of frequencies in strategic locations of the company and, if necessary, also a study of the interference of various obstacles. Here too, it is important to assess the cost-benefit balance. A simple analysis, made with a simple site survey and frequency analysis software can take a few hours but give extremely limited results. On the contrary, a thorough approach with specialist equipment (wide-spectrum antennas) and simulation software can take longer and require a considerable economic investment. The choice will then depend on the needs of the company, which may rely on wireless networks to provide connectivity to production machinery or IoT tools for monitoring. Network security is not taken into account because it belongs more to the world of configurations which will be analysed later.

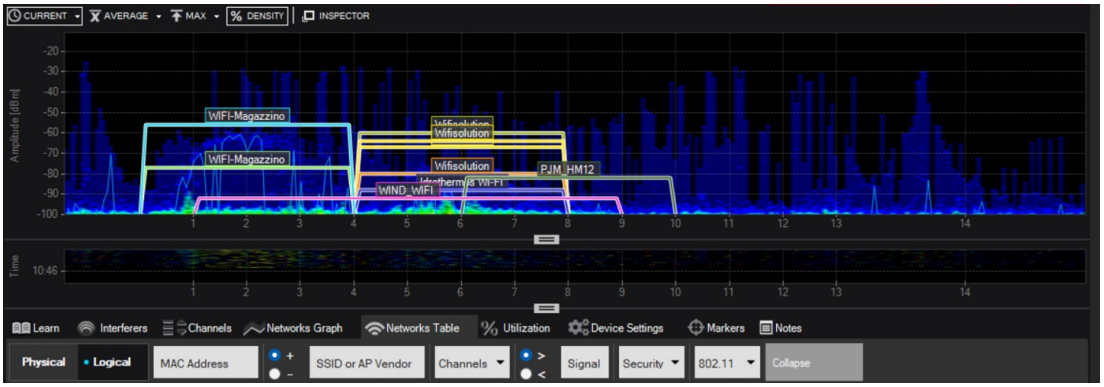


Figure 5.1: Example of wireless sampling performed with a laptop antenna, without the help of specialized tools. In this particular case, the company had no specific needs other than to ensure a decent signal in the production area.

5.1.2 Interview

The interview phase is primarily necessary to collect information owned exclusively by the company's staff, such as industrial needs and growth prospects, or by IT personnel, such as credentials and corporate policies. All other information can be derived from straight lines using other survey methods. However, the purpose of the assessment is not to proceed blindly but to obtain a complete view of the network. The interview will therefore be used to extract as much information as possible about the infrastructure. From a practical point of view, it could be said that in the case of an exhaustive interview, most of the analyses carried out subsequently would become more confirmatory than investigative processes. This approach allows to understand the actual awareness of the customer about their infrastructure. It is not uncommon that the results of the interview and those of the surveys do not match, emphasizing even more phenomena such as the lack of adequate policies or monitoring systems.

5.2 Automatic Data Collection

5.2.1 IT management platform

IT management platforms are software that allow centralized control of the devices in a network. It consists of a series of agents that can be installed on various devices, which have administrative privileges and communicate directly with a centralized console. In practice they do what every hacker tries to do, but with the consent of the user who goes to install it. The effectiveness of these solutions also depends on the possibility of being installed in the widest

possible operating system landscape, from the most famous Windows and MacOS, to Linux, to mobile OSs or systems for ARM architectures. Having administrative privileges on these machine opens the way to a wide range of features that can be exploited. In the first place they allow data collection over the machine on which they are installed. This means having, first of all, to have a complete software inventory. This includes the operating system in all its components, the BIOS and all installed applications with their respective versions. If the operating system allows it, data can also be collected on the hardware component, real in case of a physical device, otherwise only virtual. This is a necessary point because you must be aware of distinguishing one case from the other. While collecting these static data this software have the possibility of collecting and displaying statistics on real-time operation. For this reason this type of software is left in the infrastructure for a prolonged period (at least 7-10 days) in order to collect data over time and extract statistics on the machine usage. This data includes CPU usage, RAM, available storage but also connected users and log history of processes.

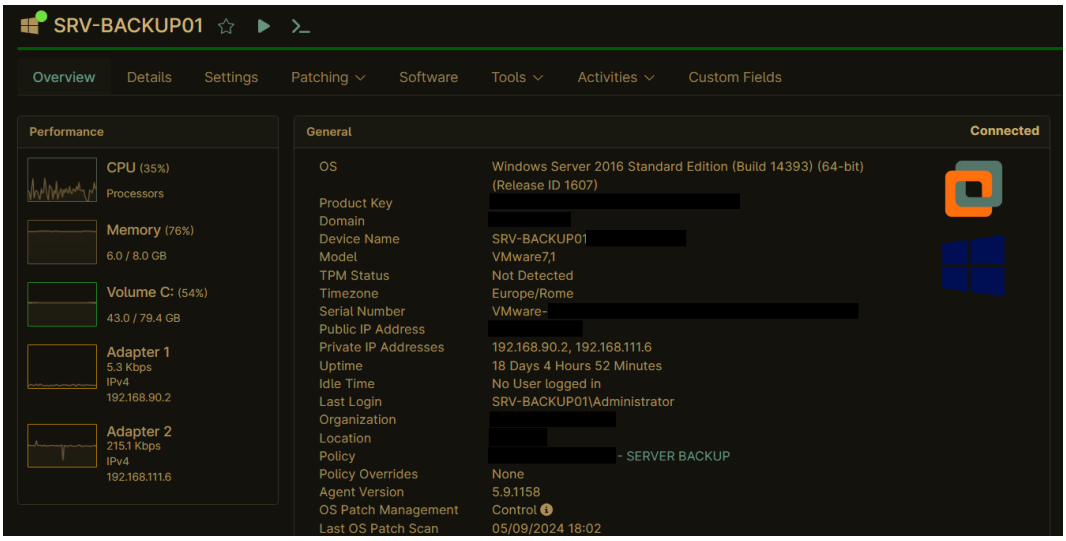


Figure 5.2: Control console of the NinjaONE software. In this image you can see the information collected by the RMM on a generic server.

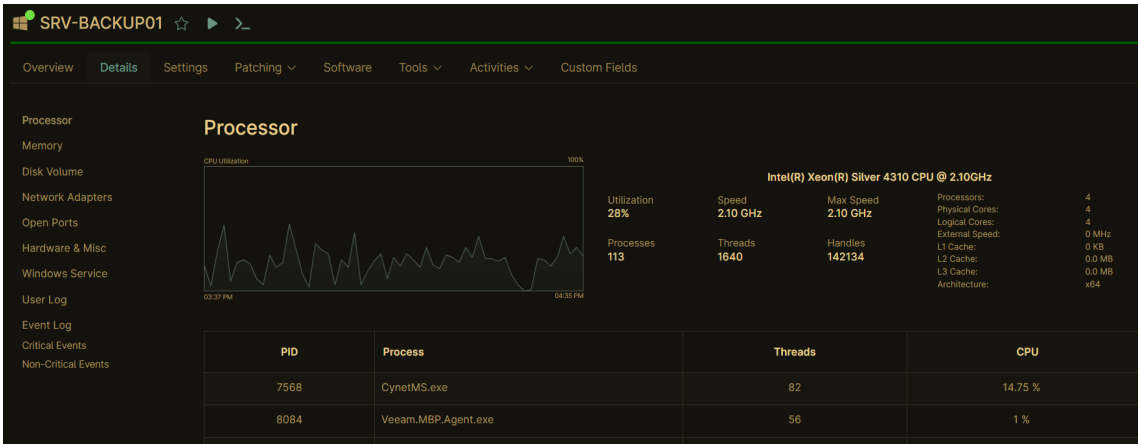


Figure 5.3: Control console of the NinjaONE software. Example of real-time data on performance and processes in place.

Another feature for which they are often used is the possibility of running scripts on devices, always with administrative privileges. Since we can write in low-level languages like powershell or bash, the possibilities are almost unlimited. Considering the context, however, except for some simple commands to collect logs or information, this functionality does not find much space in the assessment. Automation is one of the main reasons for developing RMMs, but it seems secondary for our objectives.

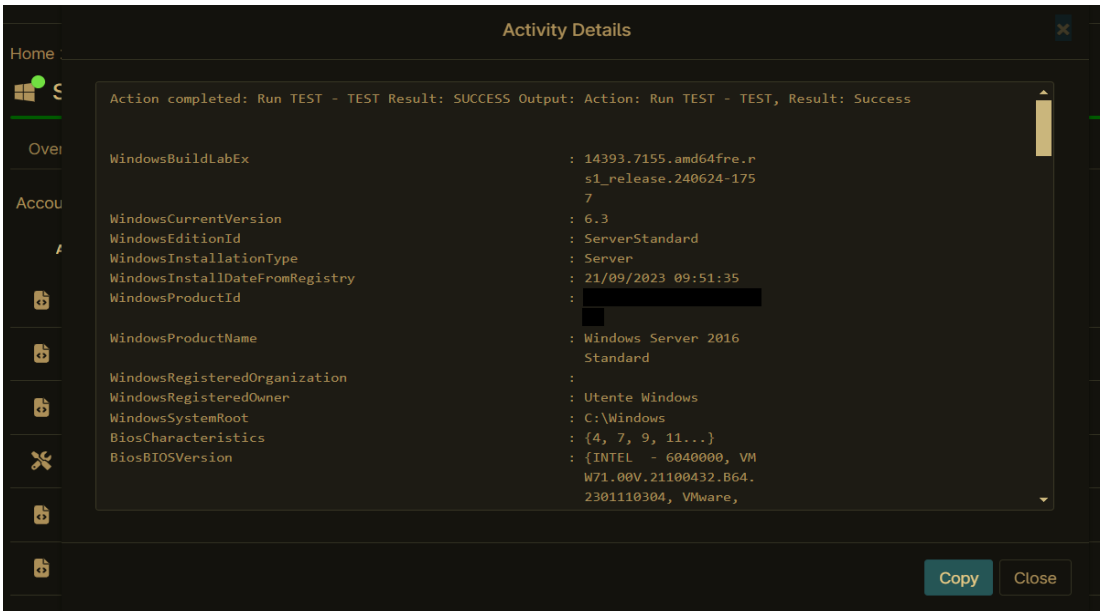


Figure 5.4: Control console of the NinjaONE software. Execution of a simple information-gathering script (Powershell - Get-ComputerInfo).

On the other hand, the network probe function is very useful. In fact, the ability to collect information depends heavily on the ability to install the agent on a device, which is not always possible. Basic devices such as firewalls and switches, but also cameras, sensors or many production tools, do not allow the installation of additional software. In these cases the analysis is done by means of queries over the network. Basic protocols such as the Internet Control Message Protocol (ICMP) or the User Datagram Protocol (UDP) can be used to test whether a device is online and on which ports it is listening. Even at ISO/OSI level 2, ARP tables can be used to collect information about IP and MAC addresses of devices connected to the network but not directly hosting an agents. Many other information can be collected with more sophisticated protocols such as SNMP or NETBios, but these examples will be further developed later with more specific tools. What interests us is that having even a limited number of agents within a network it is possible to reconstruct in a practically automatic way a good topology of the network, an inventory of hardware and software and to get an idea of how much and how the nodes are used.

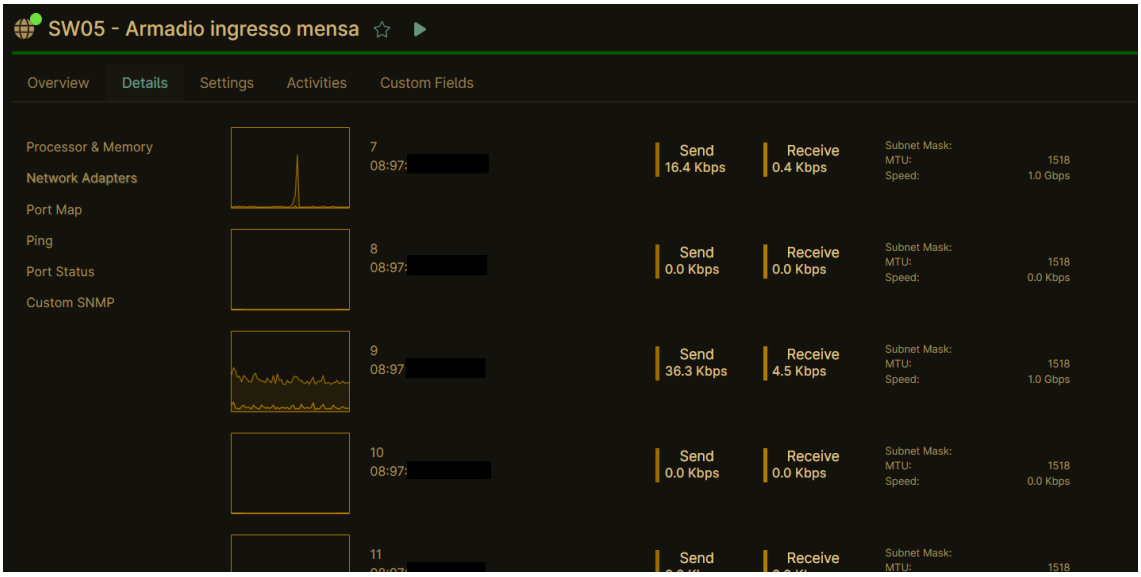


Figure 5.5: Control console of the NinjaONE software. Example of monitoring on a network element (switch) where no agent is installed. Monitoring is mainly done by means of SNMP packets.

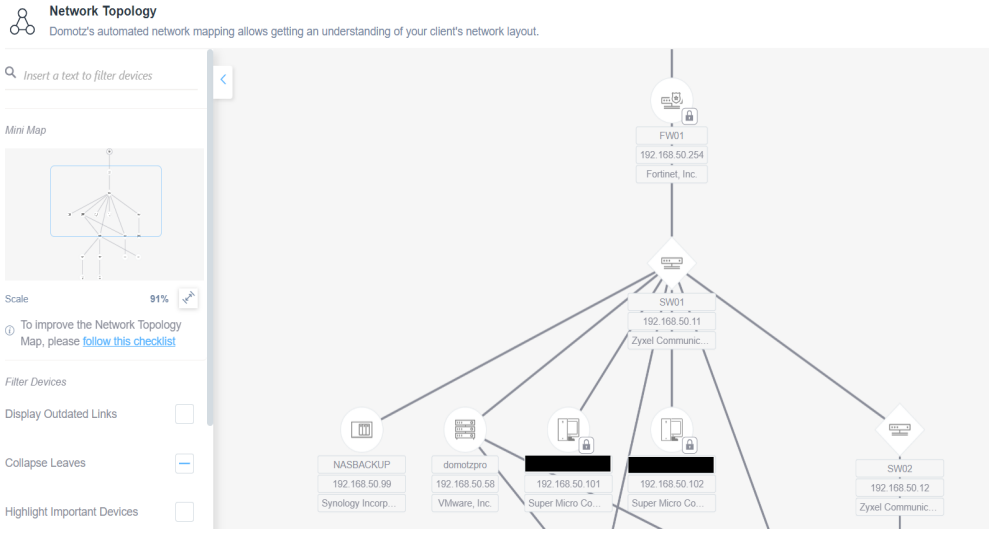


Figure 5.6: Control console of the Domotz software. The topology is automatically reconstructed by detecting packet hops.

5.2.2 Vulnerability Scanner

The network scanner is definitely the most powerful tool among all those I will present in this section. Not by chance it is also the most expensive from an economic point of view and the most complex to manage. It is basically a combination of multiple analysis tools, orchestrated to operate in parallel and bundle all data into one console. It acts more or less like an RMM but focuses more on the security aspect. For example it collects a software inventory too, but highlights mainly software versions and known CVE present in it. The more up-to-date and modern versions also classify the CVEs found according to CVSS and EPSS scales and use them to assign an evaluation to each node. Other variables for this evaluation are for example the presence or absence of EDR, the activation or absence of firewall or the fact that a backup is active or not.

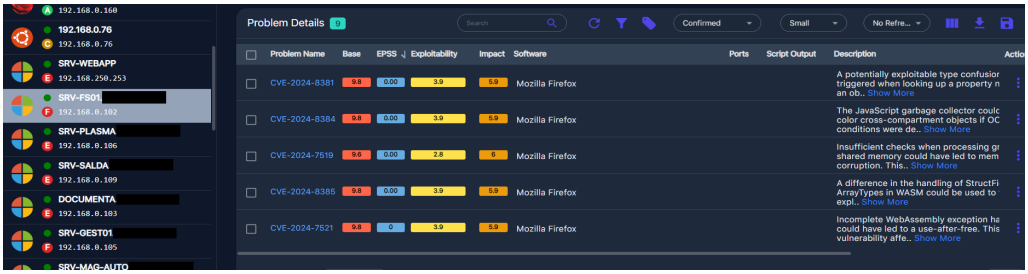


Figure 5.7: Control console of the ConnectSecure software. Example of a vulnerability scan on a generic virtual machine. The CVE are presented with their assessment and a remediation plan is also presented.

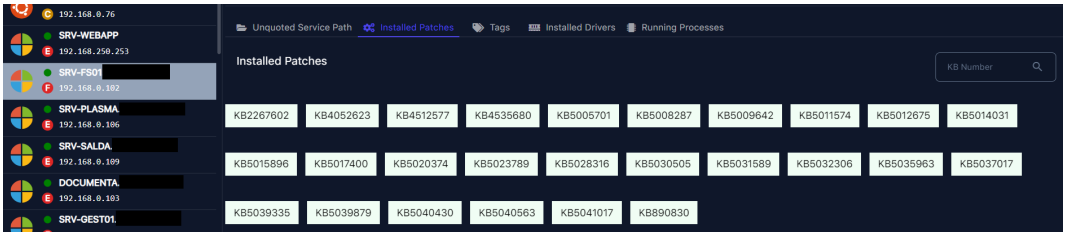


Figure 5.8: Control console of the ConnectSecure software. This section shows installed Windows patches. Software version inventory is critical to finding CVE.

In addition, a wide range of network traffic information is collected. These include for example the protocols used, active ports and services or encryption algorithms configured. This analysis is perfectly consistent with the first, as the combination of exposed services and outdated software is the most serious form of vulnerability that a network can present. The analysis of the protocols and encryption algorithms used is essential for confidentiality. Outdated protocols or insecure encryption algorithms could allow an intruder to intercept and sniff traffic.

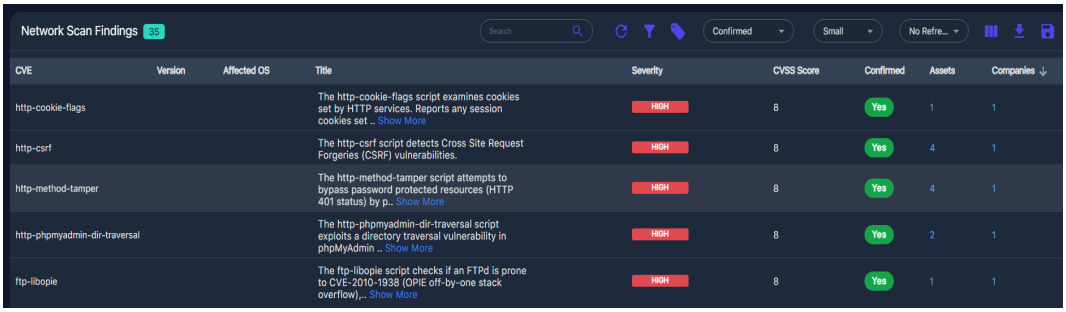


Figure 5.9: Control console of the ConnectSecure software. Esempi di vulnerabilità relative alla rete. ConnectSecure è in grado di rilevare protocolli insicuri o obsoleti, rischio di injection e XSS scripts.

These services typically also include additional tools to analyze, for example, the Active Directory configuration or injection vulnerabilities. But here too I will go more in detail on in the next paragraphs. Another very interesting function is the possibility of carrying out automated audits of compliance with certain standards. In this specific case the software is able to check compliance with all the main frameworks, such as the GDPR, NIS or the ISO. This is not part of our needs but if you want to deepen in that sense it remains a good resource.

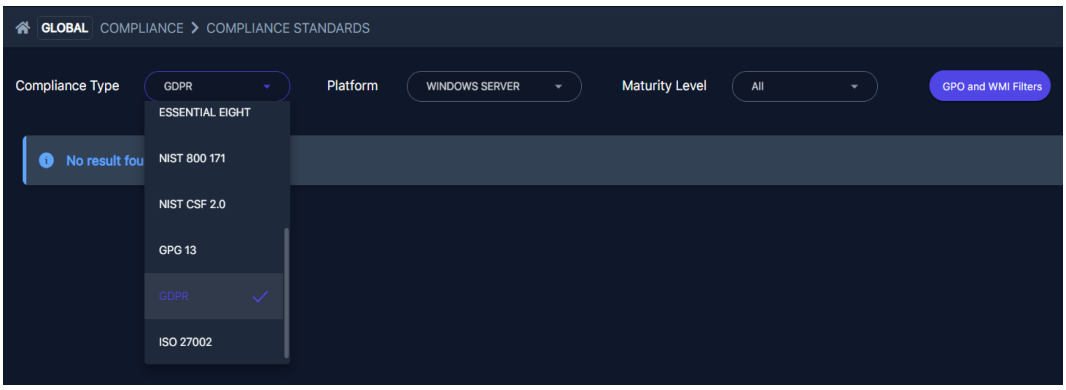


Figure 5.10: Control console of the ConnectSecure software. Section to set up the analysis related to compliance with major standards.

5.2.3 Targeted Inspection

I have already stated how the use of sophisticated tools such as those presented so far can be replaced by open source tools. These may be more difficult to manage and lack a centralized data collection system. In the course of the analyses carried out for the company I preferred to add them to the other solutions when I identified potentially vulnerable nodes and wanted to study them individually with greater attention.

The first tools, the most important, are widespread in the field of systems and cover the scanning function of the network. I'm talking about Nmap and Wireshark. The first is a tool capable of performing an infinite amount of different types of network scans, the second is a collector of sniffed packets. I will not go too far on their presentation because what I am interested in highlighting is more their role, it will then be up to the analyst to decide whether and how much to specialize in their use. Both can safely cover all the main needs of generic scanning, but there are other more specialized tools in some areas for which they are optimized and easier to use.

Nikto, for example, is better than Nmap when it comes to scanning web servers for vulnera-

bilities, misconfigurations, and insecure scripts. It is designed specifically to scan for issues on services like Apache, Nginx, IIS an so on. It checks for known vulnerabilities, default files, insecure HTTP methods (like PUT or DELETE), and outdated software versions. Everything thanks a database of over 6,700 potentially dangerous files, 1,250 version-specific problems and 270 version-specific web server vulnerabilities. Here some examples of Nikto commands:

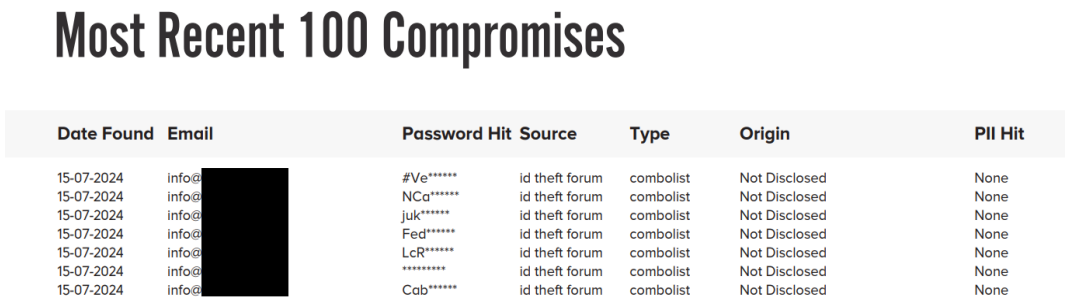
```
nikto -h http://example.com -Tuning 9
```

The -Tuning option allows you to focus on specific types of vulnerabilities. Tuning 9 specifically looks for injection vulnerabilities like command injection.

```
nikto -h https://example.com -ssl
```

This command scans HTTPS (SSL/TLS-enabled) sites for misconfigurations, weak encryption, and outdated SSL versions that could lead to vulnerabilities like man-in-the-middle attacks.

Other tools are even more specific and focus on a single protocol. Enum4linux is great for comprehensive NetBIOS/SMB enumeration on Windows and Samba systems, providing deep insights into users, shares, and policies. NetBIOS in particular is a protocol to be particularly considered because it spreads messages containing the hash of domain credentials over the network. This is not equivalent to sharing the credentials in plain text, of course, but in the case of a node with a fragile password it can mean getting to crack it within just a few hours. Moreover, regarding this time the SNMP protocol, Snmpwalk and Onesixtyone are the most effective tools for SNMP enumeration. SNMP (Simple Network Management Protocol) is a protocol used to manage and monitor devices on a network by collecting data and configuring network devices remotely using management information bases (MIBs). This protocol in its version 1 and 2 shares information without encryption, which could easily be sniffed. Snmpwalk is a tool made to extract detailed SNMP information while Onesixtyone is a fast scanner for finding SNMP devices and weak community strings.
An interesting feature that is not done by the tools presented so far concerns the search for cracked passwords. In general, data breaches are made public so that anyone can find out how many or which passwords among their own are no longer secure. There are also automatic tools that scan these public databases and, if necessary, sites that sell profiles and passwords on the dark web.



Most Recent 100 Compromises

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
15-07-2024	info@[redacted]	#Ve******	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	NCa******	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	juk******	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	Fed******	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	LcR******	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	*********	id theft forum	combolist	Not Disclosed	None
15-07-2024	info@[redacted]	Cab******	id theft forum	combolist	Not Disclosed	None

Figure 5.11: Result of a search delegated to third parties. This is a list of cracked passwords found in online databases and forums on the dark web.

5.3 Internal Solution Analysis

5.3.1 Network Devices

The measures presented so far both allow to collect information on the organization and the general functioning of the network. However, details of the configurations cannot be collected through network protocols as those presented so far. It is therefore important to inspect the main distribution nodes of the network directly during the analysis. This kind of analysis is not a penetration test, so the analysts have full and complete access to all the network devices. In this case, if you are lucky the network is subject to a centralized controller, which gives access to all configurations from a single centralized console. In most cases, however, network devices are different, of different types and brands, often installed at different times and configured as the network grew. In these cases, one-on-one access to each node is needed to collect the necessary information, which could be time and labour intensive. That's why it is important to keep your focus and start your survey with your goals in mind. The first step is obviously to take into analysis the firewall.

A firewall serves as a critical barrier between trusted internal networks and untrusted external networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. Stateless firewalls examine each packet in isolation, making decisions based solely on predefined rules without considering the context of the connection. In contrast, stateful firewalls maintain awareness of the state of network connections, tracking the entire conversation and making more informed decisions based on the full context of the traffic. By studying these rules, it is possible to understand the level of isolation of the various subnetworks and the routing policies implemented. At this level, safety depends mainly on

the detail in the configurations. The safest rules are those that limit connections and even protocols to what is strictly necessary for the operation of the nodes concerned. At this level we are not interested in the routing policies and services attached to them (the difference between RIP and OSAF at these scales is not significant) except for some particular cases such as the configuration of a dynamic backup line. It is one of the main factors for availability in case of internet failures. The firewall also typically configures all the VLANs (Virtual LANs) used in the network. VLANs are essential because they greatly simplify the network's provisioning process, especially when the distribution network relies on switches that can manage them.

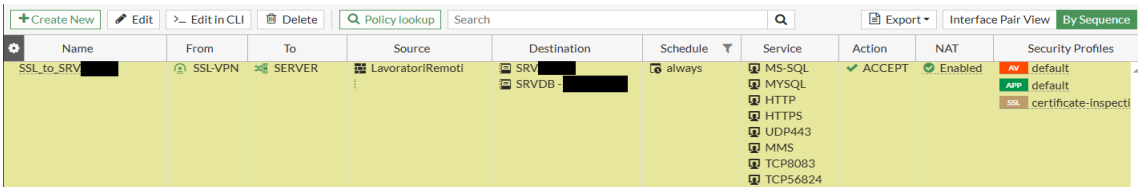


Figure 5.12: Web interface of a Fortinet firewall. In this example you can see a very precise policy, where source and destination are limited to a small number of ports and protocols.

VLAN Settings

ID	NAME	ZONE	IPV4 ADDRESS	IPV6 ADDRESS
110	OFFICE	Trusted	192.168.110.254	
120	VoIP	Trusted	192.168.120.254	
130	PRODUCTION	Trusted	192.168.130.254	
140	TVCC	Trusted	192.168.140.254	
150	PRINTERS	Trusted	192.168.150.254	

Figure 5.13: Web interface of a Watchguard firewall. List of VLANs configured within the firewall.

Next step concerns the so called UTM (Unified Threat Management). Next-generation firewalls in fact are systems build upon traditional firewall capabilities by incorporating advanced features. These functions can be condensed into three macrogroups. The first is about controlling outgoing traffic and includes mainly features to block traffic to certain IPs or domains. It is usually joined by an application control, which instead intervenes on the applications used by the nodes to generate those connection attempts. The second is about the inspection of incoming packets, both in plain text and acting as a proxy for SSL/TLS encrypted packets. The last function is to analyse the traffic as a whole, looking for patterns in the data flow or concatenations of the data contained in the packets. These tools are classified as intrusion detection/prevention systems (IDS/IPS) according to their ability or not to act independently. All these systems, such as VLANs, are then extended to other network devices, if integration is

allowed. Regarding security in that case it is important to analyze how the switches' trunks are configured, i.e. the connections between multiple switches. The rule is always to allow nothing more than necessary, therefore operating at the layer 2 in order to limit VLANs.
Shifting focus back to network operation, usually network devices also allow for the collection of statistics on throughput over time and resource utilization. In these cases the best possible case also includes the high availability policy, according to which at least core elements (firewall and core switches) are redundant. By redundant, I mean two twin network elements in parallel, capable of replacing each other instantly in the event of failure.

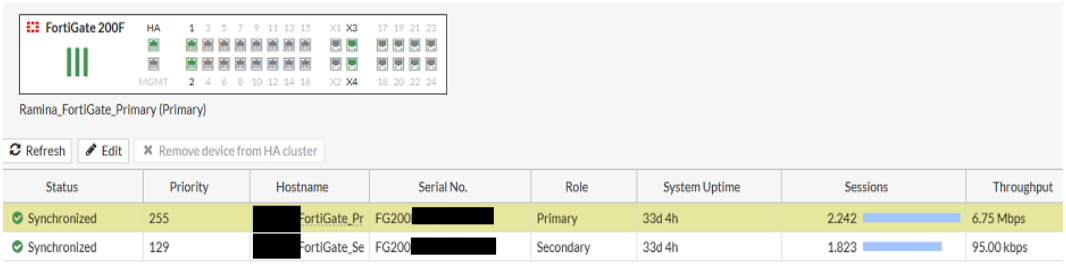


Figure 5.14: Web interface of a Fortinet firewall. In this widget you can observe the mutual monitoring of two firewalls configured for HA.

The last aspect to consider when it comes to networks is the configuration of encryption algorithms, especially with VPNs and Wi-fi. This is not a treatise on cryptography and I do not intend to dwell too much on the various possibilities. They often depend not so much on the intentions of users as on the possibilities made available by the software. These have only a limited range of algorithms for encryption, whether symmetric or asymmetric, and hashing. In these cases the analysis should touch on the various steps of authentication and identify which solutions have been adopted and if they are or are not considered obsolete.

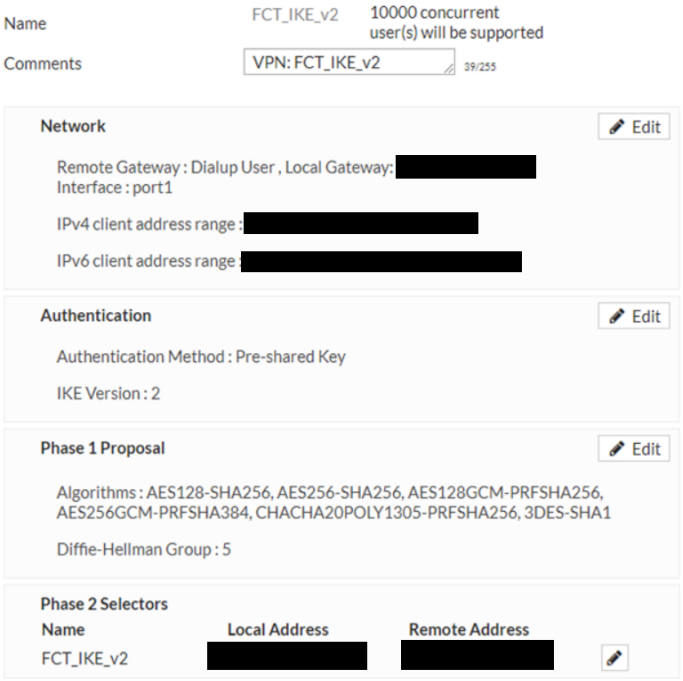


Figure 5.15: Web interface of a Fortinet firewall. Configuration options for an IKEv2 VPN tunnel. In the image you can see the possibility to choose from a wide range of different algorithms for both negotiation and authentication.

5.3.2 Backup

Backups are an element that comes back on several different spots in my evaluation and this is enough to underline how important they are for both availability, confidentiality and integrity. In addition to this, however, they also prove to be an excellent point of information collection. Backups usually protect the main infrastructure nodes, outlining priorities and touching on a whole range of elements that I have not yet explored as storage nodes. It is common practice in companies to have a role distribution that sees some devices delegated to computing and others delegated to storing information. This is the role of NAS (Network Attached Storage) and SAN (Storage Area Network), which differ only in a performance aspect, but which essentially perform the same task. The study of these nodes falls within the analysis of the company's resources and their sufficiency or redundancy. On the other side, for what concern backup security, it is important to investigate the level of encryption adopted by this nodes for storage and communication protocols over the network. Protocols such as SMBv1-v2 are classic examples of outdated configurations that pose a serious security risk while more modern implementations such as ISCSI and SFTP are definitely to be preferred.

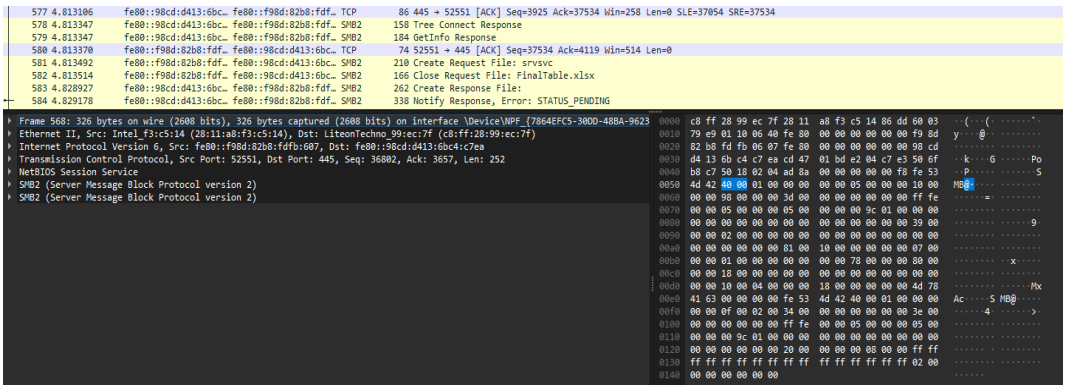


Figure 5.16: Inspection of a packet in SMB v2 using wireshark on a listening device in the network.

Backup analysis then moves on to the business continuity and incident response component. From this point of view, it is important to highlight the need for a double search in parallel between the needs of the client and the measures taken. Short-term backups must be made with a frequency and time interval that strongly depends on the speed at which a company needs to update its data. What is always essential is, otherwise, a long-term retention backup (at least 30 days) to preserve the company in case of infiltrations or prolonged malware attacks. All longer retention backup policies depend, again, on specific needs of the company or on personal decisions.

Once you have understand the storage policies for backups, you must take into account the speed with which you can restore them. This is a factor which does not concern safety but which heavily influences the ability of a company to recover from an accident. The best possible solution in this case is high availability. As with networking, there are also strategies for creating some redundancy for servers and clients. They take the form of backups in executable formats. These formats can vary from ISO to the most common virtualization formats, and allow you to replace with very short time a possible failure. The last object of concern on backups is therefore to probe the high availability, even in its most widespread form in the context of SMEs, which hyperconvergence.

5.3.3 Internal Domain

The internal domain analysis is an analysis that completes the investigation process of the solutions implemented by the customer. It should be stressed that this kind of data collection could also be carried out by specific software tools, but which I have decided to include in this area because I believe it should be done only after another analysis. As with backups, in fact,

this part of the analysis is heavily influenced by company policies. It could be safely said that the domain survey serves as confirmation for three important corporate policies: the password policy, the staff inboarding and outboarding policy and the access roles to various levels of information inside the company. Once these three standards are defined, the internal domain analysis is almost a confirmation of the exact execution of these directives. From a practical point of view that means to inspect the list of users, the list of groups and any GPOs with its logon/logoff Scripts.

5.3.4 Security Tools

In the event that the client's infrastructure implements specific software for cybersecurity will then be the last effort of the technician to ascertain its effectiveness and configurations. By cybersecurity tools I mean endpoint protection systems but also and above all antispam and mail security. These two elements are the main source of countermeasures to limit users' lack of awareness. I have not gone into too much detail, however, as the configuration of these services is extremely variable and must be studied on a case-by-case basis. They could be supplemented by digital signature, biometric or physical authentication systems and video surveillance systems. The range is varied and does not allow to standardize the process beyond the awareness of having to investigate all these various entities.

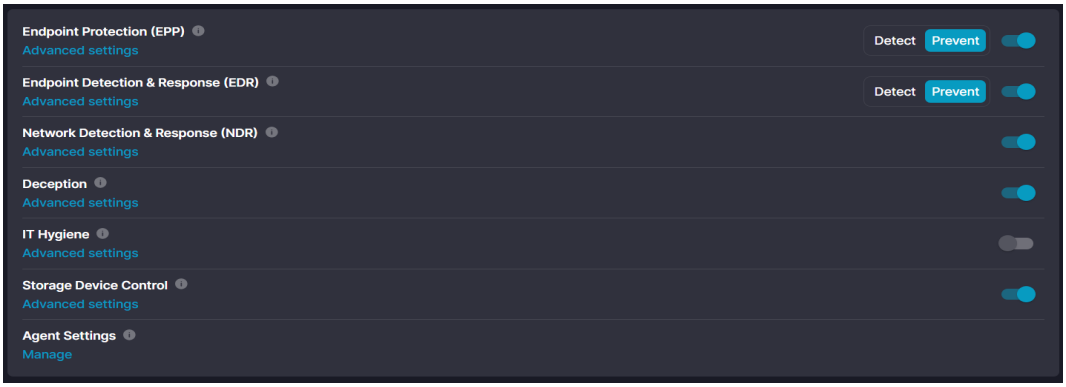


Figure 5.17: Control console of the Cynet software. Overview of the features of a new-generation XDR. The software is able to monitor the node (EDR), its interaction with other nodes (NDR), to create honeypots (Deception), but also has functions of RMM (IT Hygene) and peripheral control (Storage Device Control).

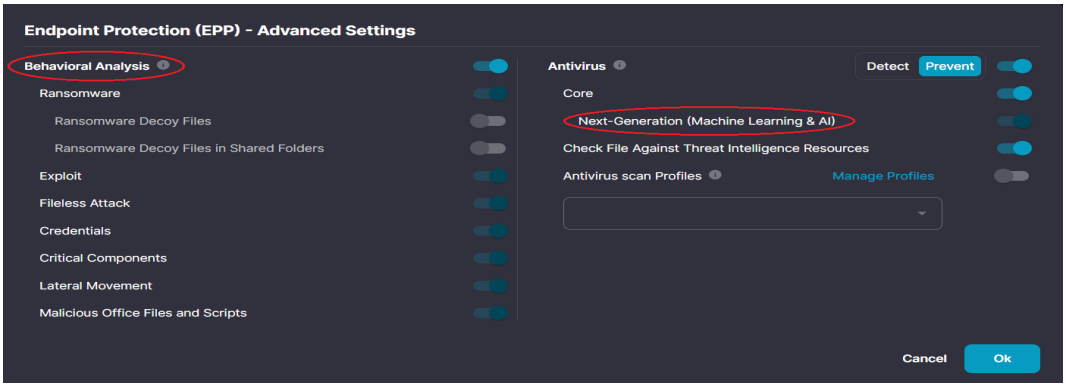


Figure 5.18: Control console of the Cynet software. The options highlighted are those that use AI to memonize behavior within the network. This feature is definitely the one that most distinguishes XDR from simple antivirus because it prevents not only malicious software but also legitimate software misused.

5.4 Other

This category essentially comprises most element of personnel assessments. From a practical point of view, this category would include staff questionnaires, phishing campaigns and OSINT analysis. I decided not to go into this section too much for two main reasons. The first is that during my research period I have been able to apply and refine only the operational assessment and security assessment. The staff analysis is still in development and I have not been able to gather enough data to present a comprehensive practical implementation. The second reason is that the three analyses mentioned above, especially regarding surveys and OSINT, would require a much greater effort to be in depth than I can put into this work. This category therefore remains an open chapter in my research, a point to be developed in the near future to give a definitive form to the assessment.

6

Conclusions and Future Works

In this thesis I tried to analyze the assessment service provided by my company to adapt it to its needs and the context in which it is applied. My starting point was a disorganized and selective analysis, difficult to organize, replicate and present to clients. From there I decided to reinvent assessment through a framework built around the needs of SMEs. The framework that has been developed respects the criteria of modularity, clarity and focus on safety that I had set myself at the beginning of my work, extending also to the possibility of evaluating company personnel. Within the framework, issues are divided into thematic clusters and evaluated on the basis of their impact on the company. These evaluations, both graphical and numerical, are consistent with the parameters I had decided to emphasize during the presentation of the report. I had the opportunity to test in production the first two of the three modules, obtaining some initial feedback on the effectiveness and applicability of the service. The results were very positive but I could not quantify mathematically these advances because the surveys made so far, especially in terms of comparison with other similar services, are not in sufficient number to be considered them a reliable source.

In future, two are the next steps that I believe it is necessary to take to complete this project. The first one concerns the actual implementation and production of the personnel assessment, in order to make the framework finally complete. After that the three assessments will be refined through a campaign to collect feedback on the assessments, in order to collect constructive criticism from both technical and customer points of view. Creating a structured feedback

system would also allow to start an adaptation cycle that would keep the framework up-to-date, both with regard to the evolution of cybersecurity and SMEs.

Finally, I hope that this kind of approach can serve as a starting point for similar research but in different fields of the economy. From a study of the various economic contexts, variations of the framework could be created tailored to companies of different sizes (large companies), or even for types of company (manufacturing, services, ...). A wider spread of cybersecurity practices means a safer, more stable and therefore stronger economic fabric. After all the diffusion of a process is due to the ability to optimize it, make it simpler and, consequently, even cheaper.

References

[1] Y. Ozkan and M. Spruit, *Cybersecurity for SMEs - Part 1*. ETSI, 2021.

[2] *CIS Critical Security Controls (CIS Controls) Measures and Metrics for Version 7*. Center for Internet Security, 2022.

[3] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, *Analysis of Cybersecurity Standard and Framework Components*. International Journal of Communication Networks and Information Security (IJCNIS), 2020.

[4] H. Taherdoost, *Understanding Cybersecurity Frameworks and Information Security Standards — A Review and Comprehensive Overview*. MDPI, 2022.

[5] B. Saha and Z. Anwar, *A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework*. Journal of Information Security, 2024.

[6] A. Emer, M. Unterhofer, and E. Rauch, *A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises*. Enginering Management Review - Volume 49, 2021.

[7] C. Paulsen and P. Toth, *Small Business Information Security: The Fundamentals (NISTIR 7621 Revision 1)*. National Institution for Standard and Technology, 2016.

[8] R. T., I. I, G. D., and M. T, *Guidelines for the empirical vulnerability assessment*. GEM Technical Report, 2014.

[9] P. Mell, K. Scarfone, and S. Romanosky, *Common Vulnerability Scoring System*. IEEE Security & Privacy - Volume 4, 2006.

[10] Q. Liu and Y. Zhang, *VRSS: A new system for rating and scoring vulnerabilities*. Computer Communications - Volume 34, 2011.

[11] J. Srinivas, A. K. Das, and N. Kumar, *Government regulations in cyber security: Framework, standards and recommendations*. Future Generation Computer Systems - Volume 92, 2019.

[12] T. Ncubukezi, *Risk Likelihood of Planned and Unplanned Cyber-Attacks in Small Business Sectors: A Cybersecurity Concern*. University of Technology, Cape Town, 2023.

[13] R. Mohamed and M. M. Ismail, *Evaluation of Cyber Insecurities of the Cyber Physical System Supply Chains Using α-Discounting MCDM*. Neutrosophic Systems with Applications - Volume 12, 2023.

[14] E. Doynikova, A. Fedorchenko, and I. Kotenko, *Ontology of Metrics for Cyber Security Assessment*. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 2019.

[15] B. Y. Ozkan and M. Spruit, *Adaptable Security Maturity Assessment and Standardization for Digital SMEs*. Journal of Computer Information Systems, 2023.

[16] S. Almuhammadi and M. Alsaleh, *Information security maturity model for NIST Cyber Security Framework*. University of Dhahran, Saudi Arabia, 2021.

[17] A. Calder and S. Watkins, *IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002*. Kogan Page, 2018.

[18] *Rapporto Regionale PMI 2021*. Confindustria e Cerved, 2021.

[19] M. Spruit and B. Y. Ozkan, *Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda*. International Journal of Standardization Research - Volume 17, 2019.

[20] R. Leszczyna, *Review of cybersecurity assessment methods: Applicability perspective*. computer & security 108, 2021.

[21] *Verizon Data Breach Investigations Report*. Verizon and partners, 2021.

[22] M. Shepherd, *Surprising Small Business Cyber Security Statistics Fundera Ledger*. Fundera, 2023.

[23] N. Mmango and T. Gundu, *Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs*. International Conference on Electrical, Computer and Energy Technologies (ICECET), 2023.

[24] K. Rahmonbek, *Alarming Small Business Cybersecurity Statistics for 2023*. StrongDM, 2023.

[25] *Cyberthreat Defense Report 2022*. CyberEdge Group, 2022.

[26] M. de Fátima Brilhante, D. Pestana, P. Pestana, and M. L. Rocha, *Measuring the Risk of Vulnerabilities Exploitation*. AppliedMath 2024, 2023.

[27] *Cyber Essentials: Requirements for IT infrastructure*. National Cyber Security Center (UK), 2023.

[28] *Cyber security guide for SME (Belgium)*. Center for Cyber Security Belgium, 2023.

[29] *CIS Controls: Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)*. Center for Internet Security, 2022.

[30] C. R. Junior, I. Becker, and S. Johnson, *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. University College of London, 2023.

[31] M. Kappea, R.-C. Härtinga, C. Karga, and D. Deffnera, *Cybersecurity in SMEs – Drivers of Cybercrime, Insufficient Equipment and Prevention*. 27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, 2023.

[32] S. Chaudhary, V. Gkioulos, and S. Katsikas, *A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprise*. Computer Science Review 50, 2023.

[33] I. H. Sarker, *Automation in Cybersecurity: Current and Future Prospects*. Annals of Data Science, 2022.

[34] A. Alfaadhel, I. Almomani, and M. Ahmed, *Risk-Based Cybersecurity Compliance Assessment System (RC2AS)*. MDPI, 2023.

[35] C. Ponsard, P. Massonet, J. Grandclaudon, and N. Point, *From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium*. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020.

[36] M. M. Mijwil1, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, *Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview*. Mesopotamian journal of Cybersecurity, 2023.

[37] A. Moneva and R. Leukfeldt, *Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures*. Journal of Criminology, 2023.