

# Applied Cybersecurity in Healthcare: A Real-Life Remediation Case Study

UNIVERSITY OF TURKU  
Department of Computing  
Master of Science (Tech) Thesis  
EIT Digital Cyber Security  
May 2025  
Titouan LE BLE

Supervisors:  
Seppo Virtanen  
Saku Lindroos

UNIVERSITY OF TURKU  
Department of Computing

TITOUAN LE BLE: Applied Cybersecurity in Healthcare: A Real-Life Remediation Case Study

Master of Science (Tech) Thesis, 87 p., 25 app. p.

EIT Digital Cyber Security

May 2025

---

In recent years, the increasing digitization of healthcare facilities in France has highlighted major cybersecurity vulnerabilities, exacerbated by chronic underinvestment and fragmented IT governance. This thesis explores how hospitals can nevertheless strengthen their IT security through low-cost strategies. Conducted within the Esquirol Hospital Center in France, this concrete case study focuses on the remediation of Active Directory vulnerabilities, the reduction of the internet-exposed attack surface, and the implementation of a secure remote maintenance platform, following the French national agency for information system security's recommendations and the CaRE program's requirements. Beyond the specific case, this thesis can be used as a basis for creating a replicable methodology for other establishments of all sizes seeking to improve their resilience to cyber threats, even with limited resources. Finally, it advocates for the systematic integration of cybersecurity from the design phase of hospital digital projects, to make it a strategic issue in its own right.

Keywords: Cybersecurity, Active Directory, Attack Surface, Internet Exposition, Telemaintenance

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>IT Security in Healthcare</b>	<b>5</b>
2.1	Global Historical and Economical Context . . . . .	5
2.2	Issues and Evolution of Cybersecurity Practices and Regulations in Hospitals . .	9
2.3	Regulatory Framework: The CaRE Program . . . . .	12
2.3.1	1st Axis: Governance and Resilience . . . . .	14
2.3.2	2nd Axis: Resources and Mutualization . . . . .	15
2.3.3	3rd Axis: Awareness . . . . .	16
2.3.4	4th Axis: Operational Security . . . . .	17
2.3.5	Insights from a Service Provider . . . . .	20
<b>3</b>	<b>Overview of the Esquirol Hospital Center’s IT Infrastructure</b>	<b>23</b>
<b>4</b>	<b>Auditing Tools and Results</b>	<b>28</b>
4.1	Tools’ Internal Mechanisms . . . . .	29
4.1.1	Mechanism Behind Attack Surface Mapping . . . . .	29
4.1.2	Active Directory Enumeration and Analysis Process . . . . .	33
4.2	Detailed Review of Audit Reports . . . . .	35
4.2.1	Analysis of Exposed Services and Entry Points . . . . .	35
4.2.2	Results of Active Directory Security Review . . . . .	37

<b>5</b>	<b>Attack Surface and Internet Exposition Remediation</b>	<b>40</b>
5.1	Requirements Analysis for the Virtual Private Server . . . . .	40
5.2	Architecture and Design . . . . .	42
5.3	Implementation of the Solution . . . . .	45
<b>6</b>	<b>Active Directory Vulnerabilities Remediation</b>	<b>55</b>
6.1	Level 1 ANSSI . . . . .	56
6.2	Level 2 ANSSI . . . . .	58
6.3	Level 3 ANSSI . . . . .	59
6.4	Level 4 ANSSI . . . . .	62
<b>7</b>	<b>Secure Telemaintenance Platform Deployment</b>	<b>65</b>
7.1	Requirements Analysis for the Secure Telemaintenance Platform . . . . .	65
7.2	Architecture and Design . . . . .	67
7.3	Implementation of the Solution . . . . .	71
7.4	Transition for External Service Providers . . . . .	78
<b>8</b>	<b>Analysis of Results and Discussion</b>	<b>79</b>
8.1	The CaRE Program’s Limitations . . . . .	79
8.2	Evaluation of Security Improvements . . . . .	80
8.3	Limitations and Future Enhancements . . . . .	82
<b>9</b>	<b>Conclusion</b>	<b>85</b>
	<b>References</b>	<b>88</b>
	<b>Appendices</b>	
<b>A</b>	<b>: Service Provider Q&amp;A</b>	<b>A-1</b>
<b>B</b>	<b>: Password Renewal’s Script</b>	<b>B-1</b>

<b>C</b> : Python application's code	<b>C-1</b>
<b>D</b> : On The Use Of LLMs	<b>D-1</b>

# List of Figures

2.1	Density of full hospitalization beds, in France, in 2019. . . . .	6
2.2	Number of DDoS attacks observed by ANSSI against French targets . . . . .	11
3.1	High-level diagram of the Esquirol Hospital Center IT infrastructure . . . . .	27
4.1	Attack Surface and Internet Exposition Report Summary . . . . .	36
4.2	ISARS Active Directory Report Summary . . . . .	37
4.3	ORADAD Active Directory Report Summary . . . . .	38
5.1	Virtual Private Server implementation schema . . . . .	45
5.2	Nginx Proxy Manager special configuration . . . . .	54
7.1	Jump server implementation schema . . . . .	71
7.2	Hospital's firewall internal rules for the maintenance platform . . . . .	72
8.1	Attack Surface and Internet Exposition Result Report Summary . . . . .	81
8.2	ORADAD Active Directory Result Report Summary . . . . .	82

# List of acronyms

**ACDRP** Activity Continuity and Disaster Recovery Plan

**AD** Active Directory

**ANS** Digital Health Agency

**ANSSI** National Agency for the Information Systems' Security

**API** Application Programming Interface

**CB** Cyber Baseline

**CISO** Chief information security officer

**CVE** Common Vulnerabilities and Exposures

**CVSS** Common Vulnerability Scoring System

**DC** Domain Controllers

**DMZ** DeMilitarized Zone

**DoS** Denial of service

**GPO** Group Policy Object

**GRADeS** Regional Support Groups for the Development of e-Health

**HAS** High Authority for Health

**HIS** Hospital's Information System

**IDS** Intrusion Detection System

**IS** Information System

**KDC** Kerberos Distribution Center

**NPM** Nginx Proxy Manager

**OWASP** Open Web Application Security Project

**RDP** Remote Desktop Protocol

**REST** Representational state transfer

**SIEM** Security Information and Event Management

**SPN** Service Principal Name

**SSH** Secure Shell

**SSO** Single Sign-On

**THG** Territorial Hospital Groups

**VNC** Virtual Network Computing

**VPN** Virtual Private Network

**VPS** Virutal Private Server

**WAM** Web Access Management

# 1 Introduction

In their perpetual quest to offer better quality care to their patients, French hospitals began a progressive but radical transition towards all-digital in the 1980s [1], transforming, in the process, the habits of the approximately 200 professions [2] working to their proper functioning. However, after an initial encouragement from the French State in favor of this transition, a blatant lack of organizational, legislative, and monetary support led hospitals to focus their efforts on a strategy centered around cost rationalization and innovation; neglecting, in the process, the optimization and modernization axes that were nevertheless essential for the implementation of a coherent and scalable system. Forty years later, the IT departments are still paying the price and spend the majority of their working time maintaining the existing infrastructure. This includes an average fleet of several thousand devices, across all media, usable on-site or remotely, by employees or visitors. To this must also be added a plethora of business software developed to meet the specific needs of a profession without necessarily taking into account interoperability with other software or integration within the Hospital's Information System (HIS).

The consequences of this lack of attention from both the French state and hospital directors are particularly evident in the area of cybersecurity. Indeed, hospitals still suffer numerous large-scale cyberattacks [3]. These attacks targeting hospitals are essentially ransomware [4] that paralyzes entire systems by encrypting hard drives and databases, forcing the activation of a cyber emergency plan, called the cyber white plan, and the implementation of degraded procedures in all affected departments. These procedures require returning to the paper format

for all tasks to be performed. Few measures were taken during these years to improve this state of affairs. Often limited to mentions in sections not directly addressing these problems and never being at the center of programs, it was not until the 2012 "Hôpital numérique" program [5] that the first government plan including a significant portion dedicated to cybersecurity came to be.

However, the damage was done, as the accumulated delay in systems and infrastructures over the years required an outlay of resources that French hospitals, already in a difficult financial situation following numerous crises and budget cuts, could not easily spend. According to the French Hospital Federation: "The deficit of public hospitals will further increase in 2024 to reach approximately 2.8 billion euros." [6].

It is within this context of difficulties that the CaRE program was created by the Ministries of Health and Digital Affairs. With a budget of 750 million euros spread over 4 phases of action and a period of four years, this program aims to: "accelerate the upgrading of French hospital information systems in the face of the threat landscape and sustainably strengthen the resilience of healthcare facilities." [7] Although this program is not perfect, it is nevertheless a significant step forward for the security of French hospitals.

This thesis proposes a real-life case study of IT security improvement designed to address the economic, organizational, and technical constraints of a leading hospital. It highlights the numerous challenges faced by healthcare facilities in a context where cyberattacks are becoming more frequent and targeted.

This thesis is primarily aimed at the HIS teams that have not participated in the CaRE program and who nevertheless wish to strengthen the security of their infrastructures at a lower cost. However, its contribution is not limited to the hospital sector. It also constitutes a valuable resource for Information System (IS) managers of medium-sized to large companies seeking concrete examples to initiate or structure their cybersecurity approach. By demonstrating that it is possible to lay the foundations for solid security without necessarily resorting to massive

investments, this thesis helps to make cybersecurity more accessible and easier to integrate into practical IT strategies.

My contribution lies in the implementation of several projects aligned with the strategic priorities of the CaRE program. My mission has focused on domains 1, 2, and 3 of this program, although only the first is published to date, which respectively address the securing of Active Directory (AD) and the reduction of the attack surface, threat detection, and the securing of remote maintenance access.

AD is a critical component of the IT infrastructure of healthcare facilities. It is a prime target for attackers seeking to compromise a system on a large scale. Securing it not only reduces the risks of privilege escalation but also prevents the lateral spread of attacks within the network. Reducing the attack surface, described as every potential entry point that an attacker could exploit, complements the security of the HIS. By limiting these exposure vectors, particularly those accessible from the internet, we not only decrease the number of intrusion attempts but also complicate the task for attackers, forcing them to deploy more resources to hope to compromise a system. This approach constitutes a fundamental line of defense for any organization because it makes the task infinitely more difficult for attackers while being relatively simple to implement, thus limiting the number of attacks.

In parallel, a new remote maintenance platform as well as a Security Information and Event Management (SIEM) system were implemented. Although the official requirements of the program are not yet defined for these areas, this anticipatory approach is already contributing to the strengthening of the security of the establishment's systems. It also helps to reduce the future workload of the HIS team, which will take over during the full implementation of these components.

However, this thesis is not limited to a simple technical feedback. It also proposes a reflection on the importance of centering the conception of the hospital's digital projects around cybersecurity. The objective is to show that security should not be a last-minute addition but an essential component, just like performance or compatibility. By identifying existing vulner-

abilities and suggesting avenues for improvement, it seeks to encourage more responsible and better-adapted practices to field reality.

This thesis begins with a contextualization that traces the major historical, economic, and regulatory steps that have influenced the construction of IS's security in the hospital sector. It highlights the impact of the digital transition on the growing exposure to cyber risks, as well as the emergence of new requirements regarding infrastructure resilience. This framework leads to the study of the CaRE program, implemented to structure and strengthen cybersecurity within healthcare facilities in France.

This theoretical and regulatory foundation then serves as the basis for the case study conducted at the Esquirol Hospital Center. It begins with a detailed description, centered around the essential points necessary to understand the remediation measures taken, and the existing IT infrastructure. The audit tools used, their operation, as well as the results obtained are then presented. This phase allows for the identification of existing vulnerabilities and reports on the priorities and corrective measures assigned to each of them.

Based on these findings, the corrective actions implemented to improve the SI's security are detailed. These include migrating the websites to a virtual private server (VPS), deploying a secure remote maintenance solution, and addressing vulnerabilities in Active Directory (AD). These initiatives are fully documented, from the needs analysis to their production deployment, and a prioritization based on their level of criticality. This section illustrates the translation of the CaRE program's objectives within a healthcare facility.

Finally, an evaluation of the results obtained and the progress made in the SI's security is proposed. The section also revisits the limitations of the CaRE program and suggests technical improvements.

## 2 IT Security in Healthcare

### 2.1 Global Historical and Economical Context

According to a report published in 2023 by the French Court of Accounts, an independent french institution responsible of ensuring the proper use of public funds following budgets approved by Parliament [8], the public hospital plays an essential role in giving access to healthcare, particularly in rural areas and socially disadvantaged communities [9]. In these territories, where the private sector's presence is minimal, it handles the vast majority of patients. The public sector also distinguishes itself by its capacity to treat severe pathologies and chronic illnesses, requiring complex and long-term care. In contrast, private establishments mainly focus on short-term hospitalizations and surgical procedures. In 2020, according to the same report, the distribution of hospital beds was 66% for the public sector compared to 34% for the private sector. Figure 2.1 illustrates the shortage of hospital beds, which exacerbates the challenges faced by hospitals. The data is based on statistics published by the DREES (Directorate for Research, Studies, Evaluation, and Statistics), an agency under the authority of several French ministries [10].

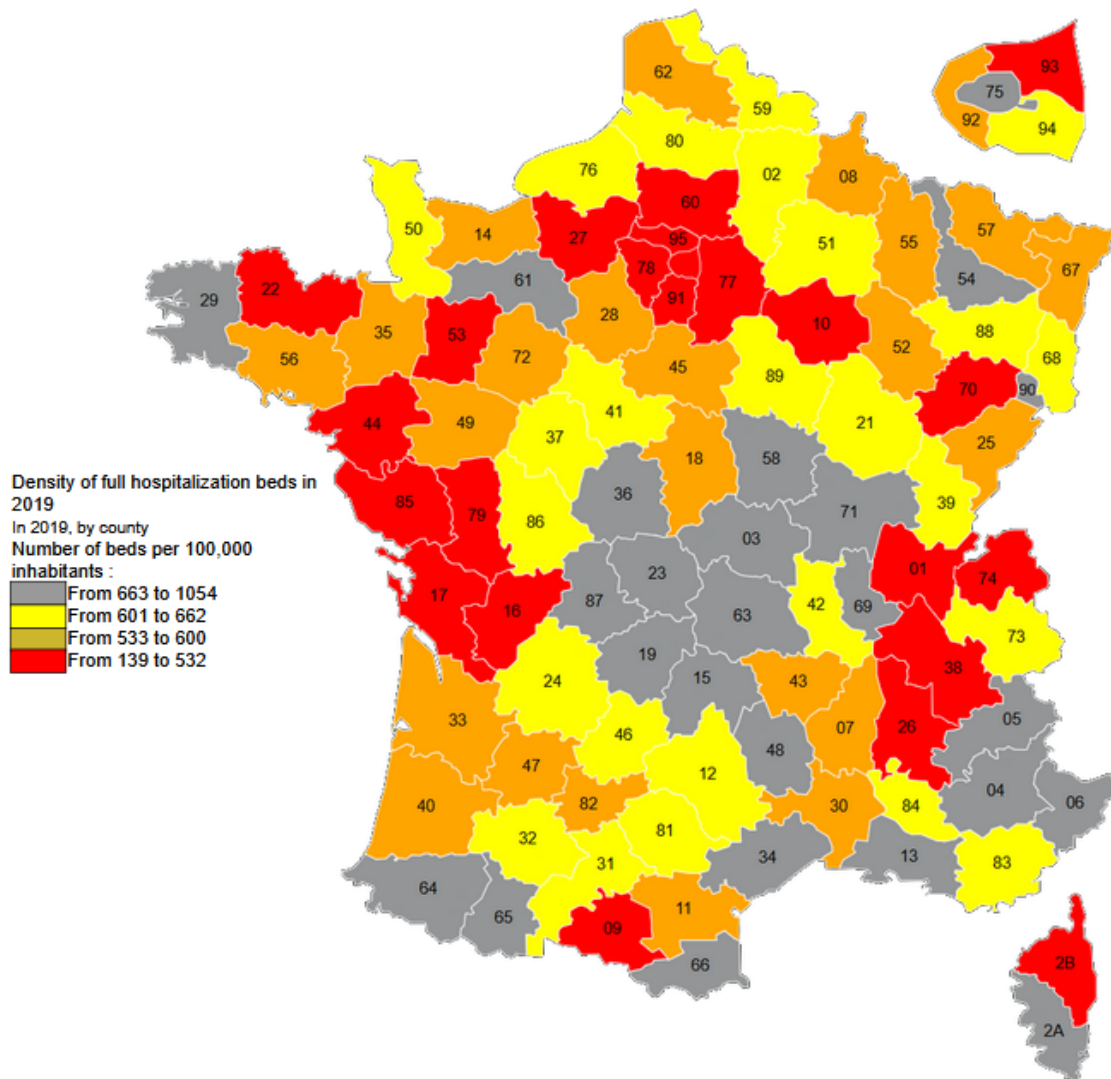


Figure 2.1: Density of full hospitalization beds, in France, in 2019.

Since the 2016 law modernizing the healthcare system [11], a new hierarchical level has been added to the network of the French public hospital service: the Territorial Hospital Groups (THG).

Previously, the network was composed of specialized hospitals based on the type of patients or pathologies they admitted or treated, such as psychiatric hospitals or mother-and-child centers. Each hospital was structured into several departments, grouping either medical disciplines such as oncology or nephrology, for instance, or support functions such as finance or IS [12].

These departments include one or more divisions, called services, each focused on a type of pathology or organ, such as cardiology, the management of eating disorders, or addictions. Each division is then subdivided into functional units, which constitute the operational level closest to the patient. These units bring together care teams, pieces of equipment, and beds to ensure continuous and adapted care, whether in full hospitalization, day hospitalization, or outpatient consultations.

The THGs bring together several hospitals within the same area to strengthen coordination between healthcare establishments and optimize patient care. The main objective of this organization is to rationalize costs by mutualizing the human, material, and financial resources of members. Economies of scale can be achieved while improving the overall efficiency of the healthcare system. By harmonizing care pathways, the THGs ensure consistent and continuous patient care, regardless of their place of residence or the nature of their medical needs. This approach also promotes better access to specialized care by facilitating the referral of patients to the best-equipped and most competent establishments to address their pathologies, which helps to reduce waiting times and unnecessary travel. Furthermore, this reorganization enhances local expertise by allowing each hospital to focus on its areas of specialization. The entire grouping can thus offer a range of care that is comprehensive, diversified, and adapted to the needs of the territory [13].

This reform follows the 2004 reform of the French hospital system, which profoundly modified the funding mechanism for public hospitals in France [14]. Before this date, establishments received an annual budget primarily calculated based on their size, with little consideration given to the actual number of patients admitted. Thus, a hospital facing a significant and sustained increase in its attendance did not benefit from a rapid increase in its budget, which limited its capacity to respond to a rapidly growing demand. To remedy this rigidity, a new funding system was introduced: activity-based pricing, where hospitals are remunerated based on the procedures performed and the pathologies treated. This change in logic allows the French Ministry of Health, which sets the price of procedures, to adjust hospital budgets more

precisely according to the objectives set by the Parliament. However, this reform has generated several side effects. As some pathologies are better remunerated than others, establishments are indirectly incentivized to prioritize these more profitable treatments, to the detriment of less lucrative but equally essential specialties. On the other hand, hospital managements have been pushed to optimize care pathways to increase the volume of procedures performed. Although healthcare staff are not paid per procedure, they are subject to this pressure and must adapt their work organization. The first major change for caregivers was the disappearance of the paper patient file, implemented in 2008 for the Esquirol Hospital Center. The second change is the significant increase in outpatient care, with a 15% rise, as well as home care, up by 45%, while inpatient care has decreased by 21% [15].

In practice, despite the consolidation into THGs, each hospital continues to individually declare the number of procedures it performs and receives financial allocation based on it. Thus, the less favorable results of some members are not offset by those of other members. The mutualization operated within the THGs mainly impacts the awarding of public contracts [13]. The THG negotiates, for all its members, single acquisition contracts for software, equipment, or technical solutions. This centralization certainly lowers the price conditions, but it also imposes a standardization of tools and practices. This homogenization, even if cost-efficient, can contradict the specific needs or preferences of some members.

More broadly, the French public hospital system faces numerous difficulties, largely inherited from policies implemented over the past two decades. One such example, frequently cited by media of every political inclination [16] [17] [18], is the constant hospital beds deletion. This decrease, often attributed to successive budget reforms, also results from positive developments: medical advances have allowed for faster care and shorter hospital stays, justifying a partial reduction in reception capacities. However, this decrease remains a national average that masks significant disparities and does not accurately reflect the realities experienced in some hospital departments. It is not uncommon to observe times of saturation, with patients placed on beds in hallways due to a lack of available rooms, revealing resource management issues at the

local level. Furthermore, hospital staff, and particularly caregivers (nurses, nursing assistants, etc.), face serious difficulties. In addition to a relatively low level of remuneration, up to 40% lower than the one observed in other European countries such as Germany, according to OECD data, in purchasing power parity [19], these professionals are under increasing pressure due to the increasing staff shortage. Retirements or resignations are often not replaced, forcing the remaining employees to absorb the workload without any salary increase. This deterioration of working conditions contributes to a worrying phenomenon: many young professionals leave the profession after a few months or years [20].

In 2024, the French Court of Accounts issued new recommendations aimed at mitigating the structural difficulties encountered by French hospitals, by re-centering their financial and administrative strategy around the THGs. They reiterate the initial goals of the THGs, asserting that they are best equipped to address future challenges like the aging population. To this end, the French Court of Accounts encourages the creation of territorial health centers and shared teams among the members of the THGs, already planned by the 2016 law but never applied, to compensate for the growing shortage of healthcare staff. They also emphasize that, despite the persistent pressure on bed availability, a certain easing could only be considered on the condition that the "ambulatory shift" continues. That is to say, developing care outside of traditional hospitalization, and improving the coordination between the various healthcare actors at the territorial level: hospitals, medico-social structures, and general practice. The objective is clear: optimizing the distribution of patients, reducing the length of hospital stays, and freeing up beds, while preserving the quality and safety of the provided care.

## 2.2 Issues and Evolution of Cybersecurity Practices and Regulations in Hospitals

The computerization of hospitals began in 1982 with the launch of the Information Systems Medicalization Program [21]. This program aims to "describe in a synthetic and standard-

ized way the medical activity of healthcare facilities, based on the recording of standardized medico-administrative data in a common format". Despite the somewhat vague wording, this text marks a first step towards the digitization of hospital practices, to accelerate, structure, and homogenize care pathways using digital tools. However, although it profoundly modified the operating methods of healthcare professionals, the program does not consider the newly implemented systems' security.

After several years of gradual digital transition, numerous academic reports and articles began to raise concerns about the lack of consideration for issues related to systems and data security. This negligence affects, directly or not, the patient's data protection. The French Data Protection Act, adopted in 1978 [22], four years before the start of hospital computerization, already defined obligations for the processing of personal and sensitive data, one of cybersecurity's fundamental pillars. This law, visionary for its time, should have served as a solid foundation for securing HIS (Hospital's Information System) by drawing on its core principles. This law did not undergo major changes before 2016 and 2018 [23] and the discussions surrounding the GDPR [24], of which it would even become one of the inspiration sources.

The thesis written by Mr. Ormancey in 2003 and dedicated to IT risk management in hospitals [25], was among the early works to underscore the HIS increasing complexity, even though they were only in their early stages. It also emphasized the lack of interest in improving HIS security, which was often relegated to the background compared to the priority given to the infrastructure's rapid improvements. At the time, these security issues were only just beginning to emerge in discussions. However, while technical improvements could generate a direct return on investment for institutions, it was much more difficult to financially justify cybersecurity investments, the benefits of which were uncertain and difficult to quantify. An overly ambitious IT security policy could represent a significant cost for hospitals, without any guarantee, especially since cyberattacks, and in particular ransomware, were still rare. According to the National Agency for the Information Systems' Security (ANSSI), the number of cybercrimes has risen steadily over the past decade and continues to grow in 2024. For

instance, the volume of DDoS attacks in 2024 significantly exceeds that of previous years (cf. figure 2.2) [26].

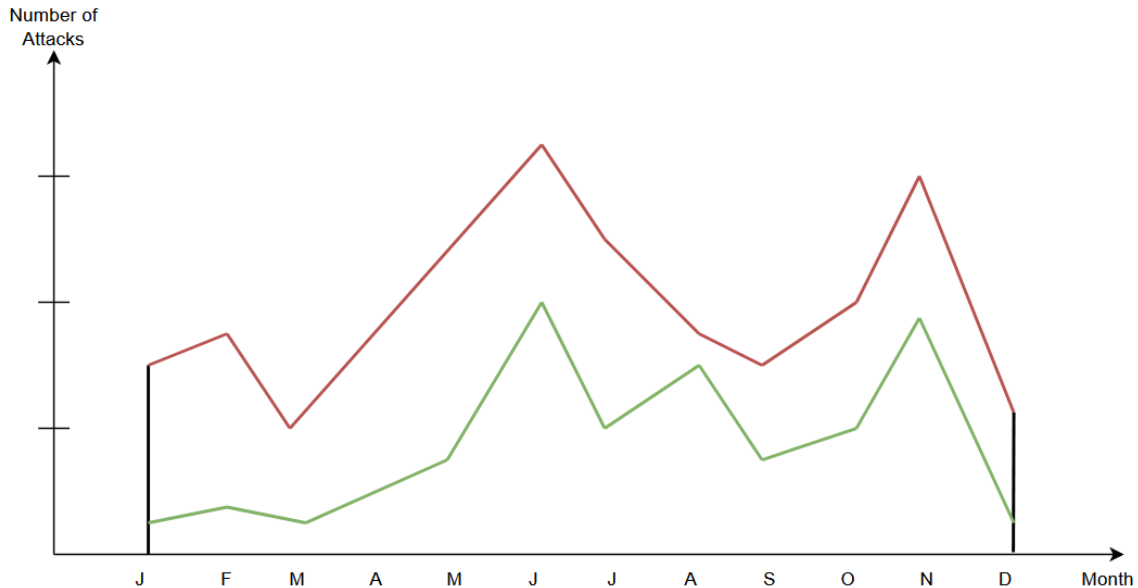


Figure 2.2: Number of DDoS attacks observed by ANSSI against French targets

Subsequently, HIS were kept up to date, to some extent, through a series of plans and programs aimed at modernizing existing infrastructures. Among them, the "Hospital 2007" plan allocated approximately 3% of its funding to a few large-scale projects such as the computerization of patient records [27]. Its successor, the "Hospital 2012" plan, allocated 15% of its budget to HIS modernization. In parallel, the "Digital Hospital" plan, also launched in 2012, followed this effort by laying the first foundations for a genuine data protection policy in healthcare facilities [28].

Finally, several programs, not specifically focused on cybersecurity, such as HOP'EN [29] and HOP'EN 2 [30], were implemented with the stated primary objective of "putting digital technology at the service of health.". Despite the fact that they do not directly target the security of information systems, these programs are indirectly contributing by replacing obsolete and vulnerable infrastructures with more recent solutions, often more secure by default. In addition, the 2021 "Healthcare Ségur" [31] allocated a budget of 350 million euros to strengthen

hospital cybersecurity. To access this funding, institutions had to commit to dedicating between 5% and 10% of their IT budget to cybersecurity measures. The Ségur also listed THGs as operators of essential services, thus subjecting them to stricter cybersecurity requirements, coupled with an obligation of compliance [32].

However, the competent authorities, such as CERT-SANTE [33] managed by the Digital Health Agency (ANS), the ANSSI, or its European equivalent, the European Union Agency for Cybersecurity, continue to warn about the risks that HIS are still facing. Although very small companies and small and medium-sized companies are the most affected by ransomware attacks, healthcare facilities still account for 4% of this type of attack in France [26]. This is partly explained by the significant lack of cybersecurity professionals, from which these sectors particularly suffer [34]. The data hosted by healthcare facilities is particularly prized by cybercriminals because they are worth a lot on parallel markets and can be used to commit other offenses, such as identity theft or various frauds [35]. These threats concern all European countries, which, although less targeted than France, remain highly exposed [36].

## 2.3 Regulatory Framework: The CaRE Program

The CaRE program, the result of a partnership between the French Ministry of Health and Prevention and the French Ministry of Digital Affairs, constitutes "an unprecedented action plan to strengthen the cybersecurity of healthcare facilities and medico-social structures." Developed by a group of experts in consultation with field professionals, based on the analysis of past cyberattacks [37] and related research [38]. This program aims to address shortcomings in the protection of information systems against the cybercriminal threats weighing on the healthcare sector [7]. With a budget of €750 million by 2027, it is structured around four strategic axes and twenty key objectives [39]. Each of these axes plays an essential role, without which the program's impact on hospital cybersecurity would be diminished. Together, they cover all the necessary levers to sustainably embed these new cybersecurity measures in the hospital environment. This includes the integration of cybersecurity requirements into the governance

of establishments, the continuous evaluation of existing systems, the pooling of resources within the THGs, the allocation of dedicated cybersecurity budgets, the implementation of targeted training at all hierarchical levels to raise staff awareness, as well as the securing of existing systems through the adoption of good practices to reduce the risks identified in section 2.2.

More than a set of technical prescriptions, this program encourages establishments to consider cybersecurity as a strategic issue. It proposes a change in posture: moving from a logic of reaction to a logic of anticipation, by equipping healthcare structures with the capacity to absorb an attack and limit its impact, both on their operation and on patient pathways.

To this end, healthcare facilities have a certain degree of freedom regarding the implementation of the CaRE program measures. Depending on their needs, they can recruit dedicated personnel or train existing teams. Regarding the remediation of vulnerabilities, a catalog of solutions and tools carefully selected by the CaRE Task Force is made available to hospital management and HIS teams. These solutions, all compatible with the program's requirements, allow establishments to choose those that best meet their specific constraints (budget, ease of deployment, durability beyond the program, technical support, etc.) [40]. The vast majority of these tools are offered by third-party vendors specializing in cybersecurity.

The long-term viability of the CaRE program is also ensured by the integration of its success criteria into the requirements or objectives of other certification processes that hospitals must imperatively satisfy to continue operating. Among these certifications, that of the High Authority for Health (HAS) is the most crucial. Conducted every four years, it aims to guarantee "the quality and safety of care as well as all the services provided by hospitals and clinics in France" [41]. In its 2025 framework, certain criteria specifically target the HIS. This is notably the case of Criterion 3.1-07, which states in its introduction that "the establishment conducts digital security audits and cyber crisis exercises to manage an action plan", a requirement that directly aligns with the objectives of the CaRE program [42].

### 2.3.1 1st Axis: Governance and Resilience

The CaRE program seeks to establish robust and collaborative governance based on local and national actors, both public, such as ANSSI or healthcare facilities, and private, such as industrial companies and service providers. Led by the Digital Health Delegation, which oversees the entire program, its role is to set the course that all actors will follow to blend national strategic orientations and on-the-ground realities best. Specifically, the national steering committee, which meets monthly, aims to bring together all stakeholders by progressively integrating representatives from hospital federations, user associations, as well as a newly created community of Chief Information Security Officers (CISO). This organization allows for collective, rapid, and effective management, necessary to address current complex challenges.

At the healthcare facilities level, this cybersecurity strengthening involves integrating it into their governance strategy. One of the program's central requirements is the recruitment or training of CISOs in all establishments to ensure this mission, which must be completed by 2025 for all THGs. This evolution is supported by increased regulatory structuring, notably through the integration of cybersecurity into the Multi-Year Contracts of Objectives and Resources, which govern the formalization of objectives and attached financial resources to anticipate the medico-social offer [43], signed between the Regional Health Agencies and the establishments. The latter are now encouraged to include specific cybersecurity objectives in their establishment project.

In parallel, as mentioned in the introduction, the HAS has amended its HIS component of its certification process by integrating criteria dedicated to cybersecurity and stemming from the program. To ensure its application, specialized visiting experts have also been recruited by the HAS to conduct targeted audits throughout 2024.

However, all advances in governance would have little real impact without a reinforced focus on the establishments' resilience. The program seeks to embed a culture of resilience that goes beyond the obligations defined by the various programs and certifications, to be integrated both into the daily practices of the various system users and into the management strategies

of the establishments. In particular, the development and updating of Activity Continuity and Disaster Recovery Plan (ACDRP) as well as the creation of a cyber white plan, specific to HIS and cybersecurity, are becoming a priority to guarantee the safeguarding of critical functions in the event of a crisis. A national ACDRP kit has notably been designed to help structures formalize their approach. These tools should allow for a rapid restoration of activity while ensuring the continuity of care in a degraded environment. In addition, crisis simulation campaigns, the funding of which is supported at the regional level, are made mandatory by the program to concretely prepare personnel for simulated major crisis events.

Finally, in a logic of continuous improvement, the program also requires establishments to implement a self-assessment approach to their cyber maturity. A national self-assessment framework is provided, with this program, to identify their priorities and build an adapted roadmap. This tool, which must be adopted by all structures by mid-2025, has the main objective of facilitating the gradual adaptation to the requirements of the European NIS 2 directive and providing means to anticipate the implementation of future directives and laws. Ultimately, the objective for the establishments will be to rely on this self-assessment to update their cybersecurity action plan.

### **2.3.2 2nd Axis: Resources and Mutualization**

The success of the program's objectives and future missions largely depends on the healthcare sector's ability to become more attractive and attract talents in the digital and cybersecurity fields. Aware of this tension, the program notably emphasizes the sustainability of human resources while seeking to value new profiles. Pending the results of the measures put in place to increase attractiveness, the adopted strategy is mainly oriented towards the pooling of resources among the members of a THG and, more generally, among healthcare facilities. This approach, while relying on existing resources, guarantees consistent support for all establishments.

Convergence within the THGs constitutes the main lever actionable by the authorities to encourage the THG's leading establishment to play a driving role, notably via the CaRE funding

calls. This establishment is responsible for its members' application to the CaRE program and ensures that they achieve the set objectives. Each domain mentioned in section 2.3.4 is subject to quantified objectives that each THG's member must achieve for the THG to be eligible for funding. In other words, the failure of a single member leads to the collective failure of all members within the THG.

The major question regarding the digital professions in healthcare attractiveness is being addressed head-on. Indeed, a revaluation of the salary scales for hospital engineers came into effect by decree a few months after the program's announcement [44]. In addition, forward-looking job and skills management tools are being made available to hospital management to ensure the sustainable integration of recruits.

Finally, to ensure the sustainability of this transformation, it is essential to recognize the cyber challenge from a budgetary perspective. Without the allocation of at least 2% of the establishments' overall budget to digital and cybersecurity activities, this transformation risks being neglected in favor of medical activities, which generate more significant revenue. Although this target is already met in some, it is being progressively extended to encompass all establishments by June 2025. Such a transformation requires the involvement of all levels and all the means available to Hospitals in France to ensure that it meets the specific needs of each structure and that it is properly proportionate. The objective is twofold: to anticipate and sustain the resources dedicated to digital transformation, while ensuring the hiring and integration of qualified personnel specifically dedicated to this transformation.

### **2.3.3 3rd Axis: Awareness**

This Axis addresses the problems related to a lack of awareness regarding cyber risks by placing the training of all hierarchical levels at the heart of its action. By holding directors and department heads responsible and by designating them as guarantors of good cybersecurity practices, the program aims to compel establishments to comply with these new requirements. Furthermore, the training of all personnel, at all levels, contributes to the sustainability of the

measures by integrating caregivers, administrative staff, and technicians into a daily approach of awareness and acquisition of cyber reflexes. The objective is that they consider themselves, in the medium and long term, as key players in the cyber defense of the establishment.

To address this challenge, targeted awareness campaigns are being deployed at national and territorial levels. Testimonials from establishments that have suffered cyberattacks are also being highlighted, as their feedback is crucial in raising awareness among hospital directors. These frequent examples serve as a reminder that actions must be taken, and can act as a wake-up call.

Establishment management also has the responsibility to ensure the continuous awareness of staff and the implementation of IT hygiene measures. To assist them, adapted educational resources, developed with feedback from the field, are made available to them. The CISO is at the center of this awareness policy as they are responsible for creating, implementing, and leading training dedicated to HIS security. More broadly, the community of CISOs aims to strengthen the visibility of their role, to make them recognized interlocutors by management, and to create a network of peers capable of sharing best practices.

#### **2.3.4 4th Axis: Operational Security**

This final axis's goal, with a strong technical component, is to concretely address the intensification of cyberattacks, particularly ransomware and data exfiltration carried out by organized groups. This involves correcting existing vulnerabilities, deploying advanced detection technologies, and strengthening IT recovery capabilities in the event of compromise. This axis is divided into four main domains, defined by the CaRE Task Force in close collaboration with field professionals. The first domain was published at the program's announcement, while the following ones are gradually made public at the end of each phase. Furthermore, this axis also integrates several complementary, less technical elements, which do not directly fall within one of the four domains but contribute to the overall effectiveness and reliability of the approach. Key measures notably include the creation of a dedicated team for monitoring and verifying

audits, to guarantee the effectiveness of the implemented solutions and the remediation actions undertaken. The monitoring of the "Cyber Baseline" (CB), recently established within the framework of the CaRE program and intended to evolve to remain in line with emerging threats, is also essential to ensure the sustainability of the undertaken actions. In addition, funding is planned to encourage establishments to achieve the objectives set by the CB.

As an application is only valid for a single domain, establishments wishing to apply to several domains of the program must submit a separate file for each of them. Each application implies a firm commitment to adhere to a strict timetable, a prerequisite for being able to benefit from the allocated funding. The targets of the first domain [45] are two critical attack vectors: the unintentional exposure of establishments' services on the Internet and the vulnerability of technical directories, mainly the AD, which can be exploited to obtain elevated privileges within hospital information systems.

In parallel, specific objectives are set to validate eligibility for funding. Among these obligations is the regular conduct of security audits. More precisely, the AD must be audited every 45 days, while the system's Internet exposure must be assessed every two months. To be considered compliant, the last two consecutive AD audits must reach at least security level 2 as defined by ANSSI, and no critical vulnerability must have been detected during the last two Internet exposure audits.

Establishments must also self-assess using the oSIS tool [46], which allows for the collection, via forms, of precise data for each member of a THG. This data is then used by the team in charge of the CaRE program at the THG level to keep track of the remediation actions undertaken and the overall improvements made. They are also required to plan and conduct, at least once a year, a cyber crisis management exercise. No minimum level of difficulty is imposed for this exercise, but its regularity is mandatory. Finally, establishments must monitor maturity indicators, notably the proportion of the budget allocated to digital technology. For THGs in particular, coordinated governance and an AD convergence strategy are also required to structure and harmonize the cybersecurity approach at the territorial level.

The actions of the following domains are subject to in-depth discussions among the various stakeholders of the CaRE program to refine the definition of needs and adapt the objectives, taking into account the results obtained, as well as the difficulties encountered during and after the implementation of this first domain. Only general pieces of information are available at the moment.

The second domain aims to strengthen the capacity of healthcare facilities to rapidly detect intrusions into their information systems. Attackers frequently target workstations, often outdated or using obsolete, or unupdated, operating systems. These machines constitute privileged entry points during the intermediary phases of an attack, a period during which attackers seek to escalate their privileges to take control of the HIS. It is therefore essential to deploy surveillance and alert mechanisms both on these workstations and on the network to block attacks before they reach critical systems. Beyond the technical aspects, the program also encourages a dynamic of cooperation: the sharing of information on threats between establishments allows each to benefit from alert signals identified elsewhere. This pooling of feedback and indicators contributes to raising the overall level of detection and increasing the speed of response throughout the healthcare sector.

Remote maintenance access points are a common attack vector in healthcare facilities. Used by many service providers to remotely administer equipment or software, they represent a major risk if not rigorously secured, as they allow direct access to critical infrastructures. This is why they are the third domain's target. The challenge is to transform these 'open doors' into strictly controlled, monitored, and traced entry points. This could involve the implementation of strong authentication, systematic logging of connections, recording of actions performed, as well as precise and controlled segmentation of access rights. By strengthening the control over these sensitive access points, establishments significantly reduce their attack surface and reinforce the integrity of their information systems.

Finally, facing the growing threat of ransomware, the fourth domain's objective is to ensure business continuity, which must rely on a backup strategy that is both robust and resilient.

During an attack, cybercriminals aim to compromise not only production data but also backups to block any possibility of restoration. It is therefore essential to deploy air-gapped backups, or other, less costly solutions, to improve protection against ransomware attacks, for Instance [47]. These solutions also need to be tested regularly to ensure their reliability in a real-world situation. This domain could emphasize establishments' active preparation for critical incidents, including the development of ACDRP, the implementation of rapid restoration procedures, as well as the prioritization of essential applications and services.

### 2.3.5 Insights from a Service Provider

This subsection illustrates the functioning of the CaRE program from a service provider's perspective. It is based on the answers provided by Mr. Schmitlin, partner at AKYL, and should therefore be interpreted with care. AKYL is a company offering several solutions, including an audit tool for the attack surface and internet exposure, specifically designed to meet the CaRE program's requirements. These solutions have been validated by the program teams and integrated into the official catalog. Mr. Schmitlin kindly agreed to share his feedback in the appendix A on how providers perceive the CaRE program and its operational deployment.

The participation of companies in the CaRE program occurred in a relatively natural way. Indeed, many companies listed in the solutions catalog have long collaborated with the French healthcare system. Some of them count former or current members of the CaRE Task Force among their staff, which nevertheless raises some legitimate questions about potential conflicts of interest. For these players already well-established in the sector, getting involved in the program was a logical continuation. Their main motivation lies in the desire to preserve their existing customer base in the face of competition and to prevent the market from being invested in by companies from other sectors or foreign countries, which could raise issues of digital sovereignty.

Participation in such a program is not insignificant. In AKYL's case, for example, the development of their solution required two months of work, followed by three months of testing

and adjustments in collaboration with pilot establishments. The scale of the CaRE program imposes significant development constraints: to remain competitive, companies must design solutions capable of meeting high standards of reliability. The volume of users to support requires the implementation of robust infrastructures capable of absorbing the number of audits, which represents a substantial, technical, and financial investment. On the technical front, the AKYL team notably faced serious stability issues related to the use of sovereign cloud offerings, which proved insufficient to meet the program's requirements, unlike the solutions offered by AWS or other GAFAM, for example. These numerous crashes significantly slowed down the deployment of their solution.

Furthermore, the very nature of the audits conducted involves the use of scanners on assets sometimes hosted by third-party providers, which can lead to a degradation of the reputation of the IP addresses used. This situation leads to blockages by certain security equipment, thus deteriorating the audit results. In addition, as the audit scope's definition is left to the healthcare facilities' discretion, incidents have occurred. In very rare cases, assets not directly belonging to client establishments were included in the audits without the explicit consent of their owners. This led to complaints filed against AKYL, highlighting the complex legal and technical issues raised by this type of large-scale exercise.

The question of the developed solutions' official certification has raised many questions. Although AKYL highlights on its website the conformity of its solution presented as "guaranteed compliant with the CaRE program domain 1" [48], this guarantee is not based on a certification issued by an official body. In reality, the tool's validation relied on feedback from the field, provided by various Regional Support Groups for the Development of e-Health (GRADEs) and pilot establishments that participated in the testing phase. In addition, the company reinforces this guarantee by mobilizing a cybersecurity expert, responsible for manually validating the audits that establishments wish to transmit to the ANS. It is important to emphasize that this absence of official certification is not due to a lack of initiative on AKYL's part, but rather on a choice made by public structures not to back up the proposed solutions. To date, no industrial

solution has been formally certified by an authority. Finally, to offer their solution to the CaRE program Task Force, a contact form was provided by the latter [49].

# 3 Overview of the Esquirol Hospital Center's IT Infrastructure

The Esquirol Hospital Center IT infrastructure is complex and hard to visualize, even at a high level. Figure 3.1 provides a schematic overview to aid in understanding the details discussed in the subsequent section. This HIS (Hospital's Information System) infrastructure spans eleven geographically dispersed sites of varying sizes and includes approximately 1,400 workstations. It currently lists 1,957 user accounts, of which only ten are administrative accounts, within the AD (Active Directory). The client machine fleet still consists of 53% Windows 10 workstations, although the proportion of Windows 11 machines, currently at 36%, is steadily increasing, driven by the equipment's gradual replacement. On the server side, the majority have been migrated to Windows Server 2022, although some servers still run on Windows Server 2016 or 2019. This retention is unavoidable as compatibility with specific professional applications, sometimes obsolete or poorly maintained, must nonetheless be ensured. In parallel, the hospital has provisioned specific workstations for teleworking and on-call duty. These devices are equipped with a Virtual Private Network (VPN) access, providing a user experience identical, but slower, to that of a workstation used on-site. There is also a growing adoption of "thin terminals": these terminals, lacking local applications, connect to remote servers for software execution via virtualization solutions such as CITRIX. This solution, for example, enables the centralization of applications and desktop environments, minimizing local storage and software installation on individual workstations.

The HIS hosts over 80 business applications, apart from those used by the HIS team. Access to these applications is restricted to authorized users, with granular rights management per application. In some cases, responsible users can even administer specific parameters of their applications. This diversity and customization make the application environment's management complex and demanding for the IT teams. System updates are entirely managed centrally and deployed automatically via Group Policy Objects (GPO), running notably when workstations are shut down. Finally, certain entities of the Hospital Center have their own websites, the maintenance of which is either provided by an external service provider or has been neglected for several years. These websites mainly serve as information showcases for the activities of the concerned departments. The HIS also provides the staff with various digital tools, such as a professional email system, an internal telephone system, an intranet, and a centralized document database, which are essential for the proper functioning of the hospital services.

In network architecture, the demilitarized zone (DMZ) refers to a subnetwork designed to isolate internet-facing services from the rest of the internal information system [50]. This area of the network contains so-called "untrusted" machines because they are accessible from the internet and therefore more exposed to attacks. This is in contrast to the internal network, which contains trusted machines and servers. Trusted machines are those authorized to access other machines and servers based on their needs and granted permissions; however, this notion of trust in no way guarantees their infallibility [51]. This zone-based design helps reduce the risk of compromising the internal network if an online service is compromised.

The ANSSI (National Agency for the Information Systems' Security), in its guide concerning the SI's interconnection to the internet [52], recommends the systematic implementation of a DMZ for any IS hosting services accessible from the internet. This DMZ must be rigorously segmented to isolate the different services it contains. Services should not be able to communicate with each other, or only in a strictly controlled manner. To achieve this, internal firewalls restrict and filter inter-service traffic. Perimeter firewalls, in opposition to internal firewalls, are specifically used between a trusted zone and a DMZ, and between the DMZ and the internet,

on the other hand [53]. Several virtual firewall instances are recommended to compartmentalize the management of different incoming and outgoing flows, hosted services, VPNs, and to customize the security associated with the different firewalls. The DMZ architecture deployed within the hospital largely complies with the recommendations formulated by ANSSI, except for the use of multiple perimeter firewalls. A simplified diagram of this architecture is presented for illustrative purposes in figure 7.1.

Protection could be enhanced by using next-generation firewalls that offer more advanced features like deep packet inspection, which allows for the analysis of packet content beyond simple headers to detect the presence of malicious or abnormal content. As the Hospital uses a proxy and a reverse proxy, incoming and outgoing packets could be intercepted at their respective levels and then deconstructed. However, in France, the use of deep packet inspection is regulated by the General Data Protection Regulation [54], which prioritizes user privacy and data confidentiality, even in a professional context. This prohibits any form of intrusive surveillance without legal or proportionate justification.

Web Access Management (WAM) refers to the set of mechanisms used to control and secure user access to the web resources of an information system. It is a centralized authentication and authorization solution whose goal is to ensure that only duly authorized individuals can access the web applications made available [55].

The operation of WAM is based on security rules configured by administrators, following a logic comparable to that of user groups in an Active Directory. Groups are created based on, for example, their profession, and each group is associated with specific access rights to a restricted set of applications. After authenticating on this portal using specific credentials, the user only sees the applications they are authorized to access. This preliminary filtering constitutes a first layer of security, upstream of the authentication specific to each application. Services accessible via WAM include the remote maintenance platform, reserved for service providers, and an internal cloud storage service for the hospital.

External service providers access the hospital's internal resources via a jump server [56], an

intermediary server specifically designed to serve as a secure entry point to critical systems. This setup, commonly used in sensitive environments, allows for the administrative connections' centralization and limits the direct exposure of internal machines to remote access. To manage these connections, the hospital gives providers access via a VPN, allowing them to connect to the jump server located in the DMZ. From this server, providers can then establish a second connection to interact with the systems assigned to them, as the jump server has the right to connect to all servers that any provider might need. However, this architecture presents significant security vulnerabilities. The system relies primarily on restrictive password management: providers only receive the credentials for the servers they need to work on, without knowledge of those for other systems. Nevertheless, this approach proves insufficient in the event of a provider account compromise. An attacker with these credentials and VPN access could not only penetrate the hospital's DMZ but also exploit the jump server as a pivot point to reach other internal resources and thus compromise the entire HIS.

The protocols Virtual Network Computing (VNC), Remote Desktop Protocol (RDP), and Secure Shell (SSH) [57] are commonly used solutions for the IS's remote administration. Although they share a common goal: enabling access to a remote machine, each has distinct characteristics, and they must be used simultaneously to effectively cover all needs.

VNC and RDP both allow the transmission of the remote desktop environment's graphical reproduction, thus facilitating visual interaction with the user interface. However, VNC is particularly popular in organizations offering technical support services (hotlines) due to its ability to take control of a workstation without disconnecting the active user. This specificity allows technicians to resolve an incident while maintaining a dialogue with the user, or even explaining the manipulations performed in real-time. In contrast, RDP, developed by Microsoft, is specifically optimized for Windows environments, making it particularly suitable for the administration of Windows servers. It offers better performance in terms of display, stream compression, and remote resource management compared to VNC. Finally, the SSH protocol is the reference solution for administering Linux servers. Unlike VNC and RDP, it

relies exclusively on a command-line interface.

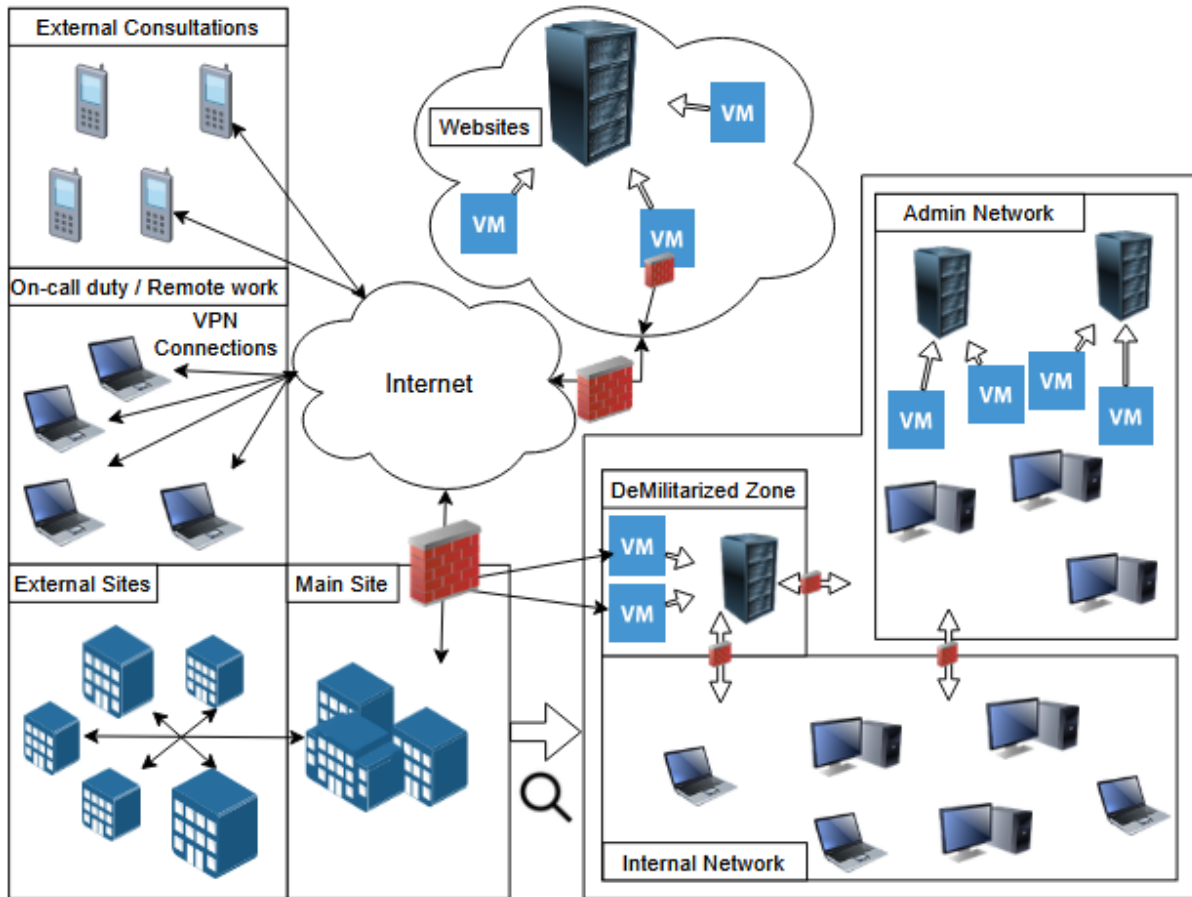


Figure 3.1: High-level diagram of the Esquirol Hospital Center IT infrastructure

## 4 Auditing Tools and Results

As the hospital lacks the necessary human resources to conduct regular penetration tests and audits on its infrastructure, these are carried out by external service providers not affiliated with the hospital environment. In practice, the overall scope is divided into several sub-sections such as Wi-Fi, internet exposure, Active Directory, network equipment, and the connections to these pieces of equipment. Although the hospital's infrastructure is never audited in its entirety at a single point in time, these regular audits still make it possible to correct a significant number of flaws. In addition to this, phishing audits are carried out, which aim to simulate the sending of fraudulent emails to medical and non-medical staff to test their reaction and plan future security training schedules to be provided based on their results. For the audits requested by the CaRE program, the ISARS's solution, for the Active Directory audit, and AKYL for the attack surface and internet exposure were selected over tested solutions that did not meet the specifications.

In addition, a cyber crisis exercise, made mandatory by the CaRE program, is organized annually. This exercise tests the staff's responsiveness to a larger-scale attack and how they implement the various actions planned by the cyber white plan. This exercise can include different difficulty levels and must adapt to current threats. The goal is to immerse staff in crises by introducing, for instance, a demilitarized ransomware, with no real impact on the hospital, that would block affected machines [58]. This type of exercise is extremely costly for a healthcare facility that cannot dedicate a portion of its team, for several months, to the creation of such an exercise. Solutions offered by providers such as AUCAE [59], are thus chosen, but

at a very high price. Added to this is the human cost of mobilizing the necessary personnel for this type of exercise. All directors, as well as most healthcare and administrative managers, are notified, prior training is also necessary to prepare for the exercise, and a temporary degradation of working conditions must be taken into account.

## 4.1 Tools' Internal Mechanisms

### 4.1.1 Mechanism Behind Attack Surface Mapping

AKYL is a cybersecurity consulting and audit firm, founded in 2022 and based in France. Having no partnerships with software vendors, this company presents itself as independent. It assists organizations in protecting their IS (Information System) by offering various services such as risk analysis, IS policies, penetration testing, phishing campaigns, incident response, threat intelligence, and team awareness training. The company is also recognized by the "ExpertCyber" [60] and "France Cybersecurity" [61] labels, attesting to both its French origin and its cybersecurity expertise. These distinctions guarantee its skills in system security, maintenance, and technical support [62]. The technical solution's in-depth analysis was also made possible thanks to the answers provided by Mr. Schmitlin in his interview (full transcript available in Appendix A).

The company's solution is a type of tool called Early Warning System, developed specifically for the CaRE program but intended to evolve. During the creation and testing phases, numerous feedback from pilot healthcare facilities, such as GRADeS (Regional Support Groups for the Development of e-Health) [63] and THGs (Territorial Hospital Groups), were integrated and led to adjustments, particularly regarding vulnerabilities' classification, the authentication types' detection, the results' presentation, and the monitoring of modifications made by analysts. This collaboration helped to adapt the tool to the specific needs of the healthcare sector.

From a user's perspective, all administration and usage tasks are carried out through a clean and clear web interface. The solution offers the ability to add assets, IP addresses, and

domain names that the institution considers to be within the scope of the CaRE program. Subsequently, an audit can be automatically configured on these assets once a week; this audit will serve as evidence for the result validation stages of the CaRE program. Audits can also be manually launched at the users' discretion and without any limitations. Once a certain number of vulnerabilities have been corrected, the intervention of a human expert can be requested to validate the results and reclassify certain vulnerabilities that were detected but are not problematic for the CaRE program's requirements. However, if any adjustments are made to the vulnerabilities discovered by the software, these modifications will only apply to the weekly audit; the vulnerabilities will not be reclassified in the manual audits. This human validation is directly integrated into the platform via a messaging system, which differentiates it from some competitors and the solutions previously used by the hospital that required direct contact at the THG level.

AKYL's solution is based on software developed by the company that combines several open-source cybersecurity tools. Among the tools integrated during this development, Nmap, used for host and active service reconnaissance on a network, is employed to scan the ports of the assets registered by the user on the web interface and identify active services that could represent a vulnerability due to either an outdated version or a weakness in the application security measures. Nuclei, used in conjunction, is a tool that allows for template-based scans to quickly detect known vulnerabilities and misconfigurations on the services identified by Nmap. The Shodan Application Programming Interface (API) is used to correlate the information found by the previously mentioned tools with a vulnerability database to establish an initial list of vulnerabilities to be corrected, which will then be reduced based on the program's requirements.

AKYL's software also performs a search for assets related to the audited institution that are unknown or, in any case, not added to the declared list. To do this, it leverages the Subfinder tool, which is specifically designed to discover a wide range of subdomains by querying various passive data sources such as DNS records, SSL/TLS certificates, search engines, and past

attack datasets. Its effectiveness is significantly increased by the integration of the Security Trails API, which offers a historical and comprehensive view of DNS records, allowing for the identification of subdomains that may no longer be active but could potentially be reactivated or forgotten in the organization's inventory [64]. The service is also designed to examine the configuration pages of web services when it detects them. For example, the presence of standardized configuration files such as the Microsoft Azure Domain Tenant ID, accessible via the URL "https://login.microsoftonline.com:443/poleressources-clana.fr/v2.0/.well-known/openid-configuration", can reveal sensitive information about the infrastructure and identities used by the organization, thus representing a potential entry point for attackers.

This quick overview of the tools and APIs that make up this solution is obviously just scratching the surface, as it's based only on what was disclosed by Mr. Schmitlin. It goes without saying that other tools were used and that modifications to these tools had to be made to adapt the final tool to the infrastructures of healthcare facilities.

Maintaining HIS's (Hospital's Information System) integrity is a top priority during the execution of audits. Indeed, the actions performed by AKYL's tool are nothing more than what an attacker could carry out during the system enumeration phase. Incorrect configuration of this tool could lead to a DDoS attack on the hospital's services. The company has implemented a testing policy with pilot healthcare facilities to adjust the Nmap and Nuclei commands, which offer numerous customization options, to avoid disruption or unavailability of critical services while thoroughly analyzing all registered assets. These tests have made it possible to identify and correct any unexpected behavior of the scanning tools and to determine a limit on the concurrency of requests and volume per minute. Finally, even though the rates have been tested and are considered safe, customization options are still available to users to minimize the audit's footprint on the targeted systems.

My following questions concerned a sentence visible on the promotional page for this audit tool: "Our risk-free scanner for your assets detects obvious vulnerabilities that an attacker could exploit." [48]. As specified in the CaRE program specifications in section 2.3, only passive scans

are authorized, which leads to a certain number of limitations. The solution will generally not detect vulnerabilities that require authentication to be exploited, complex web vulnerabilities that only manifest through specific interactions with the application, such as SQL injections or XSS flaws, or assets and vulnerabilities located behind security mechanisms such as web application firewalls [65] that block malicious requests. Assets not exposed on the internet or those that do not respond to scan requests will also not be identified.

Experts can intervene, on healthcare facilities' requests, to add to the feedback provided without impacting the systems by acting more offensively on them. Finally, although it would be easy for the company to develop this solution to increase the number of vulnerabilities detected or expand the search surface. However, doing so would make this tool less attractive to healthcare facilities, which would certainly prefer the competitors' solution, as it is simpler to satisfy.

The correlation between the findings of AKYL's solution and Common Vulnerabilities and Exposures (CVE) [66] is an important aspect of criticality assessment. When a detected vulnerability corresponds to an existing CVE, this information is integrated into the report. It is then supplemented with a standardized description of the vulnerability, recommendations for remediation, and often a Common Vulnerability Scoring System (CVSS) criticality score [67]. This CVSS score, when available, is an effective way to establish the criticality level assigned to the vulnerability. However, many vulnerabilities, particularly those related to configuration errors, are not associated with a CVE. In these cases, the assessment of the criticality level relies on expert analysis conducted by AKYL's cybersecurity analysts. They take into account the context of the discovery, the potential impact on the confidentiality, integrity, and availability of the HIS, as well as the specific guidelines of the CaRE program specifications. Thus, even in the absence of a CVSS score, a rigorous and contextualized assessment is carried out to determine the level of risk associated with each identified vulnerability.

### 4.1.2 Active Directory Enumeration and Analysis Process

Two solutions were used during the audits conducted on the Active Directory. The first, which will serve as the reference for the CaRE program, is the Active Directory Security service [68], offered by the ANSSI (National Agency for the Information Systems' Security). The stated objective of this service is "to support the security of critical actors' Active Directory" [69], and it is based on the open-source tool ORADAD [70], also developed by the ANSSI.

ORADAD, or "Automatic Active Directory Data Recovery Tool" is a program developed in C++ by the ANSSI. Designed to facilitate Active Directory environments' security audits, it interacts with the directory via the LDAP protocol to automatically extract critical information, such as the object structure, trust relationships, permissions, privileged groups, as well as scripts and files present in the SYSVOL folder. The tool is configurable via an XML file, allowing for the audit parameters' specification and the limitation of the collected data's scope. The results obtained, a '.mla' file, are then transmitted to the THG, which possesses a second program allowing for the recovered data's translation into a report in HTML format. This report is then returned to the IT department of the THG member, who can then analyze it and implement corrective measures.

This tool, just like the second solution, ISARS [71], used by the THG, relies on a list of control points rigorously defined by the ANSSI. The purpose of this list is to identify the most critical potential vulnerability vectors within an Active Directory environment and to guide the corrective actions to be implemented. It is structured around five maturity levels, of which only the first four have been published to date, each representing a step of progression towards a state-of-the-art secure AD (Active Directory). The list is continuously enriched by the ANSSI, which adapts it to new threats and attacks.

Level 1 aims to correct the most critical and directly exploitable vulnerabilities in the Active Directory. It consists of fundamental and simple-to-implement security measures that every organization should apply. This level includes, for example, the detection of dangerous permissions on sensitive objects such as domain controllers, the presence of privileged accounts

whose passwords never expire, or poorly configured authentication delegations. The second level reinforces this security by focusing on elements often neglected in default configurations. The goal here is to limit the attack surface and eliminate structural weaknesses. This level targets, among other things, active user accounts with weak Kerberos encryption using the DES algorithm, for example, and insufficient domain password policies. Level 3 seeks to refine and strengthen controls over the AD. Attention is focused on the quality of access control and the actual state of Active Directory objects. It is at this level that the presence of privileged accounts that are not members of the "Protected Users" group or the presence of objects with an inappropriate owner is verified. Finally, levels 4 and 5 represent the highest level of AD maturity. It imposes a rigorous compartmentalization and granular control approach, in line with the Zero Trust principle. The objective here is to prevent the propagation of lateral attacks or unauthorized privilege escalation. The actions necessary to validate the control points become very difficult to implement on older ADs due to the significant number of side effects with each modification.

The solution proposed by the company, ISARS, was chosen for several reasons. More intuitive to learn and use, automated, requiring less manual configuration, and above all, manageable by the hospital team without going through the THG, it offers a significantly superior user experience. It also far exceeds the requirements of the ANSSI checklist by integrating advanced controls not required by the CaRE program specifications, such as verifying the encryption level used for certificates based on their validity period, or the detailed analysis of permissions applied to GPO (Group Policy Object) concerning Domain Controllers (DC). In addition, ISARS also integrates a second audit tool that broadens the analysis beyond just Active Directory security. This tool also covers account management, the health status of Windows machines, as well as system administration practices. Thanks to this more comprehensive approach, the solution enables the identification of a wider spectrum of vulnerabilities and thus contributes to a better visualization of paths threats could exploit. The choice not to limit itself to the solution recommended by the ANSSI is part of a long-term sustainability strategy. Although

this solution represents a non-mandatory investment to meet the current requirements of the CaRE program, it will allow for the maintenance of a high level of security even after the program ends. Furthermore, unofficial information suggests that the requirement levels of the CaRE program could be raised in the future, particularly with the publication of new domains, even if these do not directly concern Active Directory security. Having a more comprehensive audit tool will facilitate the achievement of these new objectives.

ISARS also provides a web interface, allowing for the audit reports' detailed visualization. Although the content is generally comparable to that generated by ORADAD, the ISARS solution stands out due to its increased readability. Each maturity level is presented, with access to the list of points that comprise it. For each point, a gauge indicates the number of vulnerable elements identified. By clicking on a specific point, the user accesses a summary table displaying all the affected elements, accompanied by precise details for each vulnerability. ISARS is probably based on ORADAD with additional specific developments. However, e-mails have been sent to the hospital's contacts at ISARS to obtain further details on how their tool works. However, in the absence of a response, it has not been possible to provide a more detailed description of its operation.

## 4.2 Detailed Review of Audit Reports

### 4.2.1 Analysis of Exposed Services and Entry Points

The initial audit report provided by AKYL's solution in early October for the Esquirol Hospital identified 96 vulnerabilities, of which 58 were deemed critical, 6 high, 18 medium, and 14 low, as shown in the audit report summary in figure 4.1. These figures are primarily explained by the shared architecture chosen for hosting the websites, which, by definition, leaves numerous ports and services accessible from the internet, by default, multiplying the entry points [72] and artificially inflating the number of errors detected. To better understand these findings and their implications, it is necessary to place each category of vulnerability within the audited

infrastructure's context to propose appropriate corrective measures.

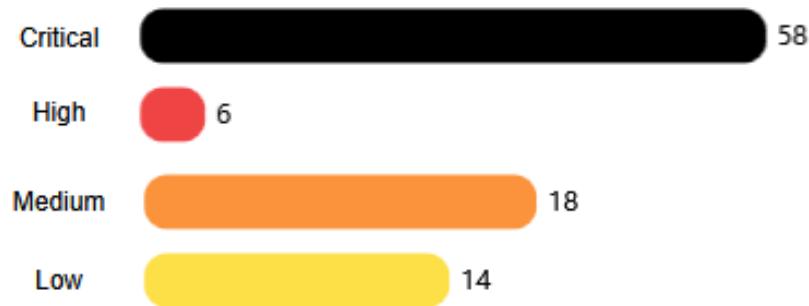


Figure 4.1: Attack Surface and Internet Exposition Report Summary

All services (SSH, FTP, MySQL, telnet, netbios-ssn, microsoft-ds, ms-wbt-server, etc.) are exposed without filtering on the shared OVH server, which generated a significant portion of the critical errors. The audit tool, due to its design, analyzes each declared asset independently. Therefore, all open ports are detected as belonging to distinct hosts, even though they are part of the same machine. The other part of the critical errors concerns the MySQL databases whose administration pages are publicly accessible without controls, potentially allowing brute-force attacks on credentials.

Among the few high errors, there is an expired and subsequently revoked internal SSL/TLS certificate, used by a portal of the Esquirol Hospital that is not compatible with Let's Encrypt automation. As the manual renewal of this certificate was not a priority since the portal is only accessible internally, this vulnerability was not addressed and was even downgraded from high to medium after validation by an expert from AKYL. There is also an unrestricted VoIP SIP service that is the subject of four high errors, potentially leading to call diversions or resource exhaustion, for instance [73].

The medium and low severity vulnerabilities, although having a more moderate impact, must also be addressed if a complete reduction of the hospital's attack surface is desired. Nearly half of the medium points concern the absence of DNSSEC on the domains, exposing DNS records to spoofing attacks or cache poisoning [74]. This problem's remediation simply

involved checking an option on the OVH administration panel, which also hosts the domain names. This modification has only advantages since the management of the protocol is never handled by the hospital, addressing the problems highlighted by Suranjith Ariyapperuma and Chris J. Mitchell [75]. The site's administration pages are exposed without protection against brute-force attacks, such as the implementation of CAPTCHA, limiting the number of attempts, or multi-factor authentication, leaving credentials vulnerable to automated attacks [76].

Finally, the low errors characterize vulnerabilities that might not be vulnerabilities. The majority of these errors concern the presence of configuration, backup, or log files (.editorconfig, .html, Thumbs.db, etc.) that are publicly accessible and could serve as evidence to exploit more serious flaws [77]. The remaining low errors concern the Wildcard TLS Certificates used to secure several subdomains. As a significant portion of the applications covered by these certificates do not allow the use of Let's Encrypt to automate certificate renewal, the use of a Wildcard greatly simplifies system maintenance and will therefore remain as it is.

### 4.2.2 Results of Active Directory Security Review

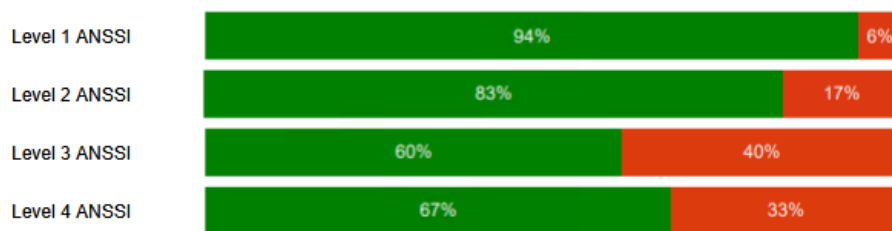


Figure 4.2: ISARS Active Directory Report Summary

The first audit report generated by the ISARS tool indicates, in figure 4.2, an overall maturity level of 1, with 94% of compliance, according to the ANSSI's assessment criteria. This result is encouraging as it reveals a very low proportion of major vulnerabilities. However, four critical vulnerabilities remain and require urgent correction as their exploitation could compromise all the resources of the HIS. Furthermore, only 17% of the criteria are not met at level 2, 40% at level 3, and 33% at level 4, highlighting the importance of implementing a progressive action

plan to rapidly move towards a state-of-the-art Active Directory security. This is confirmed by the ORADAD report, which shows the current level of the AD at the time of the audit, as illustrated in figure 4.3. The progression through levels represents a gamified approach, where resolving each issue earns points contributing toward advancement to the next level. This mechanism is similar to the percentage-based scoring used in the ISARS report.



Figure 4.3: ORADAD Active Directory Report Summary

The only errors identified at level 1 mainly concern the security of privileged accounts. Firstly, no password rotation has been implemented for these accounts, which constitutes a significant risk. Secondly, inadequate management of the "servicePrincipalName" (SPN) attribute has been observed: it is enabled on certain privileged accounts, which could allow, after a targeted attack, the retrieval of their passwords and lead to privilege escalation. Furthermore, excessive permissions persist on certain objects related to certificate templates, exposing the system to abuses such as fraudulent certificate requests. This could notably allow an attacker to impersonate an employee by posing as them via the authentication certificate of their smart card.

Level 2 reveals a still largely insufficient password management policy, particularly concerning their renewal, within the analyzed Active Directory environment. One domain is noted as being governed by an overly lenient password policy, the password for the 'Krbtgt' account has

not been renewed for over a year, and five servers are still using passwords unchanged for more than 90 days. Furthermore, although the impact is mitigated by the use of CPS cards for user authentication, no formal password management policy is enforced by default on active user accounts, which could lead to a vulnerability in the event of a temporary cessation of card use, for instance, in a major crisis. It is therefore essential to correct this weakness by establishing strict rules regarding the complexity and validity period of passwords.

At level 3, several significant shortcomings are observed: a significant number of Active Directory objects have an inappropriate owner, certificates using weak encryption algorithms are still in use, and numerous privileged accounts are not integrated into the 'Protected Users' group, which is crucial for strengthening Kerberos security.

Finally, at the most advanced levels, which assess the maturity and fine-grained segmentation of administration silos, the audit reveals vulnerabilities such as the presence of privileged groups' members outside the defined silos, as well as functional levels of the forest and domains that are too low. These limitations prevent the activation of advanced security mechanisms such as Smart Card Logon or the "Protected Users" group settings. To reach this level of maturity, it would notably be necessary to isolate all critical operations within bastions, according to ANSSI's recommendations for secure administration architecture. However, implementing these changes proves complex in the short term, as it would involve a complete redesign of the hospital's Active Directory, which was initially conceived without these architectural principles. Therefore, it was decided to correct as many of these weaknesses as possible without fundamentally altering the infrastructure.

# 5 Attack Surface and Internet Exposition Remediation

## 5.1 Requirements Analysis for the Virtual Private Server

Although the action phase of the CaRE program for Domain 1 began in March 2024, the report presented in section 4.2.1 dates back to early October. While several audit tools were tested and used for quite some time, none provided satisfactory. The first tool, recommended by the ANSSI, was deemed insufficient by the IS team of the THG (Territorial Hospital Groups). It was used as a temporary solution in the absence of a more suitable alternative. The second tool, PATROWL, also proved unsatisfactory. It failed to provide comprehensive or replicable assessments, as it omitted certain criteria specific to the CaRE program. Obvious vulnerabilities were missing from the reports, while non-existent errors were flagged. Additionally, the communication delays with the tool's support team prevented the active resolution of encountered issues.

The funding conditions are highly specific regarding the technical objectives that hospitals must meet. As a result, a provider change was decided to ensure the program's success. These decisions were made at the THG level following the usual procedure presented in section 2.2, which inevitably extended the approval and adoption periods. The third selected tool, AKYL, was deployed in early October 2024. However, due to time constraints, only a few of the identified vulnerabilities had been remediated since.

After reviewing the AKYL's audits, it became clear that the critical issue to address was the hosting of the websites on a shared server provided by the OVH company. OVH's support team recommended migrating all assets, previously hosted on a shared server, to a VPS (Virtual Private Server) to guarantee total control over the machine. As the THG management did not wish to adopt this solution for its members, and the latter possessed neither the skills nor the time to ensure this transition, another solution was deployed. This solution consisted of placing all the websites behind a reverse proxy managed by the THG's leading hospital to resolve this port issue. All connections to any of the THG's member services would pass through this reverse proxy that would redirect them towards the shared server at OVH. This solution proved ineffective, as the reverse proxy did not resolve the fundamental cause of the problem in any way and just hid the issue at hand. During a Question-And-Answer session with the CaRE program's managers, it was argued that this problem did not directly fall under the program's objectives because it did not directly impact the hosted sites. It was therefore decided to remove these errors from AKYL's audit reports after an expert's manual review. Nevertheless, the Esquirol Hospital Center chose to follow the hosting provider's recommendations by opting for a VPS to maintain control over its data and to manage its infrastructures and services more efficiently and locally.

The VPS infrastructure's design must be based on a balance of security, performance, and scalability. This hosting solution's conception must meet strict requirements regarding data protection and resilience against cyber threats. One of the major objectives is to correct the vulnerabilities identified by AKYL's audits, while ensuring that no new weaknesses are introduced during deployment. This redesign must also guarantee that the user experience, as well as that of the administrators responsible for maintaining the sites, remains seamless and unchanged. Reduced or zero availability of the hosted applications would lead to a reversion to a backup of the previous solution, which would waste administrators' time by forcing them to reproduce the changes made between the last backup and the appearance of problems. Furthermore, instability or unavailability could cause potential patients and their families to

lose interest in the sites, which are primarily used to provide information about the hospital's care offerings, thus reducing their support.

## 5.2 Architecture and Design

Within this new architecture (cf. figure 5.1), the services' virtualization has become a strategic choice to maximize flexibility and strengthen isolation between hosted applications. Docker has been adopted to encapsulate each website within an isolated environment (round rectangles on the schema), ensuring that a single server can host as many versions of web servers and databases as necessary for the proper functioning of unmaintained sites, if required. The use of Docker also guarantees that the different instances cannot interact directly with each other. This approach prevents software dependency conflicts, a frequent problem on shared infrastructures where an update to one service can lead to unexpected malfunctions in other applications. The orchestration of containers via Docker Compose has also been designed to facilitate automated deployment, continuous updates, and centralized configuration management, minimizing manual interventions and reducing the risk of human error.

One of the fundamental principles of this design is the strict isolation of internal networks (in blue and orange on the schema). Each site must be hosted within a specific subnet, where only a limited number of components can interact: the web server and its associated database. This segmentation prevents a potential compromise of one site from impacting other hosted services. Only a few essential management tools, such as phpMyAdmin and Nginx Proxy Manager (NPM), should be accessible transversally, but they are themselves isolated and cannot communicate with each other. This network compartmentalization is a key element of the security system, as it drastically limits internal attack vectors and restricts the propagation of potential infections.

Traffic optimization and the exchanges' securing between clients and servers are ensured by the integration of a centralized reverse proxy. NPM was chosen for its ease of administration and its native integration with Let's Encrypt, which allows for the automatic management

of SSL certificates and ensures systematic encryption of communications. This automation guarantees that all web connections are protected without requiring frequent intervention from administrators. Furthermore, NPM also has security options to prevent the main known attack vectors, as well as HSTS support to prevent downgrade attacks on web servers.

To prevent any attempted intrusion, a dual firewall system should be implemented. The first level of defense would be provided by the OVH firewall, which filters traffic upstream and protects the infrastructure against volumetric attacks, particularly Denial of Service (DoS) and Distributed Denial of Service attacks. This system would block malicious requests before they reach the VPS, thus reducing the load on internal services. In addition, an internal firewall must be configured directly on the VPS, with strict rules for filtering incoming and outgoing connections. This ensures that only strictly necessary services are exposed, preventing the risks of exploiting vulnerabilities related to unnecessarily open ports.

Protection against website file enumeration and brute-force attacks targeting the SSH port needs to be strengthened through the implementation of an Intrusion Detection System (IDS). Fail2Ban could play a central role in this defense by automatically blocking suspicious IP addresses after a certain number of failed access attempts, thus preventing brute-force attacks on sensitive services. The SSH port must also be changed so that brute-force attacks on port 22 are rendered ineffective. Enumeration of the server's ports would be necessary to find the one hosting the SSH service, thus making the attack easily detectable.

Particular attention has to be paid to securing the databases, which are a critical element of this infrastructure. Unlike an approach where all applications would share the same MariaDB instance, each site here will benefit from its own dedicated database, thus ensuring complete data isolation. This segmentation would prevent any risk of contamination in the event of a site compromise and limit access to the only applications that actually need it. To further enhance this security, connections to the databases need to be encrypted, and access to phpMyAdmin to be restricted only to those with an absolute need to access it. Adding a new connection will require modifying the rules of both firewalls. MariaDB instances must also be executed within

their container as an unprivileged user. This latter security measure, coupled with the option preventing privilege escalation in Docker Compose, would make this type of attack almost impossible.

One of the guiding principles of this architecture is based on a Zero Trust approach, where no access is granted by default. Each permission must be explicitly validated, and all access requests are controlled to prevent abuse. In other words, all services offered by the websites that do not directly impact website users, as well as administrator access to the various site administration pages, will initially be disabled and reactivated only upon request from the individuals concerned. This philosophy will strengthen the infrastructure's resilience against internal and external attacks, reducing the attack surface exploitable by malicious actors.

Finally, to ensure maximum resilience, an automated and encrypted backup system needs to be implemented. All databases and critical configurations need to be stored on a secure remote server, allowing for rapid restoration in the event of compromise or hardware failure. These backups would be regularly tested to ensure they are functional and that no data corruption would occur if recovery were ever needed.

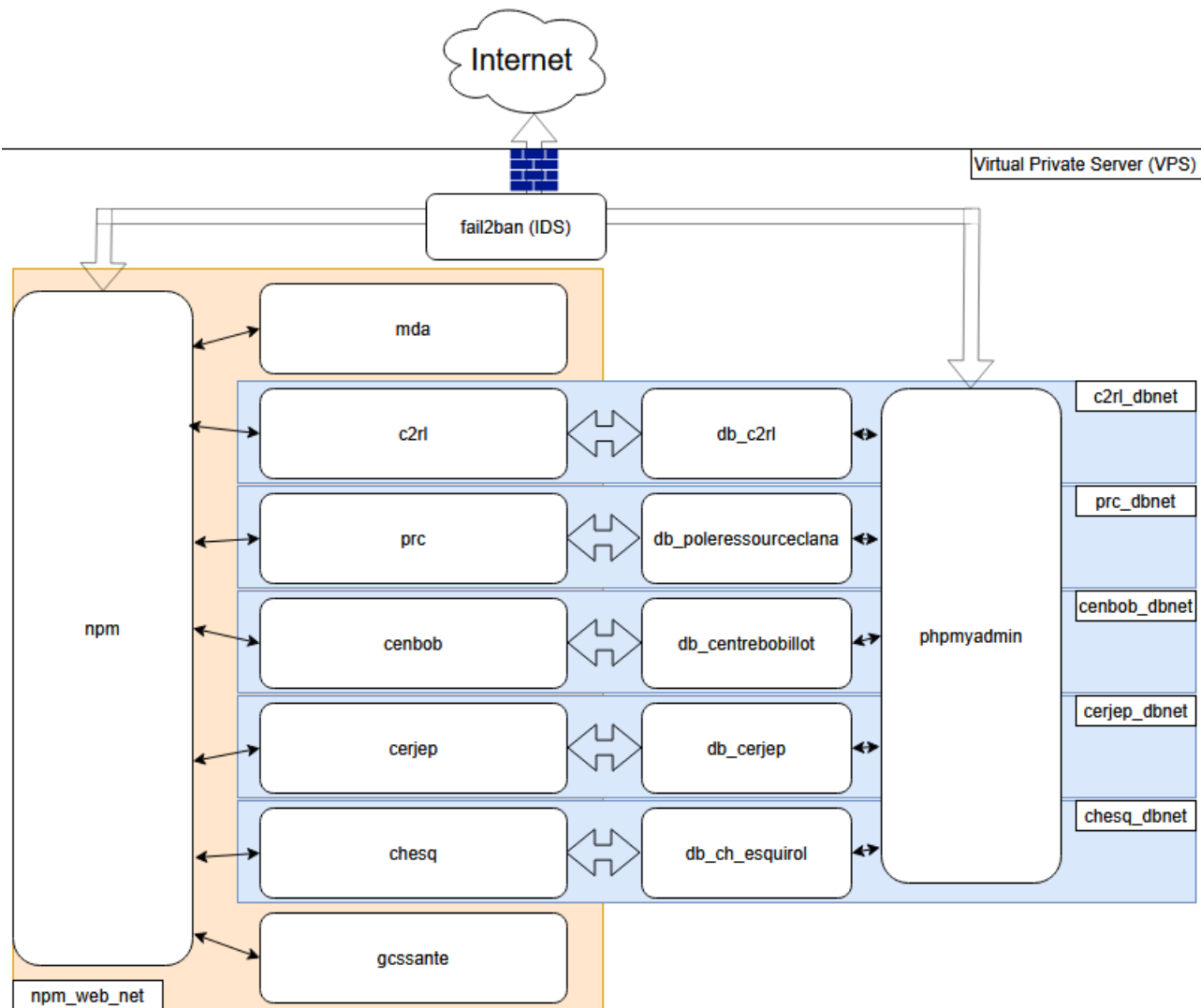


Figure 5.1: Virtual Private Server implementation schema

### 5.3 Implementation of the Solution

Implementing a web server on a VPS, while technically straightforward thanks to solutions like Docker, actually involves numerous challenges when it comes to designing a secure, sustainable, and adaptable infrastructure for future developments. Managing web services, the reverse proxy, the IDS, and databases via containers offers significant modularity but demands greater rigor. While online documentation provides many examples of ready-to-use Docker Compose

configurations, their effective implementation in a real-world environment often reveals unexpected complexities. Between service isolation and security constraints, every architectural decision must be carefully considered to avoid introducing new vulnerabilities exploitable by attackers or instabilities compromising service availability [78] [79].

The first implementation phase involved an assessment of existing infrastructures to identify the versions of web servers and databases in use. This process was not limited to a simple technical inventory but also included consultation with the owners of the various sites to raise their awareness of the risks associated with outdated versions and to gather their specific needs. This dialogue identified several extremely old sites, some of which no longer had an assigned maintainer. The decision was therefore made to permanently close some, while others were updated to meet minimum security requirements. However, this one-time update does not guarantee long-term security, as among the seven sites concerned, only two benefit from monitoring by a service provider and will therefore be regularly updated. The others will inevitably become vulnerable over time. It is therefore necessary to ensure complete isolation of all services as well as total compartmentalization of each within its container.

The chosen approach was to compartmentalize each website within distinct subnets within the VPS (cf. listing 1). Docker facilitates network management by allowing the automatic creation of private subnets for containers declared in the same Docker Compose file. However, the default configuration is not sufficient for this specific implementation, as it does not guarantee sufficient isolation between the hosted sites. It was therefore necessary to design a network architecture involving the manual creation of multiple dedicated subnets.

Assigning static IP addresses to the containers, although not a common practice, was necessary for several reasons. Firstly, it allowed for the configurations' standardization by assigning consistent IP ranges to similar services across all subnets, facilitating debugging and maintenance. For example, a database container will always have an address in the format: "xxx.xxx.xxx.35". Secondly, prior to updating one of the websites to a more recent version of PHP, the container names' resolution in the configuration parameters for database access by

the website was not functioning. A static IP address was therefore assigned in these settings. However, after rebooting the containers, the address would change, and the connection to the database would fail. Static addresses were therefore assigned to all containers to simplify system evolution for future administrators.

---

**Listing 1** Personalized dedicated subnets

---

{yaml}

```
services:
  db:
    *****
    networks:
      dbnet:
        ipv4_address: xxx.xxx.xxx.36

  wordpress:
    *****
    networks:
      npm_web_net:
        ipv4_address: xxx.xxx.xxx.72
      dbnet:
        ipv4_address: xxx.xxx.xxx.4

*****
networks:
  npm_web_net:
    external: true
    name: npm_web_net
  dbnet:
    driver: bridge
    ipam:
      config:
        - subnet: xxx.xxx.xxx.0/24
          gateway: xxx.xxx.xxx.254
```

---

Furthermore, numerous other security measures were adopted to maximally constrain potential attackers seeking to escape the containers and gain access to the host machine. These best practices come from various sources, most of which are based to some extent on OWASP (Open Web Application Security Project) recommendations for container protection. The first

measure applied to all containers is to run them under unprivileged users who are not part of the sudo group. This measure reduces the attack surface for an attacker who gains a shell within a container. The "no-new-privileges" security option is also enabled to prevent any privilege escalation, even if the attacker has a stable shell. In addition, volumes mapped with the Host are configured to be accessible only in "read-only" mode, or at a minimum in "read/write" mode, to further reduce the attack surface. The capabilities available to the containers are also reduced to the strict minimum, and the computing power, RAM, and CPU of each container are also limited to prevent a DoS attack on the Host by overloading one of the containers (cf. listing 2).

---

**Listing 2** Examples of security measures

---

{yaml}

```
services:
  wordpress:
    *****
    cap_drop:
      - ALL
    cap_add:
      - NET_BIND_SERVICE
    volumes:
      - ./wordpress:/var/www/html:ro
    security_opt:
      - no-new-privileges:true
    deploy:
      resources:
        limits:
          cpus: '1'
          memory: 128M
```

---

In the highly improbable event that an attacker manages to compromise the system and achieve privilege escalation, allowing them to take control of the host, they would then have the rights of the account running Docker. By default, this account is the root account, which poses a security risk. It is therefore recommended to opt for an alternative Docker installation that allows a non-privileged user to run it. However, not all official images available on Docker Hub are compatible with rootless mode [80], which would necessitate the use of custom images,

thus significantly complicating the infrastructure's maintenance and administration.

Another major security concern lies in protecting the host against external attacks. A strict firewall has been implemented to maximally limit incoming and outgoing connections to the VPS (cf. listing 3). As Docker automatically manages certain internal firewall rules to isolate containers, it is necessary to use the "DOCKER-USER" chain to filter direct communications from the outside to the containers. Complementary rules have been added to the Input and Output chains to restrict access to only the necessary protocols (HTTP, HTTPS, DNS) and to secure administration via SSH. This approach has significantly reduced the attack surface by blocking any unauthorized connection attempts.

---

**Listing 3** Iptables rules for Docker containers

---

```
{Iptables}
```

```
#DOCKER-USER#
ACCEPT tcp -- anywhere anywhere ctorigdstport 443 ctdir ORIGINAL
ACCEPT tcp -- anywhere anywhere ctorigdstport 80 ctdir ORIGINAL
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 8080 ctdir ORIGINAL
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 8080 ctdir ORIGINAL
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 8080 ctdir ORIGINAL
DROP tcp -- anywhere anywhere ctorigdstport 8080 ctdir ORIGINAL
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 81 ctdir ORIGINAL
DROP tcp -- anywhere anywhere ctorigdstport 81 ctdir ORIGINAL
```

---

The rules defined in the "DOCKER-USER" chain are primarily of two types: "ACCEPT" and "DROP". By default, Docker allows redirection of all incoming traffic to exposed containers. However, by using the options "ctdir ORIGINAL" and "ctorigdstport <port>", it becomes possible to restrict, through the first, only requests originating from the outside, and through the second, those that were initially targeting that specific port on the host. This method enables effective traffic filtering before Docker applies its own NAT rules, which alter both the source and destination ports. These rules are used in pairs to allow traffic for a specific IP address only (cf. listing 4).

**Listing 4** Iptables rules for other connections

---

```
{Iptables}

#INPUT#
ACCEPT  all  --  anywhere  anywhere
ACCEPT  all  --  anywhere  anywhere  ctstate  RELATED,ESTABLISHED
ACCEPT  tcp  --  x.x.x.x  anywhere  tcp  dpt:X  ctstate  NEW,ESTABLISHED
ACCEPT  tcp  --  x.x.x.x  anywhere  tcp  dpt:X  ctstate  NEW,ESTABLISHED
ACCEPT  tcp  --  x.x.x.x  anywhere  tcp  dpt:X  ctstate  NEW,ESTABLISHED
DROP    all  --  anywhere  anywhere

#OUTPUT#
ACCEPT  all  --  anywhere  anywhere
ACCEPT  all  --  anywhere  anywhere  ctstate  RELATED,ESTABLISHED
ACCEPT  tcp  --  anywhere  anywhere  sport  X  ESTABLISHED
ACCEPT  tcp  --  anywhere  anywhere  tcp  dpt:smtp  ctstate  NEW
ACCEPT  tcp  --  anywhere  anywhere  multiport  dports  domain,http,https
ctstate  NEW
DROP    all  --  anywhere  anywhere
```

---

However, this traffic restriction revealed certain limitations during the production deployment. Indeed, several auxiliary services used by the websites ceased to function due to the strict filtering applied to outgoing connections. These problems arose from the fact that the addition of new functionalities was done directly between the communication managers and the service providers, without consulting the IT department. However, according to the HIS urbanization rules, auxiliary services must be kept to a strict minimum to limit the risks of compromise. This migration was therefore an opportunity to carry out a drastic cleanup, disabling all services and reactivating only those for which a request was explicitly made. For example, several sites used contact forms that sent emails to the relevant departments. As these forms remained accessible via the sites' administration interface, their email sending functionality was deemed superfluous and was not restored by default. The restoration of this functionality was only requested a month after the migration for one of the sites, while the managers of the others never made such a request.

Finally, protection against external attacks was strengthened by the integration of Fail2Ban as an intrusion detection and prevention system. Its operation is based on a set of filters

that analyze the reverse proxy logs to identify suspicious attempts, such as the enumeration of sensitive pages or DoS attempts. Once malicious activity is detected, the offending IP address is automatically banned for a predefined period. Several custom jails have been created to address specific threats, with ban durations adjusted according to the criticality of the attacks.

All Fail2Ban jails (cf. listing 5) are based on a common structure: a name defined in brackets, followed by a set of parameters that define their action's scope and the banning methods. It is common, when using a VPS, to exclude certain IP addresses from any banning using the "ignoreip" option. This exclusion often targets the host's internal addresses, used for supervision or monitoring. This helps prevent critical service interruptions by accidentally blocking legitimate sources. Finally, basic timing parameters such as "findtime", which sets the maximum time window between the first and last suspicious log entries; "maxretry", the number of failed attempts allowed before triggering a ban; and "bantime", the ban period duration, are all defined individually within each jail. However, the "bantime" value can be dynamically adjusted by global settings defined earlier in the same configuration file to scale the duration to the offence frequency. The following examples of configuration files are presented for illustrative purposes only. They are intentionally left, almost as found online, to avoid showing the specifics of the installation and prevent potential attacks.

---

**Listing 5** Jail configuration

---

```
[enumeration]
enabled = true
ignoreip = xxx.xxx.xxx.xxx /32 xxx.xxx.xxx.xxx /8 xxx.xxx.xxx.xxx /8
action = action-ban-enumeration
filter = npm-enumeration
chain = DOCKER-USER
logpath = /var/log/npm/proxy-host-*_access.log
maxretry = 15
findtime = 600
bantime = 600
```

---

A Fail2Ban filter configuration file (cf. listing 6) is used to define log analysis rules. It mainly consists of two sections: "failregex" and "ignoreregex". The first contains one or more

regular expressions intended to identify log lines representing a potential intrusion or abuse attempt, such as frequent HTTP errors or a large number of requests in a very short time. Conversely, "ignoreregex" allows certain entries that match the rule defined by "failregex" but that we choose to ignore, not to be processed. This distinction helps reduce false positives and refine detection. The created regex rules are based on the format of the processed log files and use variables to significantly simplify their writing. For example, the variable "<HOST>" can be used, according to the official documentation: "for standard IP/hostname matching and is only an alias for (?:::f4,6:)?(?P<host>§+)" [81].

---

**Listing 6** Filter configuration
 

---

```
[INCLUDES]
```

```
[Definition]
```

```
failregex = ^.* (499|301|405|404|403|401|500|\-)
(499|301|405|404|403|401|500)
- .* \[Client <HOST>\] \[Length .*\) .* \[Sent-to <F-CONTAINER>.*
</F-CONTAINER>\] <F-USERAGENT>".*"</F-USERAGENT> .*$

ignoreregex = ^.* (404|\-) (404) - .*".*(\.png|\.txt|\.jpg|\.ico|
\.js|\.css|\.ttf|\.woff|\.woff2)(/)*?" \[Client <HOST>\]
\[Length .*\) ".*" .*$
```

---

Finally, when the suspicious log entries' number reaches the "maxretry" threshold specified in the jail's configuration, the Actions defined in the corresponding action file (cf. listing 7) are triggered. These actions consist of Iptables rules that block the offending IP address for a duration set by the "bantime" parameter in the jail file. Once this time period has elapsed, the IP address is automatically removed from the block list and access is restored.

---

**Listing 7** Action configuration

---

[Definition]

```
actionban = iptables -I DOCKER-USER -m string --algo bm
--string <ip> -j DROP iptables -I INPUT 1 -s <ip> -j DROP

actionunban = iptables -D DOCKER-USER -m string --algo bm
--string <IP> -j DROP iptables -D INPUT -s <ip> -j DROP
```

---

Issues also arose during the system's production deployment concerning NPM. Similar to the issue described in section 7.3 for the Telemaintenance platform, a desynchronization in request processing occurred, resulting in the connection being dropped. NPM was requesting the processing of a second request from the website's web server while the latter had not yet finished processing the first one, meaning that there was an imbalance between the data received by the proxy and the data expected by the web server. The solution was therefore to add a configuration setting in NPM for each site, increasing the number of buffers, their size, as well as the size of the temporary file created during communication processing. Unlike Nginx, where configurations are managed using configuration files, these changes were implemented, for each website, via the web interface provided by NPM (cf. listing 5.2).

**Edit Proxy Host** ✕

⚡ Details **📁 Custom locations** 🛡️ SSL ⚙️ Advanced

**Add location**

**Define location \***

location / ⚙️

**Scheme \*** **Forward Hostname / IP \*** **Forward Port \***

http [REDACTED] 80 ⌵

Add a path for sub-folder forwarding.  
Example: 203.0.113.25/path/

```
proxy_buffers 16 4k;
proxy_buffer_size 8k;
proxy_max_temp_file_size 0;
```

[Delete](#)

**Cancel** **Save**

Figure 5.2: Nginx Proxy Manager special configuration

# 6 Active Directory Vulnerabilities

## Remediation

Active Directory (AD) manages the authentication and authorization mechanisms for users, connected medical equipment, and critical applications. Its compromise could not only lead to interruptions in the care's continuity but also expose highly sensitive data, such as medical records, thereby jeopardizing patient safety, despite the protective measures deployed on application systems, such as the Electronic Health Record. The majority of AD environments currently in production were designed at a time when cybersecurity concerns were secondary, and when the threats to information systems were far less sophisticated. Although evolutions have been introduced over time, these infrastructures still inherit historically open, poorly segmented, and excessively permissive architectures. Such characteristics facilitate lateral movement and privilege escalation in the event of an intrusion. While reducing the attack surface remains a rational priority, as it limits the number of potential incidents, securing Active Directory is nonetheless indispensable. Although it does not directly prevent attacks, it drastically limits their consequences by making it more difficult for an attacker who has gained an initial foothold to exploit the hospital environment as a whole. Thus, in a sector as sensitive as health-care, limiting the impact of a compromise is an essential requirement to preserve the continuity of care and the confidentiality of data.

## 6.1 Level 1 ANSSI

The vulnerabilities identified at level 1 must be addressed as a priority. Their persistence exposes the hospital establishment to major risks by allowing an attacker who has breached the security perimeter to access the information system. Once this initial access is obtained, the attacker can, for example, seek to escalate privileges to take control of the entire system and deploy ransomware, or adopt a more stealthy approach by remaining hidden in the environment to discreetly collect sensitive and confidential information over time to monetize it later.

The first vulnerability addressed concerned the lack of password rotation on privileged accounts. Indeed, these accounts had been configured with passwords that never expired and, for some, had not been changed since their creation. This situation seriously exposed the Active Directory to long-term compromise risks. To remedy this, "Fine-Grained Password Policies" were defined and applied specifically to all privileged accounts [82], to enforce password rotation every 6 months and stricter complexity requirements: 20 random valid ASCII characters. At the same time, another warning sign, raised by the ORADAD tool, was taken into account: the presence of 26 privileged accounts across the entire forest, an excessive number. Although not directly a vulnerability, this situation can indicate poor access rights governance and unnecessarily increase the Active Directory's attack surface. The remediation phase, therefore, began by consulting the relevant teams, aiming to identify accounts that no longer require elevated privileges. Once this review was completed, a campaign to declassify these accounts was launched to assign them rights appropriate to their actual needs [83]. As an example, the account named "Avassys", used by an external provider, was among the accounts with unjustified privileges. This account was deleted after the new remote maintenance platform's implementation.

According to ANSSI (National Agency for the Information Systems' Security), the recommendations for password policy are 12 complex characters without mandatory expiration for non-privileged accounts, and an expiration of at most 3 years with a minimum of 16 complex characters for privileged accounts [84]. These measures aim in particular to make brute-force

attacks and their variants, or keylogging on the passwords of these accounts, more difficult.

The SPN attribute is defined as "a unique identifier for the Network Controller service instance, which is used by Kerberos authentication to associate a service instance with a service login account." [85]. Despite its essential role in the Kerberos authentication mechanism, it can be exploited in an attack known as Kerberoasting. This attack can be carried out by a malicious actor who has compromised a standard user account, that is, without any special privileges, from any computer, and provided that the targeted SPN is associated with a user account (rather than a machine service account). The principle of Kerberoasting is based on requesting a Service Ticket from the Kerberos Distribution Center (KDC). In response, the KDC provides a ticket encrypted using the Kerberos key derived from the service account's password associated with the SPN. The attacker can then proceed, outside of any network monitoring, with brute-force or dictionary attacks on this encrypted ticket to try to recover the corresponding password. This attack is all the more formidable because it relies on a legitimate mechanism of the Kerberos protocol, making its detection particularly complex in the absence of specific monitoring [86].

Depending on the case, some accounts were demoted and removed from privileged user groups, while others had their password policies modified, thus allowing the SPN to be maintained despite ANSSI recommendations. Indeed, although ANSSI advises against this practice, it accepts it in certain situations, particularly if a strong password policy is implemented or if the account in question is a Managed Service Account (sMSA / gMSA). These exceptions are necessary for many companies and establishments that have ADs too old to optimally correct the identified vulnerabilities. In the absence of such measures, although the attack is not completely prevented, it becomes extremely complex for non-professional attackers, who do not have the computing power required to crack sufficiently robust passwords.

Permissions, regardless of the objects that hold them, can become a vulnerable target if misconfigured, thereby offering an attacker the possibility of gaining control of an object. This control can be acquired by modifying sensitive properties, delegating privileged rights, or ex-

exploiting specific functionalities [87]. Once an object is compromised, the attacker can use it as an entry point to extend their presence within the system, which can lead to privilege escalations and the complete compromise of the Active Directory. The paths taken by attackers also constitute useful vectors for defenders to identify anomalies in permission management. Among the most critical rights are the "WriteDACL" right, which allows a user to modify access rights [88], as well as the "WriteOwner" right, which gives them the ability to take an object's ownership and modify its rights [89]. To mitigate these vulnerabilities, the only solution is to remove the permissions on the objects concerned.

## 6.2 Level 2 ANSSI

Level 2 presents similarities with Level 1 regarding the errors addressed. However, although issues such as password expiration, weak password policies, or dangerous permissions on certain objects persist, the potential impact of these vulnerabilities would be slightly less severe if these objects were to be compromised. Furthermore, these vulnerabilities and alerts are more complex to resolve. This level constitutes the requirement of the CaRE program and must be achieved by the end of Domain 1.

Regarding the dangerous permissions addressed at this level, they mainly focus on the "WRITE\_ALT\_IDENTITY" right assigned to accounts associated with Microsoft Exchange Server 2016 groups. This vulnerability stems from a Microsoft configuration error, which has since been addressed with patches for each currently maintained version of Exchange, resolving this issue [90]. As for the password-related vulnerabilities, they were resolved in the same way as those at the first level. A password policy has been implemented for user accounts, although these passwords are not used in practice, given that all users employ CPS cards for authentication. Furthermore, certain classes in the Active Directory schema, such as "msExch-StorageGroup," exhibit vulnerabilities related to default assigned rights, notably the ability to create child objects under computer-type objects. Similarly, a patch for this vulnerability was released by Microsoft and subsequently deployed.

Domain Controllers, just like Read-Only Domain Controllers, support several encryption algorithms for Kerberos tickets, such as DES, RC4, and AES, each with several variants. As of the writing of this thesis, only AES-based algorithms are considered sufficiently robust for production use; the others, deemed obsolete, should be disabled [91]. Level 2 of the security plan specifically targets the removal of DES algorithms, an operation that can be carried out by deploying a GPO (Group Policy Object) disabling their use on all domain controllers. However, this operation can lead to side effects. The deactivation of the RC4 encryption algorithm caused malfunctions, particularly with a specific application server, preventing some users from accessing it. This server has an SPN and relays authentication requests to the domain controller; nothing confirms that this configuration is the source of the problem. In theory, the entire mechanism should continue to function normally. This anomaly, therefore, remains at this stage and will require more in-depth testing to determine its exact cause.

Warnings still exist, however. Among them, some privileged accounts have a login script that runs when the user logs into their workstation. These scripts allow for the execution of a batch of commands that can have many uses, such as the automatic configuration of workstations during their initialization by technicians who create the workstations and who have a dedicated account used solely for workstation preparation. Scripts that have been replaced by GPOs, as recommended by ANSSI.

### 6.3 Level 3 ANSSI

Although achieving this level is not required at the end of Domain 1, it could be integrated into the requirements of the "Cybersecurity Baseline" and is, as such, considered a necessary objective to reach. The vulnerabilities addressed at this stage concern configuration elements that, while presenting a proven security risk, require modifications that can have consequences on many of the system's elements, affecting authentication, authorization, and backup processes alike. Thus, the remediation of these vulnerabilities requires particular attention, as any imprudent modification could lead to the unavailability of critical services, potentially compromising

the healthcare professionals' ability to work under good conditions.

During the workstation preparation phase, technicians integrate the machines into the domain using their domain administrator account. This practice automatically assigns this account as the integrated machines' owner. However, these technical accounts generally have extensive privileges, which poses a security risk: if one of these workstations is compromised, an attacker could potentially exploit this ownership relationship to escalate their privileges within the domain. To address this vulnerability, a script has been implemented to reassign the new machines' ownership to a specific account named "Domain's Admin" every evening (cf. listing 8). This account already existed and was initially created for the specific purpose of performing this function. It has only the strictly necessary rights, following the principle of least privilege.

**Listing 8** Ownership Modifying Script

---

```

$user = New-Object System.Security.Principal
        .NTAccount("DOMNT2\Admins du domaine")
Get-ADComputer -Filter * -SearchBase "OU=CH Esquirol,
DC=CHesquirol,DC=ad" |
ForEach-Object {
    $acl = Get-Acl -Path "AD:$($_.DistinguishedName)"
    if (($acl.Owner -like "DOMNT2\*****")
        -or ($acl.Owner -like "DOMNT2\*****")
        -or ($acl.Owner -like "DOMNT2\*****")) {
        $acl.SetOwner($user)
        Write-Host "Ordinateur :" $_.DistinguishedName " solved "
        Set-Acl -Path "AD:$($_.DistinguishedName)" $acl
    }
}

$user = New-Object System.Security.Principal
        .NTAccount("DOMNT2\Admins du domaine")
Get-ADObject -Filter * -SearchBase "OU=Groupes de distribution,
OU=CH Esquirol,DC=CHesquirol,DC=ad" |
ForEach-Object {
    $acl = Get-Acl -Path "AD:$($_.DistinguishedName)"
    if ($acl.Owner -like "DOMNT2\*****$") {
        $acl.SetOwner($user)
        Write-Host "Ordinateur :" $_.DistinguishedName " solved "
        Set-Acl -Path "AD:$($_.DistinguishedName)" $acl
    }
}

```

---

Furthermore, some certificates issued by an internal certification authority about fifteen years ago use encryption algorithms that are now obsolete and easily exploitable by attackers. These certificates were configured with exceptionally long validity periods, often between 15 and 30 years, thus exceeding current security standards. They all rely on the SHA-1 hashing algorithm, which is vulnerable to collision attacks [92]. A malicious actor could exploit this weakness to generate a fraudulent certificate with a valid signature identical to that of a legitimate certificate. This could lead to identity theft, potentially providing privileged access to sensitive areas. The certificates in circulation were replaced by new ones that meet the various recommendations. These new certificates use SHA-256 hashing algorithms with an RSA key of

more than 2048 bits, and the validity period has also been reduced.

Finally, the "Protected Users" group has been made mandatory to strengthen the security of privileged accounts by limiting the most common attack vectors. The accounts belonging to this group are critical for the proper functioning of the information system, and their compromise would have severe consequences on the integrity, confidentiality, and availability of resources. Membership in this group imposes strict restrictions on authentication methods, notably prohibiting any mechanism other than Kerberos with AES encryption [93]. However, this protection comes with numerous functional limitations. Indeed, member accounts can no longer use older authentication protocols, such as NTLM, which are still required by certain services and applications. This constraint causes many side effects, the severity of which varies depending on the privileges and uses of the accounts concerned. Resolving these incidents can be particularly complex due to the specific interactions between the restrictions of the "Protected Users" group and the application environment. These effects often require opening a support ticket with Microsoft or the support for the problematic applications, the processing of which can take several weeks. For example, some administrator accounts of the HIS (Hospital's Information System) team also exhibit inexplicable connection failures, but only on certain Windows 2016 or 2019 servers. Similarly, adding the "AdminSSO" account, which manages Single Sign-On (SSO), to the "Protected User" group, by disabling the use of the NTLM protocol, prevented all users from authenticating on their workstations, causing a major service interruption for one hour. This change, however, took place at the end of the day and outside peak hours, in anticipation of such problems, to minimize disruption to users.

## 6.4 Level 4 ANSSI

The privilege management model recommended for AD separates administrative accounts into several hierarchical levels called "tiers", each with specific permissions and access rights. The objective is to limit the attacks' propagation by dividing administration and management accounts according to their level of access. These accounts can be assigned to three distinct levels:

Tier 0, Tier 1, and Tier 2 [94].

Tier 0 encompasses the most sensitive accounts, such as those of domain controllers and AD administrators, who have complete access to the entire network and its resources. These accounts should only be used for specific and pre-defined actions, and their usage must be subject to strict control. Tier 1 includes server administrators and administration accounts for applications interacting with domain member business servers. Although these accounts are privileged, they should under no circumstances be used to administer domain controllers or the most critical systems on the network. Finally, Tier 2 concerns administration accounts for workstations or non-critical applications, having limited access to machines with lower sensitivity. Communication between criticality levels is prohibited from a less critical level to a more critical level and must be strictly controlled and exceptionally authorized in the other direction [84].

However, these recommendations come from the latest ANSSI report of 2023 and were not part of previous guidelines. This objective is by far the most difficult to implement in legacy infrastructures because they have an organization of account functions and compartmentalization that, if it exists, is based on an insufficient proprietary logic. Implementing the tier system would involve creating new administrator accounts dedicated to specific tasks, migrating rights and activities to these new accounts, as well as reclassifying the old accounts. This would also require, for instance, an operation's revision of all scripts and patches currently centralized under the "adminBatch" account, which has access to all AD objects to perform its processing. This would mean multiplying the accounts managing the batches and organizing the different scripts by levels, so that each process is executed by an administrator account of the corresponding level. Although this step is essential, it is not considered a priority in the hospital's current projects.

Nevertheless, some vulnerabilities have been corrected, notably those related to sensitive parameters associated with "dSHeuristics." This parameter, specific to Active Directory, allows certain functionalities to be enabled or disabled at the forest level [95]. If misconfigured, it

can introduce exploitable security flaws in specific contexts, particularly if an attacker has advanced rights, such as the ability to create objects in Active Directory. Among the problematic options identified in the report, two deserve particular attention: "AttributeAuthorizationOn-Add," which allows access controls to be ignored when adding new objects via LDAP [96], and "BlockOwnerImplicitRights," which prevents object owners from automatically obtaining rights over them [97]. In certain configurations, these parameters can be exploited by an attacker to modify the security attributes of objects (for example, machine accounts) that they created, thus paving the way for privilege escalation [98]. To eliminate these vulnerabilities, it is recommended to explicitly set the value of these bits in the "dSHeuristics" parameter to 1 to disable default behaviors that could be misused.

Another vulnerability was also easily corrected. This one was related to the default setting allowing any authenticated non-privileged user to add up to ten machines to the domain. However, this can allow for privilege escalation: by adding a machine to the domain, the user becomes its owner, which can be exploited for malicious purposes. An attacker could then target a DC with the ultimate goal of authenticating as the user of that controller by requesting a new certificate after modifying the "dNSHostName" attribute of the compromised machine to match that of the DC. This vulnerability has been corrected by setting the value of the "ms-DS-MachineAccountQuota" attribute to 0 at the root of the domain, thus preventing non-privileged users from adding new machines.

# 7 Secure Telemaintenance Platform

## Deployment

### 7.1 Requirements Analysis for the Secure Telemaintenance Platform

Before my arrival, the established method involved providing service providers with VPN (Virtual Private Network) access, along with the creation of an administrator account on the targeted servers, as well as an administrator account in the Active Directory. Using these access credentials, providers could connect directly to the relevant machines. However, this approach presented several major flaws. Firstly, granting VPN access to numerous providers allowed for free movement within the hospital's internal network, without any real granular control over accessible resources. The only restriction is the non-disclosure of passwords for unrelated servers, which remains insufficient in terms of security. Secondly, the passwords for administrator accounts on critical servers were communicated to providers without any mechanism guaranteeing their proper management. There was no assurance that these credentials were kept secure, nor that they would not be compromised or misused, especially since security practices can vary greatly from one provider to another. Furthermore, no traceability of the actions carried out by providers was in place. The existing monitoring system relied solely on screenshots taken at regular intervals during active sessions. This system, in addition to being obsolete and unreliable, had not been functioning since an update several years prior.

Finally, it was observed that many employees of providers shared a single account belonging to a colleague within their company to pool access to the hospital's servers. Such a practice completely compromises the separation of privileges and makes any traceability of connections and actions undertaken impossible.

Although it is difficult to assign a precise criticality value to these vulnerabilities due to a lack of knowledge about the security level of the providers' information systems, it is nevertheless clear that, given the importance and consequences that a breach in the HIS (Hospital's Information System) would have, no doubt is allowed, and the greatest caution must be exercised.

This model's main attack scenario lies in the fact that an attacker who has compromised a provider could, theoretically, pivot to the hospital network with great ease. Worse still, the absence of an effective supervision mechanism means that the intrusion could go completely unnoticed until the detection of malicious events on machines, facilitating the enumeration of the HIS and therefore the search for other vulnerabilities. Currently, network logs are not analyzed, and the absence of a SIEM (Security Information and Event Management) prevents any correlation of suspicious events. Faced with these risks, the implementation of a secure jump server has become a more robust solution.

This jump server must comply with strict specifications to limit the known flaws of the current system as much as possible. Among these criteria, strict data segmentation, providers' authentication when using the service, activity logging, and the individual accounts' use for each employee of each service provider are the major axes that this new solution must respect. Providers would only have restricted access to strictly necessary resources via a dedicated channel. Two-factor authentication using applications such as Google Authenticator would protect access to the jump server and prevent colleagues' accounts from being used to connect. Provider sessions on the servers would be recorded and reviewable afterwards by hospital IS members or other competent bodies, such as the ANSSI (National Agency for the Information Systems' Security), to investigate problems or attacks. Finally, the access rights' simplified

management for provider accounts on servers and the deletion or deactivation of these accounts would allow IT department members to save valuable time. This transition to a more secure model represents both a technical and organizational challenge, as it involves changing the habits of dozens of providers who have been operating with the previous system for several years. However, it is essential to ensure the protection of hospital infrastructures against cyberattacks and the risks associated with uncontrolled access.

## 7.2 Architecture and Design

This solution's design was relatively quick and seamless. Many proven technologies were already in place for other services provided by the hospital and could be reused to facilitate the implementation of the jump server. The main objective was to eliminate direct access to the internal network via the current VPN, while establishing a secure alternative solution. This necessarily involves opening a new access point, but in a controlled and protected manner. A complete schema of the solution is shown in figure 7.1 and will be described in the following paragraphs.

The only viable option would therefore be to authorize access to the jump server from the outside, via the Internet. However, this opening would have to be designed with the utmost rigor to prevent it from creating an even more critical security flaw. Several measures need to be put in place to secure this access. First of all, direct exposure of the jump server on the Internet would have been a major threat. To remedy this, the hospital's reverse proxy needs to be used, allowing the real address of the server to be concealed and, coupled with the hospital's firewall, to better control incoming connections by limiting them to only authorized connections. Only the port of the server access application must be opened, thus preventing any attempt to exploit an unintended service. The reverse proxy must also be configured to display a more neutral and professional domain name for providers, avoiding any explicit indication of the critical nature of the service.

After an in-depth analysis of the available maintenance platform's solutions, the choice

fell on Apache Guacamole [99] under Docker. This choice was motivated by several decisive factors, including the maturity of the product, which makes it a reliable and proven solution, the ease of use, which reduces training needs for both administrators and end-users, and the ability to automate a large part of access management thanks to its (REST) API (Application Programming Interface). One of the major advantages of this solution lies in its ability to record provider sessions, thus offering better visibility into the actions performed on the servers. Unlike the old system, providers never have access to the credentials of the target servers, which significantly limits the risks associated with sensitive information leaks. In addition, Guacamole supports several protocols such as VNC, RDP, and SSH, which makes it particularly flexible and capable of adapting to the hospital's various infrastructures. This flexibility also suggests the possibility of a future evolution of the jump server into a true administrative bastion if the hospital's IT department deems it necessary.

Other solutions were considered, but they presented limitations that led to their rejection. Some professional applications, like TeamViewer, offered interesting features, but their unannounced cost made them incompatible with the hospital's budgetary limitations [100]. RustDesk, meanwhile, appeared to be a promising alternative; however, its architecture seemed to be designed around a client-server software model. This meant users would need to download a client application, and we would be required to install it on each server individually. In addition, the immaturity of its web interface, which is essential for rapid and efficient administration, was not convincing [101].

That being said, Apache Guacamole is not without its flaws. Like any software solution, it can present vulnerabilities, particularly in its earlier versions. For example, version 1.5.4 had a critical vulnerability allowing for an integer overflow during VNC connections [102], potentially leading to memory corruption and arbitrary code execution. Although this vulnerability has since been patched, the existence of other flaws, potentially unknown or already discreetly exploited by malicious groups targeting sensitive infrastructures, cannot be ruled out.

This uncertainty requires a rigorous approach to securing the Guacamole execution envi-

ronment. The use of Docker containers will provide a layer of isolation, but it is essential to strengthen their configuration to minimize the risks of exploitation in the event of a compromise. Measures such as restricting container capabilities and prohibiting execution in privileged mode should help limit the damage in the event of an attack. Similarly, the host server hosting the application must be hardened, in particular by reducing the attack surface, implementing active monitoring, and systematically applying security patches. The objective is to prevent any attempt at privilege escalation or lateral movement within the hospital network.

A major flaw in Guacamole's design, however, remains and represents a critical risk for the infrastructure's security. The passwords allowing transparent connection for users to the servers are stored in plain text in the database associated with the application. This design poses a fundamental problem: in the event of a successful attack allowing access to this database, an attacker would be able to recover every registered administrator accounts' credentials. Such a compromise would provide total access to the hospital's servers, rendering any segmentation or access restriction ineffective and paving the way for complete control of the system. This vulnerability's exploitation could occur through various vectors, such as privilege escalation within the server hosting Guacamole or credentials theft from an administrator with access to the database. Once in possession of this information, an attacker could not only access critical servers but also propagate their attack to the entire hospital network, facilitating malware's installation, data theft, or even complete systems' encryption as part of a ransomware attack.

To limit this risk, several strategies must be considered. An immediate solution would be to apply strong encryption to the stored passwords, coupled with a decryption mechanism in memory only at the time of use. However, this approach is not possible with an open-source project like Guacamole. Since the source code is publicly accessible, it is difficult to implement a truly effective encryption algorithm without an attacker understanding its operation and bypassing the protection. Thus, many encryption mechanisms become inoperative in the face of a targeted attack on the database. Another, more secure approach would be to completely eliminate plain text passwords' storage by using a centralized authentication solution, such

as a secrets manager or a Vault service, which would only deliver credentials on the fly and for limited sessions. This approach, although officially proposed by Guacamole, is currently limited to a single paid vault solution, which makes it difficult to exploit in a restricted budgetary context. Faced with these constraints, the chosen solution, pending updates to Apache Guacamole allowing the use of other open-source vault solutions, will rely on a systematic renewal of every password at the end of each day. For Windows servers, this rotation must be performed automatically using the LAPS, ensuring that each local administrator account has a unique password that is regularly updated. On the Linux server side, an automated script would be implemented to change credentials periodically, thus reducing the potential impact of a compromise. Thanks to this approach, the credentials obtained by an attacker will have a 24 hours only validity period, greatly limiting their usefulness in the context of a long-term attack.

Even though this solution is not perfect and does not fully eliminate the risks, its effectiveness will be reinforced by all the added security measures around the jump server. The environment's strict isolation, the active access monitoring, and the rigorous cybersecurity best practices application will help reduce the vulnerability's criticality and prevent a single flaw from compromising the entire HIS.

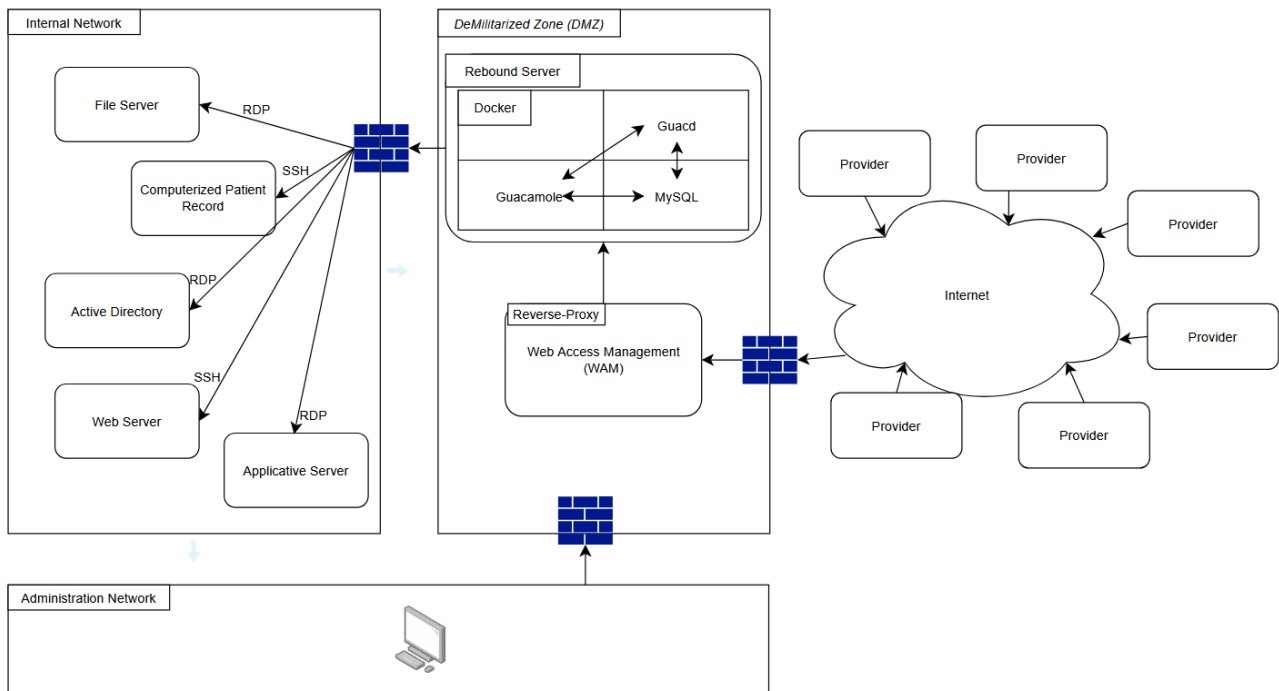


Figure 7.1: Jump server implementation schema

## 7.3 Implementation of the Solution

One of the main difficulties in configuring the WAM (Web Access Management) stemmed from the fact that the solution used by the hospital is uncommon and poorly documented. This made setting up the reverse-proxy particularly complex, especially to support Guacamole. The latter requires specific configurations at the reverse-proxy level. In the case of an Apache2-based proxy, the "flushpackets=on" option must be added to the "ProxyPass" directive according to the official Apache Guacamole documentation. This option ensures that the output buffer is immediately flushed after each data packet. Without it, access to Guacamole becomes unstable, generating critical errors. By enabling more detailed logging on Guacd (the daemon responsible for managing RDP/VNC/SSH connections), it is possible to observe that the problem occurs when a new instruction is processed before the previous packet has been finalized (cf. listing 9). This error is identical to the one encountered during the reverse-proxy installation on the

VPS (Virtual Private Server) in section 5.3.

---

**Listing 9** Extract of Guacd debug logs

---

```
guacd[1]: DEBUG: Error reading "select": End of
stream reached while reading instruction
guacd[1]: DEBUG: Guacamole connection closed during handshake
```

---

The situation was further complicated by the suspension of technical support from the company providing the WAM. Due to an increase in maintenance and after-sales service costs, the HIS decided not to renew the contract, pending renegotiation. Upon the contract's expiration, the company ceased providing any support, leaving the reverse-proxy issue unresolved for an extended period. To avoid this difficulty, a temporary reverse-proxy was set up directly on the Guacamole server. During this transition phase, providers continued to use a VPN to access internal resources before establishing their session via Guacamole. This solution ensured access continuity while limiting the direct exposure of the servers.

The hospital's firewall plays a key role in securing incoming and outgoing connections, particularly to the DMZ (DeMilitarized Zone), where servers directly accessible from the internet are located. As these machines are particularly exposed to attacks, they are subject to strict control. The management of connections to remote servers is handled by the guacd daemon, transparently to users of the Guacamole web interface. Thus, only an HTTPS connection is allowed from the outside to the Guacamole server as shown in figure 7.2. No other incoming connections are permitted. Regarding outgoing connections, only HTTPS connections are allowed, and only during manual updates of the system or container versions.

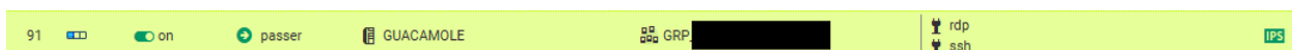


Figure 7.2: Hospital's firewall internal rules for the maintenance platform

The server's firewall, by default, blocks all incoming and outgoing connections. For incoming traffic, requests to the database are limited to a single IP address, that of the server responsible for password update scripts. Similarly, requests to Guacamole are restricted to the WAM server. In addition, only the static IP addresses of the HIS computers are authorized to connect via SSH to the server for administration, maintenance, and troubleshooting. For outgoing traffic, HTTPS connections are permanently allowed, regardless of the destination address, for updates, although these are blocked by the hospital's firewall. DNS connections are also permitted to facilitate the server names' resolution via the hospital's internal DNS, which significantly simplifies the connections' configuration to remote servers (cf. listing 10).

---

**Listing 10** Interesting Docker rules for Guacamole Setup

---

```
#INPUT#
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED
ACCEPT tcp -- x.x.x.x anywhere tcp dpt:X ctstate NEW,ESTABLISHED

#DOCKER-USER#
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 3306 ctdir ORIGINAL
DROP tcp -- anywhere anywhere ctorigdstport 3306 ctdir ORIGINAL
ACCEPT tcp -- x.x.x.x anywhere ctorigdstport 443 ctdir ORIGINAL
DROP tcp -- anywhere anywhere ctorigdstport 443 ctdir ORIGINAL
```

---

The Guacamole service relies on a Docker architecture composed of three containers: Guacamole, Guacd, and MySQL. These three containers ensure user access to remote machines based on pre-defined access rights. Due to this server's exposure to the internet, strict security measures must be implemented to comply with the best practices recommended by OWASP. These measures are the same as those applied for the VPS implementation in chapter 5. Among the specificities of this implementation, several folders are used by Guacamole to manage specific functionalities (cf. listing 11). The mapped record folder is used by Guacamole and Guacd to store and retain provider sessions' video recordings. The drive folder, on the other hand,

serves as a shared memory area when using drive redirection or "RDPDR." This feature, native to the RDP protocol, allows for a virtual disk's emulation, thus avoiding the use of an SFTP connection, which would require the installation of an SSH server on all Windows servers, making it more complex to implement.

---

**Listing 11** Guacamole volume setup

---

```
services:
  guacd:
    *****
    volumes:
    - ./drive:/drive:rw
    - ./record:/var/lib/guacamole/recordings:rw

  guacamole:
    *****
    volumes:
    - ./drive:/drive:rw
    - ./record:/var/lib/guacamole/recordings:rw
*****
```

---

Two types of servers coexist within the HIS infrastructure: Linux servers and Windows servers. Microsoft offers several tools to facilitate the management of these servers, including LAPS, which allows for the passwords' automatic renewal for local administrator accounts (not registered in Active Directory). LAPS' minimum password renewal period is 24 hours. However, although the renewal time is fixed, it can be disrupted by the servers' daily restarts or bugs. Therefore, the LAPS renewal period was set to 30 days, and the renewal, forced at a fixed time by a script (cf. appendix B). Regarding Linux servers, the script establishes an SSH connection for each server registered in the Guacamole database, resolving the retrieved names. Once the connection is established, the script generates a password that complies with the establishment's security policy and modifies the password on the server using the "passwd" command, while also updating the corresponding entry in the Guacamole database.

However, given that the batch server is still running on Windows Server 2016, version 6.2.4 of LAPS is not available, and only the older version 5.0.0 can be installed. This situation

is problematic because only the "Reset-AdmPwdPassword" cmdlet can be used. This cmdlet allows resetting the local administrator account password during the next application of the GPO, and corresponds to the current "Set-LapsADPasswordExpirationTime" cmdlet. Therefore, a second part of the script will be executed shortly after to retrieve the newly renewed passwords.

The various helper scripts enable administrators to easily create new users, groups, and connections in Guacamole, which is essential. Indeed, many steps are repetitive and require precisely following the documentation to avoid any errors. The developed application relies on a Python script that uses the Guacamole REST API [103] to interact directly with the platform. This interactive script, visible in appendix C, allows choosing the type of object to create and then prompts the user to fill in only the distinctive elements of each instance. It is divided into two parts: the authentication of the administrator account, shown in listing 12, and the sending of the object creation requests presented in listing 13.

---

**Listing 12** Rest API Authentication

---

```
def get_auth_token():
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/x-www-form-urlencoded'
    }

    data = {
        'username': GUAC_ADMIN_USER,
        'password': GUAC_ADMIN_PASS
    }

    response = requests.post(f"{GUACAMOLE_URL}/tokens",
        headers=headers, data=data, verify=False)

    if response.status_code == 200:
        return response.json()['authToken']
    else:
        print(f"Failed to authenticate.
            Status code: {response.status_code}")
        return None
```

---

This function enables authentication with the Guacamole REST API. It sends the administrator's credentials via an HTTP POST request to obtain an authentication token, known as

"authToken". This token is subsequently used to validate the user's identity during subsequent calls to the API.

The Guacamole REST API utilizes the HTTP protocol to facilitate communication between a client (such as a Python application, a browser, or a tool like Postman) and the Guacamole server. Using well-structured HTTP requests (GET, POST, PUT, DELETE), it allows access to and dynamic management of various resources (users, remote connections, groups, etc.): creating, modifying, deleting, or simply viewing these elements. Documentation is sometimes provided to describe the different functionalities and options available for each actionable item. Although documentation for Guacamole is available [104], it is unfortunately not regularly updated, and necessitates a thorough analysis of the requests' content sent during the use of the web interface to infer their attributes.

---

**Listing 13** REST API Object Creation

---

```
def add_rdp_server(auth_token, name, identifier, login_server,
password_server):
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json;charset=UTF-8'
    }

    uri = f"session/data/mysql/connections?token={auth_token}"
    data = {
        "parentIdentifier": "ROOT",
        "name": name,
        "Identifier": identifier,
        "protocol": "rdp",
        "parameters": {
            "recording-include-keys": "true",
            "create-recording-path": "true",
            "enable-sftp": "true",
            "server-layout": "fr-fr-azerty",
            "timezone": "Europe/Paris",
            "console": "true",
            "drive-name": "${GUAC_USERNAME}",
            "drive-path": "./drive/${GUAC_USERNAME}",
            "create-drive-path": "true",
            "enable-drive": "true",
            "ignore-cert": "true",
            "hostname": name + ".chesquirol.AD",
            "username": login_server,
            "password": password_server,
            "recording-path": "${HISTORY_PATH}/${HISTORY_UUID}",
            "locale": "fr_FR.UTF-8",
        },
        "attributes": {
    }

    response = requests.post(f"{GUACAMOLE_URL}/{uri}",
headers=headers, json=data, verify=False)
```

---

This second feature highlights one of the application's functionalities. It allows the new connection's creation by filling in only a limited number of essential parameters. This method offers a significant time saving, as most other parameters are automatically set with default values, identical for all connections.

## 7.4 Transition for External Service Providers

The transition to the new remote maintenance platform necessitated a thorough revision of the tools and communication procedures with external service providers. All elements were updated, including the email template sent before a provider's first connection to the service, which can be resent upon request to ensure easy access to necessary information. This email has been entirely redesigned to include clear instructions on the connection procedure, technical prerequisites, and security best practices to follow. The associated documentation has also been reworked to ensure it covers all possible scenarios, including solutions to common problems and the specific cybersecurity guidelines imposed by the hospital.

As part of this transition, an access regularization for all service providers was also implemented. Mandatory contractual documents were signed by each provider who had not yet validated the administrator charter, which clearly defines the rights and responsibilities of each party when accessing critical infrastructure, as well as a confidentiality agreement. This agreement ensures that providers formally commit to not disclosing any sensitive information and to adhering to the strict data protection standards in effect in the hospital sector. This regularization makes providers legally responsible for their actions.

Finally, account sharing among employees of the same service provider remained a significant problem. It happened that multiple technicians from the same company used the same account to connect to the hospital's servers. This practice, in addition to raising questions about cybersecurity practices within the company, caused significant difficulties in terms of the performed actions' traceability. In the event of an incident, it was simply impossible to determine which employee was responsible without the cooperation of the affected company. A strict individual authentication policy has therefore been implemented. Now, each service provider has a personal account secured by two-factor authentication, and all connections to the platform are systematically logged and recorded.

# 8 Analysis of Results and Discussion

## 8.1 The CaRE Program's Limitations

While the CaRE program represents a significant step forward in integrating cybersecurity within healthcare facilities, its scope remains partial. Only 85% of eligible establishments responded to the call for applications. This situation may reflect various realities: some non-participating establishments may already have a cybersecurity level they deemed satisfactory, while most, on the contrary, would continue to run the risk of their systems failing under the attacks of malicious actors, which could directly impact the quality and safety of the care provided, unwilling or unable to participate in the program.

Furthermore, significant disparities also appear among the participating establishments. As hospital structures in France vary considerably in size, financial resources, and internal skills, some have experienced cybersecurity teams, while others must cope with limited human resources or information systems managers whose expertise is not always sufficient to meet the deadlines imposed by the program without assistance from the leading establishment of the THG (French Territorial Hospital Group).

The CaRE program sets the achievement of Level 2 maturity, as defined by ANSSI (National Agency for the Information Systems' Security), as its objective, although five levels are planned. This level essentially corresponds to a deepening of the correction of the most basic vulnerabilities, without, however, leading to a complete upgrade of the information system to state-of-the-art standards. While this choice allows for a rapid response to critical vulnerabili-

ties, it may also encourage some establishments to limit themselves to the strict minimum required, without committing to a continuous improvement or in-depth security approach. Aware of this limitation, the CaRE program Task Force has introduced a "Cybersecurity Baseline," updated regularly based on the results obtained in the various areas of assessment as well as the evolution of the cyber context. This baseline, integrated as a prerequisite in several major certifications sought by healthcare facilities, imposes a minimum level of security and thus aims to encourage the most lagging establishments to progress, while encouraging the most advanced structures to maintain their efforts.

Similarly, the scope of the audits carried out under the CaRE program is restricted. Third-party providers, who supply, install, and maintain the majority of business applications intended for hospital staff (except those handling health data, such as the electronic health record), as well as the software used by the HIS (Hospital's Information System) team, are not included in the program. These companies, as private entities, are not subject to the same security requirements. Indeed, no obligation compels these providers to secure their systems, and the responsibility then falls to the HIS team or that of the THG to take into account and test the security measures announced by the providers to minimize risks. Although one of the primary objectives of the CaRE program is the reduction of the attack surface, this approach is limited solely to the attack surface of the hospital's internal systems, without extending this reflection to the attack surface of the entire healthcare facility. Consequently, a significant part of the HIS infrastructure escapes the cybersecurity analysis carried out within the framework of this initiative. It would be relevant, in the context of future CaRE domains or a subsequent program, to implement mandatory security certifications for third-party companies to deem them eligible to work with healthcare facilities.

## 8.2 Evaluation of Security Improvements

The new remote maintenance platform has enabled the HIS teams to offer secure, centralized, and transparent remote access to the numerous service providers working on the hospital's

technical infrastructures. It notably allows for the secure management of credentials, the connections' monitoring, the traceability of actions performed on servers, as well as the fine-grained access limitation based on each provider's scope of intervention. Furthermore, the contractual framework governing service providers has been consolidated through rigorous and systematic monitoring. The mandatory signing of a commitment charter for external administrators has helped to strengthen their accountability regarding security best practices. The automation of periodic access rights reviews also facilitates the management of obsolete accounts, ensuring that each provider retains only the access strictly necessary for their tasks. The addition of a multi-factor authentication mechanism on the platform further hardens the security posture against credential theft or identity theft attacks.

The latest AKYL security audit reports (cf. figure 8.1) only three medium-level errors and five low-level errors. These results demonstrate the effectiveness of the implemented remediations, which have significantly reduced the HIS attack surface. The medium-level errors concern an expired and subsequently revoked certificate, the replacement of which with a more generic wildcard certificate is already planned for the coming months, and the lack of DNSSEC activation on a domain name that, although included in the audit, does not directly belong to the hospital but to the VPS host. This domain had been added as a precaution during testing, without any real impact on the main security perimeter. The low-level errors are related to the use of a wildcard certificate, the use of which is criticized for security reasons, as well as the presence of configuration files exposing certain technical information that has been verified and determined to be non-problematic.



Figure 8.1: Attack Surface and Internet Exposition Result Report Summary

For the AD (Active Directory) audit, the security level went up to level 3 as shown in figure 8.2. According to the ISARS report's conclusions, only two points remain to be addressed: the migration of the last privileged accounts to the "Protected Users" group and the redesign of the AD architecture. Validation of these two actions would allow reaching a maturity level of 5, thus positioning the directory at the highest recognized security standard, in line with the state-of-the-art. However, the privileged accounts' migration requires a particularly rigorous testing phase to anticipate and resolve potential side effects. This step often requires opening support tickets with Microsoft, a procedure that can be lengthy and complex. Furthermore, as detailed in section 6.4, the redesign of the AD architecture would involve a large-scale project, mobilizing significant human resources over a prolonged period. In the current context, this operation exceeds the organizational and technical capabilities of the HIS team and is not an immediate priority.



Figure 8.2: ORADAD Active Directory Result Report Summary

### 8.3 Limitations and Future Enhancements

The current approach mandated by the CaRE program relies on superficial audits aimed at identifying simple vulnerabilities, without in-depth interaction with the targeted systems. While this method constitutes an essential first step in assessing the security posture, it overlooks more

complex or contextual flaws. Penetration tests should be carried out in addition to identify application vulnerabilities, such as those listed in the Open Web Application Security Project (OWASP) repositories, notably the Top 10 [105] or OWASP Web Security Testing Guide [106]. The use of specialized tools such as Burp Suite, Metasploit, or Nmap in interactive mode would allow for further exploration of access control logics, code injection, session management, or configuration errors, thereby broadening the scope of audits and further limiting the attack surface.

While the ANSSI guide on the secure administration of Active Directory systems constitutes a reference resource [84], its recommendations, published in 2023, even when conscientiously applied, are not sufficient on their own to guarantee complete protection of the AD environment. This document mainly offers overall guidance aimed at structuring a robust security foundation, but it has several notable limitations. Firstly, other ANSSI recommendation guides must be followed to address issues related to security incident management and activity continuity procedures [107].

Furthermore, the proposed recommendations do not cover all current threats, particularly those related to dynamic configuration changes or newly identified vulnerabilities. The effective monitoring of AD relies on multiple aspects, including the analysis of logon events, account management, directory service access, network connections, object access, policy changes, privilege usage, as well as processes and system events tracking. However, the lack of event logs' rigorous supervision represents a critical vulnerability for the overall system's security. In this regard, the 2021 Verizon Data Breach Investigations Report [108] highlights that, although the event log analysis systems' strengthening by companies has significantly reduced the time to detect attacks since 2016, thus reversing the trend and allowing, in the majority of cases, a shift from detection in several months to detection in a few days or even a few hours, approximately 20% of security incidents continue, on average, to be discovered only after several months. In this regard, the use of open-source tools such as HardenAD [109] constitutes a relevant complement. These solutions not only allow for the remediation process automation of identified

vulnerabilities using PowerShell scripts, but also continuously monitor the AD environment to detect and correct any deviation from ANSSI recommendations.

This thesis was finalized before the integration of the SIEM (Security Information and Event Management) within the HIS, a future objective of the CaRE program, yet essential in any significant IT infrastructure. This tool allows for the real-time centralization, correlation, and analysis of events originating from the IS, such as system logs, authentication attempts, or network alerts, to detect threats and, in some cases, to prevent security incidents. The choice fell on a modular open-source solution, more financially accessible but more complex to implement and maintain than third-party tools like Splunk. This approach requires significant technical expertise and a lot of time for optimal maintenance and use, which raises the question of its sustainability. It will nevertheless serve as a basis for comparison when Domain 3 of the program is released and will, if necessary, be replaced in the future by a more robust and user-friendly external solution. Ultimately, this infrastructure should evolve to integrate advanced functionalities such as behavioral detection or predictive analysis, provided that the HIS teams can ensure its management with or without the support of external providers.

## 9 Conclusion

This thesis proposed an applied case study focusing on the strengthening of cybersecurity within a leading French hospital establishment. It is a continuation of an internship carried out as part of the establishment's participation in the CaRE program, whose main objective is to correct significant shortcomings in the French Hospital's Information Systems' cybersecurity. Three projects were implemented: reducing the attack surface and exposure through the migration of websites to a dedicated VPS (Virtual Private Server), deploying a secure remote maintenance platform, and hardening Active Directory following ANSSI's (National Agency for the Information Systems' Security) recommendations. Each of these interventions is presented from the needs analysis to the evaluation of results, including production deployment, with rigorous monitoring of the corrective actions implemented. Beyond the purely technical aspect, this thesis reaffirms that security is not a simple secondary objective added a posteriori, but a priority that must be taken into account even before the performance or ease of use of a chosen solution. The example of the solutions previously chosen for website hosting and the remote maintenance service is compelling; the solutions were chosen primarily for budgetary reasons. As a simple modification of the existing systems was not enough to fill the security gaps, additional costs and a significant investment of working time had to be provided. All of this could have been avoided if the security criterion had been considered prohibitive by the HIS (Hospital's Information System) team or that of the THG (Territorial Hospital Groups).

The results obtained demonstrate that it is indeed possible to establish solid foundations in operational security, even with limited resources, provided that a significant time investment

is dedicated to it. Although French healthcare facilities benefit from the support of the CaRE program through tools, methodological guides, and the assistance of the dedicated Task Force, the approach implemented within this framework: combining passive audits, targeted remediations, application of best practices, and the use of proven open-source solutions, is largely transferable. Indeed, the latter can be adapted to any type of organization, regardless of its size or workforce, wishing to structure an effective cybersecurity approach without resorting to significant financial investments.

Nevertheless, certain limitations persist, such as the implementation of in-depth penetration tests, the maintenance of a SIEM (Security Information and Event Management), the complete redesign of the AD (Active Directory) architecture, and, more broadly, the entire resulting IT structure. These can only be overcome with more substantial budgetary investments or a strengthening of internal skills, or even the recruitment of specialized profiles. Those difficulties are aggravated by the structural lack of positions' attractiveness within HIS, particularly in the field of cybersecurity. The differences in starting salaries [110] compared to the private sector [111], the limited salary progression based on seniority, as well as the widespread shortage of qualified professionals in the field of cybersecurity [112], all constitute factors that compromise the healthcare facilities' ability to plan serenely for the future.

Finally, the undertaken work must imperatively be continued and generalized to all establishments. The ongoing training of personnel, at all hierarchical levels, on HIS tools, coupled with increased awareness of cybersecurity issues, remains one of the most effective levers for preventing future attacks. The integration of prerequisites specific to the HIS and cybersecurity into the frameworks of mandatory healthcare facilities' certifications constitutes, in this respect, a decisive step forward in permanently anchoring these issues in their culture. Furthermore, the establishment of a Disaster Recovery Plan dedicated to digital infrastructures, as well as the development of a Cyber White Plan, are essential elements to guarantee a structured and resilient response in the event of a crisis. These extensions will ensure that security becomes an evolving and shared process within the establishments, capable of anticipating and neutralizing

emerging threats.

# References

- [1] Digital Health Agency, *The 50-year history of e-health*, <https://esante.gouv.fr/les-50-ans-dhistoire-de-la-e-sante>, Last Accessed: 06-05-2025, 2022.
- [2] Ministry of Labour Health Solidarity and Families, *Careers by job families*, <https://sante.gouv.fr/metiers-et-concours/les-metiers-de-la-sante/le-repertoire-des-metiers-de-la-sante-et-de-l-autonomie-fonction-publique/article/les-metiers-par-familles-de-metiers>, Last Accessed: 08-04-2025, 2023.
- [3] Les Echos, *Thirty french hospitals hit by cyberattacks over two years*, <https://www.lesechos.fr/economie-france/social/trente-hopitaux-francais-victimes-dune-cyberattaque-en-deux-ans-2130193>, Last Accessed: 08-04-2025, 2024.
- [4] National Cyber Security Centre, *A guide to ransomware*, <https://www.ncsc.gov.uk/ransomware/home>, Last Accessed: 08-04-2025, 2025.
- [5] Ministry of Labour Health Solidarity and Families, *Digital hospital program*, [https://sante.gouv.fr/IMG/pdf/HN\\_-\\_Boite\\_a\\_outils\\_pre-requis\\_-\\_Fiches\\_pratiques\\_-\\_Octobre\\_2012.pdf](https://sante.gouv.fr/IMG/pdf/HN_-_Boite_a_outils_pre-requis_-_Fiches_pratiques_-_Octobre_2012.pdf), Last Accessed: 16-04-2025, 2012.
- [6] French Hospital Federation, *Second edition of the "access to healthcare barometer": Public hospitals at a turning point*, <https://www.fhf.fr/actualites/communiques-de-presse/deuxieme-edition-du-barometre-de-laces-aux-soins-lhopital-public-un-tournant>, Last Accessed: 08-04-2025, 2025.

- 
- [7] Digital Health Agency, *Care program's presentation*, <https://esante.gouv.fr/espace-presse/presentation-du-programme-care>, Last Accessed: 23-04-2025, 2023.
- [8] French Accounts' Court, *Role and activities*, <https://www.ccomptes.fr/fr/cour-des-comptes/nous-decouvrir/role-et-activites>, Last Accessed: 16-04-2025, 2025.
- [9] French Accounts' Court, *Public and private healthcare facilities: Between competition and complementarity*, <https://www.ccomptes.fr/fr/publications/les-etablissements-de-sante-publics-et-privés-entre-concurrence-et-complementarite>, Last Accessed: 16-04-2025, 2023.
- [10] DREES (Department of Research, Studies, Evaluation and Statistics), *Hospital capacity in france, in 2019*, <https://drees.solidarites-sante.gouv.fr/sites/default/files/2021-07/Fiche%2002%20%20Les%20capacit%C3%A9s%20d%E2%80%99accueil%20%C3%A0%20l%E2%80%99h%C3%B4pital.pdf>, Last Accessed: 16-06-2025, 2019.
- [11] French Parliament, *Law no. 2016-41 of january 26, 2016, on the modernization of our healthcare system*, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031912641>, Last Accessed: 16-04-2025, 2016.
- [12] N. Boutier, *Activity centers: Organization, operation, articulation of the activity center contract with the medical plan*, <https://www.emfps.fr/article/poles-d-activite-organisation-fonctionnement-articulation-du-contrat-de-pole-avec-le-projet-medical>, Last Accessed: 16-04-2025, 2024.
- [13] Regional Health Agency, *The territorial hospital groupings*, <https://www.ars.sante.fr/les-groupements-hospitaliers-de-territoires>, Last Accessed: 16-04-2025, 2018.
- [14] Ministry of Labour Health Solidarity and Families, *Funding of health establishments*, <https://sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante->

- medico-social/financement/financement-des-etablissements-de-sante-10795/article/financement-des-etablissements-de-sante, Last Accessed: 14-04-2025, 2024.
- [15] V. Lucas-Gabrielli and C. Mangeney, “The shift to outpatient care: Patient safety and health inequalities”, *Actualité et dossier en santé publique (adsp)*, vol. 32, no. 118, pp. 46–49, 2022.
- [16] E. de La Roche Saint-André, *Did emmanuel macron close 17,600 hospital beds in four years, as françois ruffin claims?*, [https://www.liberation.fr/checknews/emmanuel-macron-a-t-il-ferme-17-600-lits-dhopital-en-quatres-ans-comme-laffirme-francois-ruffin-20211224\\_ZDEGBEMS4BHW3CGKLAOKL275ME/](https://www.liberation.fr/checknews/emmanuel-macron-a-t-il-ferme-17-600-lits-dhopital-en-quatres-ans-comme-laffirme-francois-ruffin-20211224_ZDEGBEMS4BHW3CGKLAOKL275ME/), Last Accessed: 16-04-2025, 2021.
- [17] A. Dagnet, *Fewer and fewer beds available in healthcare facilities but more outpatient care for patients, according to drees*, [https://www.francetvinfo.fr/sante/hopital/de-moins-en-moins-de-lits-disponibles-dans-les-etablissements-de-sante-mais-davantage-d-ambulatoire-pour-les-patients-selon-la-dress\\_6254856.html](https://www.francetvinfo.fr/sante/hopital/de-moins-en-moins-de-lits-disponibles-dans-les-etablissements-de-sante-mais-davantage-d-ambulatoire-pour-les-patients-selon-la-dress_6254856.html), Last Accessed: 16-04-2025, 2023.
- [18] French Press Agency, *Nearly 5,000 hospital beds were cut in 2023*, <https://www.ouest-france.fr/sante/hopital/pres-de-5-000-lits-ont-ete-supprimees-dans-les-hopitaux-en-2023-7d284a38-9745-11ef-81c3-38013e2f80e5>, Last Accessed: 06-05-2025, 2024.
- [19] Organisation for Economic Co-operation and Development, *2019 healthcare panorama*, [https://www.oecd.org/fr/publications/panorama-de-la-sante-2019\\_5f5b6833-fr/full-report.html](https://www.oecd.org/fr/publications/panorama-de-la-sante-2019_5f5b6833-fr/full-report.html), Last Accessed: 16-04-2025, 2019.
- [20] J. Tadduni, *Healthcare workers: Why they left the public hospital*, <https://www.if-saint-etienne.fr/politique-societe/soignants-pourquoi-ils-ont-quitte-lhopital-public>, Last Accessed: 16-04-2025, 2022.

- [21] Ministry of Labour Health Solidarity and Families, *Information systems medicalization program*, <https://sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/financement/financement-des-etablissements-de-sante-10795/financement-des-etablissements-de-sante-glossaire/article/programme-de-medicalisation-des-systemes-d-information-pmsi>, Last Accessed: 25-04-2025, 2017.
- [22] French Parliament, *Law no. 78-17 of January 6, 1978, relating to data processing, data files and individual liberties*. <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000006528059/1978-07-23/#LEGIARTI000006528059>, Last Accessed: 15-04-2025, 1978.
- [23] French Parliament, *Law no. 78-17 of January 6, 1978, relating to data processing, data files and individual liberties*. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>, Last Accessed: 16-04-2025, 2018.
- [24] European Parliament, *General data protection regulation*, <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr>, Last Accessed: 16-04-2025, 2016.
- [25] F. Ormancey, “It risk management in hospitals: Protecting confidentiality and data security at the dreux hospital center”, *Master Thesis, École Nationale de la Santé Publique, France*, 2003.
- [26] CERT-FR, *2024 cyber threat landscape*, <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>, Last Accessed: 19-05-2025, 2024.
- [27] French Senat, *Computerization in the healthcare sector: Finally grasping the scale of the challenges*, [https://www.senat.fr/rap/r05-062/r05-062\\_mono.html#toc100](https://www.senat.fr/rap/r05-062/r05-062_mono.html#toc100), Last Accessed: 16-04-2025, 2023.

- 
- [28] General Directorate for Healthcare Provision, *Digital hospital program*, [https://sante.gouv.fr/IMG/pdf/HN\\_-\\_Boite\\_a\\_outils\\_pre-requis\\_-\\_Fiches\\_pratiques\\_-\\_Octobre\\_2012.pdf](https://sante.gouv.fr/IMG/pdf/HN_-_Boite_a_outils_pre-requis_-_Fiches_pratiques_-_Octobre_2012.pdf), Last Accessed: 16-04-2025, 2012.
- [29] Ministry of Labour Health Solidarity and Families, *The hop'en program*, <https://sante.gouv.fr/systeme-de-sante/e-sante/sih/programme-hop-en/article/le-programme-hop-en>, Last Accessed: 16-04-2025, 2024.
- [30] Ministry of Labour Health Solidarity and Families, *The hop'en 2 program*, <https://sante.gouv.fr/systeme-de-sante/e-sante/sih/programme-hop-en/article/hopen-2>, Last Accessed: 16-04-2025, 2025.
- [31] Ministry of Labour Health Solidarity and Families, *Healthcare ségur: The conclusions*, <https://sante.gouv.fr/systeme-de-sante/segur-de-la-sante/article/segur-de-la-sante-les-conclusions>, Last Accessed: 17-04-2025, 2021.
- [32] French Government, *The national cybersecurity strategy for healthcare institutions*, <https://www.info.gouv.fr/actualite/la-strategie-nationale-de-cybersecurite-des-etablissements-de-sante>, Last Accessed: 15-04-2025, 2021.
- [33] Digital Health Agency, *Observatory of information system security incident reports for the health and social care sectors – public report 2023*, [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/observatoire-incidents-cybersecurite-sante-2023.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/observatoire-incidents-cybersecurite-sante-2023.pdf), Last Accessed: 19-04-2025, 2023.
- [34] World Economic Forum, *Global cybersecurity outlook 2025*, [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf), Last Accessed: 19-04-2025, 2023.
- [35] National Agency for the Information Systems' Security, *Healthcare sector – state of the cyber threat*, <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-010.pdf>, Last Accessed: 19-04-2025, 2023.

- [36] European Union Agency for Cybersecurity, *Enisa threat landscape: Health sector*, [https://s3-eu-west-1.amazonaws.com/static.hospimedia.fr/documents/227458/9389/Health\\_Threat\\_Landscape.pdf?1690209701=](https://s3-eu-west-1.amazonaws.com/static.hospimedia.fr/documents/227458/9389/Health_Threat_Landscape.pdf?1690209701=), Last Accessed: 19-04-2025, 2023.
- [37] N. Oufi, C. D. la Garza, J. Ma, F. Bouzon, and N. Lot, “Initial findings from a joint foh and cybersecurity analysis of a cyberattack in a hospital setting”, in *Congrès Lambda Mu 23: Innovations et maîtrise des risques pour un avenir durable*, 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement. hal-03875736, Institut pour la Maîtrise des Risques, Paris-Saclay, France, 2022.
- [38] M. S. Jalali and J. P. Kaiser, “Cybersecurity in hospitals: A systematic, organizational perspective”, *The Journal of Medical Internet Research*, vol. 20, no. 5, pp. 33–36, 2018.
- [39] French e-Health, *Care program*, [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/doc-programme-care-231214-20h\\_pap%5B17%5D.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf), Last Accessed: 06-05-2025, 2023.
- [40] Digital Health Agency, *Cyber solutions catalog*, <https://esante.gouv.fr/strategie-nationale/cybersecurite/catalogue-offres-cyber>, Last Accessed: 24-04-2025, 2025.
- [41] High Authority for Health, *Certification of healthcare institutions for quality of care*, [https://www.has-sante.fr/jcms/p\\_3219705/fr/la-certification-des-etablissements-de-sante-pour-la-qualite-des-soins](https://www.has-sante.fr/jcms/p_3219705/fr/la-certification-des-etablissements-de-sante-pour-la-qualite-des-soins), Last Accessed: 23-04-2025, 2020.
- [42] High Authority for Health, *Certification of healthcare institutions for quality of care*, [https://www.has-sante.fr/upload/docs/application/pdf/2025-01/referentiel\\_certification\\_es\\_qualite\\_des\\_soins\\_version\\_2025.pdf](https://www.has-sante.fr/upload/docs/application/pdf/2025-01/referentiel_certification_es_qualite_des_soins_version_2025.pdf), Last Accessed: 18-04-2025, 2025.

- [43] Regional Health Agency, *Multiannual contracts for objectives and resources*, <https://www.ars.sante.fr/les-contrats-pluriannuels-dobjectifs-et-de-moyens-1>, Last Accessed: 23-04-2025, 2024.
- [44] Ministry of Labour Health Solidarity and Families, *Decree establishing the special statute for the corps of hospital engineers*, [https://s3-eu-west-1.amazonaws.com/static.hospimedia.fr/documents/229145/9810/DGOS\\_4\\_projets\\_de%CC%81crets\\_inge%CC%81nieurs\\_hospitaliers\\_17.11.2023.pdf?1700477544](https://s3-eu-west-1.amazonaws.com/static.hospimedia.fr/documents/229145/9810/DGOS_4_projets_de%CC%81crets_inge%CC%81nieurs_hospitaliers_17.11.2023.pdf?1700477544), Last Accessed: 23-04-2025, 2023.
- [45] Digital Health Agency, *Care program: Presentation webinar*, [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/20240116\\_webinaire-presentation-programme-care--industriels\\_vf.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/20240116_webinaire-presentation-programme-care--industriels_vf.pdf), Last Accessed: 24-04-2025, 2024.
- [46] oSIS, *Osis v3*, <https://osis-v3.atih.sante.fr/>, Last Accessed: 02-05-2025, 2025.
- [47] S. Patel, A. Bhadouria, K. R. Dodiya, and A. Khunt, “Evaluating modern ransomware and effective data backup and recovery solutions”, *International Journal for Science and Advance Research In Technology*, vol. 10, no. 9, pp. 50–57, 2024.
- [48] AKYL, *Internet exposure audit*, <https://www.akyl.fr/outil-audit-exposition-internet-programme-care>, Last Accessed: 24-04-2025, 2025.
- [49] Digital Health Agency, *Care program - contact form*, [https://esante.gouv.fr/contact?contact\\_theme=programme\\_care](https://esante.gouv.fr/contact?contact_theme=programme_care), Last Accessed: 24-04-2025, 2025.
- [50] K. Dadheech, A. Choudhary, and G. Bhatia, “De-militarized zone: A next level to network security”, *Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 595–600, 2018.
- [51] Cisco DUO, *What are trusted devices?*, <https://duo.com/resources/glossary/what-are-trusted-devices>, Last Accessed: 06-05-2025, 2024.

- 
- [52] National Agency for the Information Systems' Security, *Recommendations regarding the interconnection of an information system to the internet*, [https://cyber.gouv.fr/sites/default/files/2020/06/anssi-guide-passerelle\\_internet\\_securisee-v3.pdf](https://cyber.gouv.fr/sites/default/files/2020/06/anssi-guide-passerelle_internet_securisee-v3.pdf), Last Accessed: 06-05-2025, 2020.
- [53] Paloalto Networks, *What is a perimeter firewall?*, <https://www.paloaltonetworks.com/cyberpedia/what-is-a-perimeter-firewall>, Last Accessed: 02-05-2025, 2024.
- [54] European Parliament, *General data protection regulation*, <https://gdpr-info.eu/>, Last Accessed: 30-04-2025, 2018.
- [55] E. McKeown, *What is web access management (wam)?*, <https://www.pingidentity.com/en/resources/blog/post/what-is-web-access-management-wam.html>, Last Accessed: 01-04-2025, 2021.
- [56] SSH Academy, *What is a jump server?*, <https://www.ssh.com/academy/iam/jump-server>, Last Accessed: 30-04-2025, 2025.
- [57] A.Harmon, *Understanding remote access protocols: Ssh, rdp, and vnc explained*, <https://galaxy.ai/youtube-summarizer/understanding-remote-access-protocols-ssh-rdp-and-vnc-explained-QbEDRTjcom4>, Last Accessed: 06-05-2025, 2024.
- [58] National Agency for the Information Systems' Security, *Organizing a cyber crisis management exercise*, <https://cyber.gouv.fr/sites/default/files/2020/10/anssi-guide-organiser-un-exercice-de-gestion-de-crise-cyber-v1.0.pdf>, Last Accessed: 21-04-2025, 2025.
- [59] AUCAE, *What does aucae do ?*, <https://aucae.com/fr/a-propos/>, Last Accessed: 21-04-2025, 2025.
- [60] French Government, *Expertcyber label*, <https://www.cybermalveillance.gouv.fr/label-expertcyber>, Last Accessed: 05-05-2025, 2025.
- [61] French Government, *France cybersecurity label*, <https://www.francecybersecurity.fr/en/>, Last Accessed: 05-05-2025, 2025.

- [62] French Government, *Expertcyber label - questions and answers*, <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/questions-reponses-faq>, Last Accessed: 21-04-2025, 2021.
- [63] Digital Health Agency, *Regional support group for the development of e-health (grades)*, <https://gnius.esante.gouv.fr/fr/acteurs/fiches-acteur/groupement-regional-dappui-au-developpement-de-la-e-sante-grades>, Last Accessed: 21-04-2025, 2025.
- [64] MindFlow, *Automate anything with securitytrails*, <https://mindflow.io/integrations/securitytrails>, Last Accessed: 21-04-2025, 2025.
- [65] Cloudflare, *What is a waf? - web application firewall explained*, <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>, Last Accessed: 21-04-2025, 2025.
- [66] Red Hat, *What is a cve?*, <https://www.redhat.com/en/topics/security/what-is-cve>, Last Accessed: 21-04-2025, 2024.
- [67] J. Risto, *What is common vulnerability scoring system (cvss score)*, <https://www.sans.org/blog/what-is-cvss/>, Last Accessed: 02-05-2025, 2023.
- [68] National Agency for the Information Systems' Security, *Active directory security service*, [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/20221013\\_np\\_anssi\\_fiche\\_ads\\_v3d-\(1\).pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/20221013_np_anssi_fiche_ads_v3d-(1).pdf), Last Accessed: 02-05-2025, 2022.
- [69] National Agency for the Information Systems' Security, *The active directory security (ads) service: Supporting the securing of active directory directories for critical stakeholders*, <https://cyber.gouv.fr/actualites/le-service-active-directory-security-ads-accompagner-la-securisation-des-annuaires>, Last Accessed: 22-04-2025, 2020.
- [70] ORADAD, *What is oradad?*, <https://github.com/ANSSI-FR/ORADAD>, Last Accessed: 22-04-2025, 2025.

- 
- [71] ISARS, *What does isars do ?*, <https://isars.company/>, Last Accessed: 22-04-2025, 2025.
- [72] D. Schrader, *Identifying common open port vulnerabilities in your network*, <https://blog.netwrix.com/open-ports-vulnerability-list>, Last Accessed: 18-04-2025, 2024.
- [73] A. Humphreys, *Types of security threats of session initiation protocol (sip)*, <https://blog.simplicityvoip.net/types-of-security-threats-of-session-initiation-protocol-sip>, Last Accessed: 18-04-2025, 2021.
- [74] M. Bator, J. Przystasz, and M. Serafin, “Security of the dnssec protocol and its impact on online privacy protection”, *Advances in Web Development Journal*, vol. 1, no. 5, pp. 43–63, 2023.
- [75] S. Ariyapperuma and C. J. Mitchell, “Security vulnerabilities in DNS and DNSSEC”, in *The Second International Conference on Availability, Reliability and Security (ARES’07)*, Institut pour la Maîtrise des Risques, Vienna, Austria, 2007, pp. 335–342.
- [76] Login Press, *How to hide wordpress login page from hackers (4 easy methods)*, <https://loginpress.pro/hide-wordpress-login-page-from-hackers/>, Last Accessed: 18-04-2025, 2025.
- [77] OWASP WSTG Web Publishing Bot, *Review old backup and unreferenced files for sensitive information*, [https://github.com/OWASP/www-project-web-security-testing-guide/blob/master/latest/4-Web\\_Application\\_Security\\_Testing/02-Configuration\\_and\\_Deployment\\_Management\\_Testing/04-Review\\_Old\\_Backup\\_and\\_Unreferenced\\_Files\\_for\\_Sensitive\\_Information.md](https://github.com/OWASP/www-project-web-security-testing-guide/blob/master/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/04-Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information.md), Last Accessed: 18-04-2025, 2024.
- [78] OWASP, *Docker security cheat sheet*, [https://cheatsheetseries.owasp.org/cheatsheets/Docker\\_Security\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html), Last Accessed: 06-05-2025, 2025.

- [79] S. Upadhyaya and J. Shetty, “A state-of-art review of docker container security issues and solutions”, *The Computer Journal*, vol. 17, no. 1, pp. 33–36, 2016.
- [80] Docker, *Docker documentation: Rootless mode*, <https://docs.docker.com/engine/security/rootless/>, Last Accessed: 13-02-2025, 2025.
- [81] B. Hardill, *Creating fail2ban rules*, <https://blog.hardill.me.uk/2020/07/15/creating-fail2ban-rules/>, Last Accessed: 08-04-2025, 2020.
- [82] O. Thomas and R. Harwood, *Configure fine grained password policies for active directory domain services*, <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/fine-grained-password-policies?tabs=adac>, Last Accessed: 28-04-2025, 2024.
- [83] A. Moillic, *How to configure and manage the active directory password policy*, <https://blog.netwrix.fr/2024/05/02/comment-configurer-et-gerer-la-strategie-de-mot-de-passe-active-directory/>, Last Accessed: 28-04-2025, 2024.
- [84] National Agency for the Information Systems’ Security, *Recommendations regarding the secure administration of information systems based on microsoft active directory*, [https://cyber.gouv.fr/sites/default/files/document/anssi-guide-admin\\_securisee\\_si\\_ad\\_v1-0%20%283%29.pdf](https://cyber.gouv.fr/sites/default/files/document/anssi-guide-admin_securisee_si_ad_v1-0%20%283%29.pdf), Last Accessed: 07-05-2025, 2023.
- [85] A. Paul and M. Dhiman, *Kerberos with service principal name (spn)*, <https://learn.microsoft.com/en-us/azure/azure-local/manage/kerberos-with-spn?view=azloc-24112>, Last Accessed: 28-04-2025, 2025.
- [86] D. Demers and H. Lee, “Case studies of an attack on a cryptographic authentication technology. international journal of cybersecurity intelligence & cybercrime”, *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 2, pp. 25–39, 2022.
- [87] Rich, *Dangerous rights cheatsheet*, <https://happycamper84.medium.com/dangerous-rights-cheatsheet-33e002660c1d>, Last Accessed: 29-04-2025, 2023.

- 
- [88] Tenable, *Write dacl*, <https://docs.tenable.com/identity-exposure/SaaS/Content/User/AttackPath/WriteDACL.htm>, Last Accessed: 29-04-2025, 2025.
- [89] Tenable, *Write owner*, <https://docs.tenable.com/identity-exposure/SaaS/Content/User/AttackPath/WriteOwner.htm>, Last Accessed: 29-04-2025, 2025.
- [90] Microsoft, *Reducing permissions required to run exchange server when you use the shared permissions model*, <https://support.microsoft.com/en-us/topic/reducing-permissions-required-to-run-exchange-server-when-you-use-the-shared-permissions-model-e1972d47-d714-fd76-1fd5-7cdcb85408ed>, Last Accessed: 29-04-2025, 2025.
- [91] P. Bouška, *Kerberos deactivation rc4*, <https://www.samuraj-cz.com/en/article/kerberos-deactivation-rc4-part-1-protocol-principle-and-encryption-types/>, Last Accessed: 06-05-2025, 2024.
- [92] G.Leurent and T. Peyrin, “Sha-1 is a shambles: First chosen-prefix collision on sha-1 and application to the pgp web of trust”, *Proceedings of the 29th USENIX Security Symposium*, pp. 1839–1856, 2020.
- [93] M. Lewis and R. Harwood, *Protected users security group*, <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group#how-the-protected-users-group-works>, Last Accessed: 29-04-2025, 2025.
- [94] itm8.com, *The fundamentals of ad tiering*, <https://itm8.com/articles/fundamentals-ad-tiering>, Last Accessed: 07-05-2025, 2024.
- [95] Specops, *Comment configurer et gérer la stratégie de mot de passe active directory*, <https://specopsoft.com/support/fr/password-reset/understanding-privileged-accounts-and-admins-holder.htm>, Last Accessed: 29-04-2025, 2025.
- [96] Microsoft, *The add operation*, <https://ldap3.readthedocs.io/en/latest/add.html>, Last Accessed: 29-04-2025, 2025.

- 
- [97] C. Thompson, *Do you own your permissions, or do your permissions own you?*, <https://posts.specterops.io/do-you-own-your-permissions-or-do-your-permissions-own-you-c829a91f5e45>, Last Accessed: 07-05-2025, 2025.
- [98] Microsoft, *Kb5008383—active directory permissions updates (cve-2021-42291)*, <https://support.microsoft.com/en-us/topic/kb5008383-active-directory-permissions-updates-cve-2021-42291-536d5555-ffba-4248-a60e-d6cbc849cde1>, Last Accessed: 29-04-2025, 2024.
- [99] Apache Guacamole, *Apache Guacamole Manual*, <https://guacamole.apache.org/doc/gug/>, Last Accessed: 10-04-2025, 2025.
- [100] G. Ramakrishnan, “Use Cases of Apache Guacamole in Remote Work”, *International Journal of Computer Trends and Technology*, vol. 72, no. 11, pp. 172–177, 2024.
- [101] M. Hein, “Rustdesk, an open-source solution for self-hosting”, *Journées réseaux de l’enseignement et de la recherche (JRES)*, 2024, Renater, Rennes, France. hal-04894008.
- [102] Apache Software Foundation, *Cve-2023-43826*, <https://nvd.nist.gov/vuln/detail/CVE-2023-43826>, Last Accessed: 06-05-2025, 2025.
- [103] Red Hat, *What is a rest api?*, <https://www.redhat.com/en/topics/api/what-is-a-rest-api>, Last Accessed: 22-04-2025, 2020.
- [104] R. Altun, *Guacamole rest api documentation*, <https://github.com/ridvanaltun/guacamole-rest-api-documentation/tree/master/docs>, Last Accessed: 22-04-2025, 2021.
- [105] OWASP, *Owasp top ten*, <https://owasp.org/www-project-top-ten/>, Last Accessed: 28-04-2025, 2025.
- [106] OWASP, *Web security testing guide project*, <https://owasp.org/www-project-web-security-testing-guide/v42/>, Last Accessed: 20-03-2025, 2025.

- [107] National Agency for the Information Systems' Security, *Cyberattacks and remediation remediation of active directory tier 0*, [https://cyber.gouv.fr/sites/default/files/document/20230417\\_np\\_anssi\\_remediation\\_volet-technique\\_tiers0-active-directory\\_v0\\_1.pdf](https://cyber.gouv.fr/sites/default/files/document/20230417_np_anssi_remediation_volet-technique_tiers0-active-directory_v0_1.pdf), Last Accessed: 30-04-2025, 2023.
- [108] VERIZON, *Dbir 2021 data breach investigation report*, <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>, Last Accessed: 20-03-2025, 2021.
- [109] J.-M. Thiat, *Harden ad: A path toward oradad level 5 and beyond...* <https://webtv.univ-lille.fr/video/13005/harden-ad-un-chemin-vers-oradad-niveau-5-et-plus%E2%80%A6>, Last Accessed: 20-03-2025, 2024.
- [110] Emploi-Collectivités, *Salary scale for senior hospital engineer*, <https://www.emploi-collectivites.fr/grille-indiciaire-hospitaliere-ingenieur-hospitalier-principal/4/101/249.htm>, Last Accessed: 29-04-2025, 2025.
- [111] Etudestech, *Cybersecurity job salaries in 2023*, <https://etudestech.com/decryptage/salaire-cybersecurite-metier-etude/>, Last Accessed: 12-04-2025, 2023.
- [112] G. Misheva, *Mind the cyber skills gap: A deep-dive*, <https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive>, Last Accessed: 06-05-2025, 2023.
- [113] M.Gautier, *Annual cost of cybercrime in france from 2016 to 2028*, <https://fr.statista.com/previsions/550410/couts-annualises-de-l-industrie-aux-etats-unis-dus-a-la-cybercriminalite-en-par-industrie>, Last Accessed: 16-04-2025, 2025.

# Appendix A : Service Provider Q&A

This appendix includes all the questions asked to Mr. Schimtin during the interview. The original responses, written in French, have been preserved in order to accurately reflect the interviewee's words, without altering their meaning or phrasing. An English translation, between "[ ]" brackets, is provided for informational purposes only, to aid understanding for non-French-speaking readers. However, this translation is intended solely as a reference and may not fully capture the intentions or nuances expressed in the original responses.

Technical questions:

Did you develop your EWS solution specifically for the CaRE program, or is it based on an existing offering of your services?

C'est un développement spécifique (que nous ferons vivre après le programme CaRE).

[It is a specific development (that we will maintain and evolve after the CaRE program).]

What tools and technologies is your solution based on?

C'est un outil fait maison, qui orchestre sous le capot des outils open source : nmap, nuclei, dig... Et nous faisons appel des APIs (shodan et security trails principalement, mais il y en a d'autres).

[It is a home-grown tool that orchestrates open-source tools under the hood: nmap, nuclei, dig... And we use APIs (mainly Shodan and SecurityTrails, but there are others).]

How do you detect the domains and subdomains associated with the declared assets?

travers de multiples méthodes de l'outil subfinder. Les résultats les plus intéressants proviennent de l'API Security Trails dont la clé est renseignée dans subfinder.

[Through multiple methods of the subfinder tool. The most interesting results come from the Security Trails API, whose key is provided in subfinder.]

What measures are in place to limit the impact of the audit on the information systems being tested, particularly during port scans? Do you have specific thresholds for these audits? If not, how do you define the limit of requests sent?

Nous avons fait de nombreux tests avec certains grades avant le lancement de CaRE pour ajuster les commandes nmap et nuclei. Nous avons une limite de concurrence des requêtes et de volume par minute qui, d'après nos essais, n'a généralement pas d'effet de bord. Dans le doute, nous laissons malgré tout le choix à nos clients parmi 3 vitesses.

[We conducted numerous tests with certain grades before the launch of CaRE to fine-tune the nmap and nuclei commands. We have a limit on concurrent requests and volume per minute which, according to our tests, generally has no side effects. If in doubt, we still give our clients a choice of 3 speeds.]

In your presentation sheet, you state: "Our risk-free scanner for your assets detects obvious vulnerabilities that an attacker could exploit".

What do you consider "obvious vulnerabilities"?

Les vulnérabilités évidents sont celles qui ressortent sans nécessité d'être authentifié ou de crawler les différentes routes. Si des vulnérabilités se cachent derrière des authentifications ou des routes cachées, elles sont moins « évidentes ». Par ailleurs, le cahier des charges de CaRE exclue les tests plus offensifs.

[Obvious vulnerabilities are those that emerge without the need for authentication or crawling different routes. If vulnerabilities are hidden behind authentications or concealed routes, they are less 'obvious'. Furthermore, the CaRE program specifications exclude more offensive testing.]

According to you, what vulnerabilities might your solution not detect? How do you account for this in your reports?

Vulnérabilités authentifiées, vulnérabilités web, vulnérabilités cachées derrière des routes obscures, ou des vulnérabilités sur des actifs derrière un WAF. Notre offre inclue l'intervention d'un analyste qui peut compléter manuellement certaines choses pour compenser la passivité des audits, tout en conservant l'innocuité des actions menées.

[Authenticated vulnerabilities, web vulnerabilities, vulnerabilities hidden behind obscure routes, or vulnerabilities on assets behind a WAF. Our offer includes the intervention of an analyst who can manually supplement certain things to compensate for the passive nature of the audits, while maintaining the harmlessness of the actions taken.]

Do the detected vulnerabilities correspond only to those that the CaRE program requires to be corrected, or does your solution go beyond the imposed scope? If your solution goes further, how far?

Uniquement les vulnérabilités CaRE, il ne faut pas aller plus loin dans le cadre du programme car cela mettrait en difficulté les établissements par rapport aux autres solutions. Cependant, nous avons d'autres modules d'audit prévus pour les clients qui utilisent la solution en dehors du programme CaRE, et qui vont plus loin.

[Only the CaRE vulnerabilities; we must not go further within the program's scope, as this would put the healthcare facilities at a disadvantage compared to other solutions. However, we have other audit modules planned for clients who use the solution outside the CaRE program, and these go further.]

The criticality level seems to be based on the maximum CVSS score of the identified CVEs. However, many vulnerabilities (perhaps the majority) are not associated with any CVE. Why are these vulnerabilities not linked to a CVE? What criteria do you then use to assess their criticality?

Une vulnérabilité n'a pas forcément de CVE. Une CVE correspond à la publication d'un défaut de conception sur un produit logiciel courant. Un défaut de configuration, par exemple, est une vulnérabilité, mais ne reflète pas un défaut de conception, mais un défaut d'utilisation, il n'y a donc pas de CVE. Dans ce cas, c'est le cahier des charges qui définit le niveau de criticité. Nos analystes sont des pentesters expérimentés et peuvent par ailleurs évaluer justement les vulnérabilités sans CVEs.

[A vulnerability does not necessarily have a CVE. A CVE corresponds to the publication of a design flaw in a common software product. A configuration defect, for example, is a vulnerability but does not reflect a design flaw, but rather a usage defect, so there is no CVE. In this case, it is the specifications that define the level of criticality. Our analysts are experienced pentesters and can also accurately assess vulnerabilities without CVEs.]

How is the criticality level of a vulnerability determined when no CVSS score is available?

Selon le cahier des charges et l'expérience de nos analystes.

[According to the specifications and the experience of our analysts.]

Have you had to adapt your solution based on feedback from healthcare facilities? If so, what adjustments have been made?

Oui, nous avons notamment travaillé sur les niveaux des vulnérabilités, les types de mires d'authentification détectées, la présentation des résultats, la traçabilité des résultats réajustés par nos analystes. Nous avons travaillé en phase pilote avec des GRADeS et des THGs.

[Yes, we have notably worked on the levels of vulnerabilities, the types of authentication end-

points detected, the presentation of results, and the traceability of results adjusted by our analysts. We worked in a pilot phase with GRADeS and THGs.]

How does your solution distinguish itself from those of your direct competitors?

Il s'agit d'un produit créé sur mesure, parfaitement adapté au programme CaRE. La validation par un agent humain a été intégrée directement sur la plateforme, alors que chez certains concurrents il faut passer par un processus de support peu approprié. Enfin, nos clients peuvent lancer leurs audits automatisés en illimité, sur autant d'actifs que souhaité, cela nous différencie et donne plus d'autonomie aux clients qui souhaitent en avoir par rapport aux offres de concurrents qui réalisent leurs audits de manière fixe (mensuellement. . .).

[It is a custom-built product, perfectly tailored to the CaRE program. Validation by a human agent has been integrated directly into the platform, whereas with some competitors, you have to go through a less appropriate support process. Finally, our clients can launch their automated audits unlimitedly, on as many assets as desired. This differentiates us and gives more autonomy to clients who wish to have it compared to competitors' offers that perform their audits on a fixed basis (monthly, etc.).]

Administrative questions:

How did you become aware of the CaRE program?

Un membre de notre équipe était dans la task-force CaRE. Et nous sommes très présents sur le secteur de la santé.

[A member of our team was on the CaRE task force. And we have a strong presence in the healthcare sector.]

What motivated you to propose a solution dedicated to this program?

La possibilité de proposer une offre que nous jugions adéquate à des clients secteur santé que nous connaissions, et de ne pas laisser le terrain à des acteurs étrangers (au secteur, et concernant la souveraineté).

[The opportunity to offer what we considered a suitable solution to healthcare sector clients we knew, and to not leave the field open to foreign players (both to the sector and concerning sovereignty).]

On your website, we can read: "Discover EWS, your exposed surface monitoring tool, guaranteed compliant with the CaRE program domain 1."

Who guarantees the compliance of your solution with the CaRE program?

Aucune structure publique n'a voulu se porter garante. Nous avons donc travaillé au mieux sur le cahier des charges, en veillant à respecter scrupuleusement chaque point à travers un développement spécifique. De nombreux GRADeS ont choisi la solution après une phase de test. La garantie finale repose dans le fait que nos analystes valident chaque rapport envoyé à l'ANS, il ne s'agit donc pas que d'un outil, si ce dernier présentait des non-conformités, nos analystes pourraient les corriger manuellement.

[No public structure was willing to act as guarantor. So, we worked to the best of our ability on the specifications, ensuring that we scrupulously respected each point through a specific development. Many GRADeS chose the solution after a testing phase. The final guarantee lies in the fact that our analysts validate each report sent to the ANS (French National Health Agency); it is therefore not just a tool. If the tool presented non-conformities, our analysts could correct them manually.]

Can you describe the validation process of a solution by the competent authorities?

Il n'existe pas. Nous avons fait des PoC, et rempli des tableurs où nous avons expliqué à des

GRADeS les mesures techniques mises en place pour être conforme au CDC.

[It does not exist. We did PoCs (Proof of Concepts) and filled out spreadsheets where we explained to GRADeS the technical measures implemented to comply with the specifications.]

How long did it take to create the solution, and then for its validation?

Environ 2 mois pour la beta, 3 mois pour peaufiner et valider avec quelques GRADeS.

[About 2 months for the beta, 3 months to refine and validate with a few GRADeS.]

How did the validation process of your solution by the competent authorities unfold? Were you supported or audited?

Aucune autorité n'a validé de solutions d'industriels dans le cadre du programme CaRE.

[No authority has validated any industrial solutions within the framework of the CaRE program.]

What were the main difficulties encountered during all these stages?

Nous ne sommes pas producteurs de logiciel de base. Nous avons donc du travailler longuement et lourdement sur l'infrastructure pour qu'elle tienne la charge des audits. C'est un développement qui n'est pas anodin, surtout que nous avons eu plus de clients que prévu. Techniquement nous avons rencontrés d'énormes problèmes avec notre infrastructure cloud (Scaleway surtout, OVH aussi dans une certaines mesure) qui a cruellement manqué de stabilité (crashes de nos serveurs hors de notre compétence, très régulièrement), nous avons été très déçus des offres souveraines qui n'ont pas permis d'assurer nos enjeux, là où AWS et les autres GAFAM répondent parfaitement à cela. Enfin, scanner des actifs chez des hébergeurs divers et variés a entraîné une perte de réputation des IPs dédiées, et nous avons été bannis par des équipements, ce qui a faussé les résultats de certains audits (une fois bannis, nous ne voyons plus rien, ou alors les firewalls nous remontent des résultats trompeurs). Nous avons aussi eu 2 plaintes car des clients ont scanné des actifs qui ne leurs appartenaient pas, sans le consentement des cibles...

[We are not producers of basic software. We therefore had to work long and hard on the infrastructure to ensure it could handle the load of the audits. It is a significant development, especially since we had more clients than expected. Technically, we encountered enormous problems with our cloud infrastructure (especially Scaleway, and OVH to some extent) which was sorely lacking in stability (crashes of our servers beyond our control, very regularly). We were very disappointed with the sovereign offerings, which did not allow us to meet our challenges, unlike AWS and the other GAFAMs, which perfectly address this. Finally, scanning assets at various and diverse hosting providers led to a loss of reputation for our dedicated IPs, and we were banned by some equipment, which skewed the results of certain audits (once banned, we see nothing, or the firewalls give us misleading results). We also had 2 complaints because clients scanned assets that did not belong to them, without the consent of the targets...]

Before adopting your solution, the THG used another solution that did not detect all the vulnerabilities required by the CaRE program and produced many false positives. Do you have any idea how this solution could have been declared compliant despite these limitations?

Oui, car aucune autorité ne s'est positionnée pour valider les déclarations des industriels. De nombreux acteurs ont utilisé des outils du marché (Nessus, etc.) comme base, sans faire l'effort d'implémenter des développements spécifiques. Nous avons demandé en début de programme à ce qu'on nous mette à disposition une plateforme que tous les industriels auditeraient pour que l'ANS puisse comparer les résultats, mais cela ne s'est pas fait. Nous aurions aimé nous comparer et nous améliorer. En réalité je ne jette pas la pierre aux concurrents, tous les acteurs qui ont tentés d'appliquer le cahier des charges et le mettre en application dans les délais demandés tout en garantissant un minimum de stabilité de la plateforme ont mon respect.

[Yes, because no authority has positioned itself to validate the declarations of the industrial players. Many actors used off-the-shelf tools (Nessus, etc.) as a base, without making the effort to implement specific developments. At the beginning of the program, we asked for a platform to be made available that all industrial players would audit so that the ANS could compare

the results, but this did not happen. We would have liked to compare ourselves and improve. In reality, I do not blame the competitors; all the actors who tried to apply the specifications and implement them within the requested deadlines while guaranteeing a minimum of platform stability have my respect.]

## Appendix B : Password Renewal's Script

---

**Listing 14** Server password management Part 1

---

```
$dbUser = "username"
$dbPassword = ConvertTo-SecureString -String "password" -AsPlainText -Force
$creds = New-Object -TypeName System.Management.Automation.PSCredential
-ArgumentList $dbUser, $dbPassword
$dbDatabase = "database_name"
$dbServer = "server_ip"
$dbPort = "server_port"

Open-MySQLConnection -Server $dbServer -Database $dbDatabase -Port $dbPort
-Credential $creds -WarningAction SilentlyContinue

*****

$connections = Invoke-SqlQuery -query "SELECT connection_name, protocol,
connection_id FROM guacamole_connection;"
$connectionNames = $connections | ForEach-Object { $_.connection_name }

foreach ($element in $connectionNames) {
    Reset-AdmPwdPassword -ComputerName:$element

*****

$connections = Invoke-SqlQuery -query "SELECT connection_name, protocol,
connection_id FROM guacamole_connection;"
```

---

**Listing 15** Server password management Part 2

---

```

foreach ($element in $connections) {
    $connection_name = $element.connection_name
    $connection_id = $element.connection_id

    $motDePasseLAPS = Get-AdmPwdPassword -ComputerName
    $element.connection_name | Select-Object -ExpandProperty Password

    if($motDePasseLAPS -ne $null)
    {
        Invoke-SqlUpdate -query "UPDATE guacamole_connection_parameter
        SET parameter_value = '$motDePasseLAPS' WHERE
        parameter_name = 'password' AND connection_id = '$connection_id';"
    }
    else
    {
        $motDePasseSSH = Invoke-SqlQuery -query "SELECT parameter_value FROM
        guacamole_connection_parameter WHERE parameter_name = 'password'
        AND connection_id = '$connection_id';"
        $pass = $motDePasseSSH.parameter_value

        $usernameSSH = Invoke-SqlQuery -query "SELECT parameter_value FROM
        guacamole_connection_parameter WHERE parameter_name = 'username'
        AND connection_id = '$connection_id';"
        $username = $usernameSSH.parameter_value

        $SecurePassword = ConvertTo-SecureString $pass -AsPlainText -Force
        $MyCreds = [System.Management.Automation.PSCredential]
        ::new($username, $SecurePassword)
        $session = New-SSHSession -ComputerName $element.connection_name
        -Credential $MyCreds -Port 22 -AcceptKey

        $newPassword = Generate-Password

        Invoke-SSHCommand -SSHSession $session -Command "echo -e
        '$pass\n$newPassword\n$newPassword' | passwd"

        Invoke-SqlUpdate -query "UPDATE guacamole_connection_parameter
        SET parameter_value = '$newPassword' WHERE parameter_name = 'password'
        AND connection_id = '$connection_id';"

        Remove-SSHSession -SSHSession $session -Verbose
    }
}
*****
Close-SqlConnection

```

---

## Appendix C : Python application's code

---

**Listing 16** Python Application's Code Part 1

---

```
import requests
import json
import os
import random
from datetime import date

# Guacamole server configuration
GUACAMOLE_URL = "https://guacamole.chesquirol.ad/api"
GUAC_ADMIN_USER = "xxxxxx"
GUAC_ADMIN_PASS = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

# files for the guacamole's reset :
user_file = 'init_guac/users.txt'
server_ssh_file = 'init_guac/servers_ssh.txt'
server_rdp_file = 'init_guac/servers_rdp.txt'
presta_file = 'init_guac/prestats.txt'

# Function to get an authentication token
# works only without double authentication activated
# look at documentation to disable it for administrator account
def get_auth_token():
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/x-www-form-urlencoded'
    }

    data = {
        'username': GUAC_ADMIN_USER,
        'password': GUAC_ADMIN_PASS
    }

    response = requests.post(f"{GUACAMOLE_URL}/tokens", headers=headers,
                             data=data, verify=False)

    if response.status_code == 200:
        return response.json()['authToken']
    else:
        print(f"Failed to authenticate. Status code: {response.status_code}")
        return None
```

---

---

**Listing 17** Python Application's Code Part 2

---

```
def add_user(auth_token, username, password, name, company, mail):
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json;charset=UTF-8'
    }
    current_date = date.today()
    formatted_date = current_date.strftime("%Y-%m-%d")
    uri = f"session/data/mysql/users?token={auth_token}"
    data = {
        "username": username,
        "password": password,
        "attributes": {
            "guac-email-address": mail,
            "access-window-start": "xx:xx:xx",
            "access-window-end": "xx:xx:xx",
            "valid-from": formatted_date,
            "valid-until": "xxxx-xx-xx",
            "timezone": "Europe/Paris",
            "guac-full-name": name,
            "guac-organization": company,
        }
    }

    response = requests.post(f"{GUACAMOLE_URL}/{uri}", headers=headers,
                             json=data, verify=False)

    if response.status_code == 200:
        return 1
    else:
        return 0
```

---

---

**Listing 18** Python Application's Code Part 3

---

```
def add_ssh_server(auth_token, name, identifier, login_server, password_server):

    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json;charset=UTF-8'
    }

    uri = f"session/data/mysql/connections?token={auth_token}"
    data = {
        "parentIdentifier": "ROOT",
        "name": name,
        "Identifier": identifier,
        "protocol": "ssh",
        "parameters": {
            "recording-include-keys": "true",
            "create-recording-path": "true",
            "enable-sftp": "true",
            "timezone": "Europe/Paris",
            "hostname": name + "xxxxxxxxxxxxxx",
            "username": login_server,
            "password": password_server,
            "recording-path": "${HISTORY_PATH}/${HISTORY_UUID}",
            "locale": "fr_FR.UTF-8",
        },
        "attributes": {
    }
}

response = requests.post(f"{GUACAMOLE_URL}/{uri}", headers=headers,
    json=data, verify=False)

if response.status_code == 200:
    return 1
else:
    return 0
```

---

---

**Listing 19** Python Application's Code Part 4

---

```
def add_rdp_server(auth_token, name, identifier, login_server, password_server):
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json;charset=UTF-8'
    }

    uri = f"session/data/mysql/connections?token={auth_token}"
    data = {
        "parentIdentifier": "ROOT",
        "name": name,
        "Identifier": identifier,
        "protocol": "rdp",
        "parameters": {
            "recording-include-keys": "true",
            "create-recording-path": "true",
            "enable-sftp": "true",
            "server-layout": "fr-fr-azerty",
            "timezone": "Europe/Paris",
            "console": "true",
            "drive-name": "${GUAC_USERNAME}",
            "drive-path": "./drive/${GUAC_USERNAME}",
            "create-drive-path": "true",
            "enable-drive": "true",
            "ignore-cert": "true",
            "hostname": name + "xxxxxxxxxxxxxx",
            "username": login_server,
            "password": password_server,
            "recording-path": "${HISTORY_PATH}/${HISTORY_UUID}",
            "locale": "fr_FR.UTF-8",
        },
        "attributes": {
    }
}

response = requests.post(f"{GUACAMOLE_URL}/{uri}", headers=headers,
    json=data, verify=False)

if response.status_code == 200:
    return 1
else:
    return 0
```

---

---

**Listing 20** Python Application's Code Part 5

---

```
def add_prestat(auth_token, name):
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json; charset=UTF-8'
    }

    uri = f"session/data/mysql/userGroups?token={auth_token}"
    data = {
        "identifier": name,
        "attributes":
        {
            "disabled": ""
        }
    }

    response = requests.post(f"{GUACAMOLE_URL}/{uri}", headers=headers,
                             json=data, verify=False)

    if response.status_code == 200:
        return 1
    else:
        return 0

def process_users_file(auth_token, file_path):
    with open(file_path, 'r') as file:
        lines = file.read().strip().split('\n')
        print(lines)
        for i in range(0, len(lines), 6):
            name = lines[i].strip()
            login = lines[i + 1].strip()
            password = lines[i + 2].strip()
            company = lines[i + 3].strip()
            mail = lines[i + 4].strip()

            print(f"Adding user: {name}, Login: {login}, Company: {company}")
            add_user(auth_token, login, password, name, company, mail)

def process_prestats_file(auth_token, file_path):
    with open(file_path, 'r') as file:
        lines = file.read().strip().split('\n')
        print(lines)
        for i in range(0, len(lines), 1):
            name = lines[i].strip()

            print(f"Adding presta: {name}")
            add_prestat(auth_token, name)
```

---

---

**Listing 21** Python Application's Code Part 6

---

```
def process_server_files(auth_token, file_ssh_path, file_rdp_path):
    with open(file_ssh_path, 'r') as file_ssh:
        with open(file_rdp_path, 'r') as file_rdp:
            lines_ssh = file_ssh.read().strip().split('\n')
            lines_rdp = file_rdp.read().strip().split('\n')
            print(lines_ssh)
            print(lines_rdp)

            identifier = 0
            for i in range(0, len(lines_ssh), 4):
                name = lines_ssh[i].strip()
                login_server = lines_ssh[i + 1].strip()
                password_server = lines_ssh[i + 2].strip()

                print(f"Adding server SSH: {name}")
                add_ssh_server(auth_token, name, identifier, login_server,
                               password_server)
                ++identifier

            for i in range(0, len(lines_rdp), 4):
                name = lines_rdp[i].strip()
                login_server = lines_rdp[i + 1].strip()
                password_server = lines_rdp[i + 2].strip()

                print(f"Adding server RDP: {name}")
                add_rdp_server(auth_token, name, identifier, login_server,
                               password_server)
                ++identifier

def clear_screen():
    os.system('clear')

def display_main_menu():
    print("=" * 40)
    display_ASCII_Art()
    print("=" * 40)
    print("1. Add a user")
    print("2. Add a connexion")
    print("3. Add a user group")
    print("4. reset Guacamole (!)")
    print("5. Exit")
    print("=" * 40)
    print("-" * 40)

def display_dilemma():
    print("=" * 40)
    print("1. Connexion RDP")
    print("2. Connexion SSH")
    print("=" * 40)
```

---

---

**Listing 22** Python Application's Code Part 7

---

```

def display_ASCII_Art():
    ascii_art = """
    ***** * * ***** ***** ***** * * ***** * * *****
    * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
    * ** * * ***** * ***** * * * * * * * * * * * * * *
    * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
    **** ***** * * ***** * * * * * * ***** ***** *****
    """
    print(ascii_art)

def init_guacamuc(auth_token):
    process_users_file(auth_token, user_file)
    process_prestats_file(auth_token, presta_file)
    process_server_files(auth_token, server_ssh_file, server_rdp_file)

def main():
    auth_token = get_auth_token()

    if auth_token:
        while True:
            clear_screen()
            display_main_menu()
            choix = input("What do you want to do? (1, 2, 3, 4, 5): ")

            if choix == '1':
                username = input("User's identifier (first name's first letter +
                last name): ")
                print("\r")
                password = input("User's password (32 characters ASCII): ")
                print("\r")
                name = input("User's fullname (first name + last name): ")
                print("\r")
                mail = input("User's e-mail: ")
                print("\r")
                company = input("User's company name: ")

                result = add_user(auth_token, username, password, name, company,
                mail)
                if result:
                    print("success")
                else:
                    print("failure")

```

---

---

**Listing 23** Python Application's Code Part 8

---

```
elif choix == '2':
    display_dilemma()
    protocol = input("What do you want to add? (1, 2): ")
    if protocol == '1':
        name = input("Serveur's DNS entry (full upper case): ")
        identifier = random.randint(1000, 100000)
        login_server = "*****"
        print("\r")
        password_server = input("LAPS's generated password")

        result = add_rdp_server(auth_token, name, identifier,
                                login_server, password_server)
        if result:
            print("success")
        else:
            print("failure")

    elif protocol == '2':
        name = input("Serveur's DNS entry (full upper case): ")
        identifier = random.randint(1000, 100000)
        login_server = input('server's login: ')
        print("\r")
        password_server = input("server's password (32 characters
                                ASCII): ")

        result = add_ssh_server(auth_token, name, identifier,
                                login_server, password_server)
        if result:
            print("success")
        else:
            print("failure")

    else:
        print("Incorrect choice")

elif choix == '3':
    name = input("service provider's name (full upper case): ")

    result = add_prestat(auth_token, name)
    if result:
        print("success")
    else:
        print("failure")

elif choix == '4':
    result = init_guacamuc(auth_token);

    if result:
        print("success")
    else:
        print("failure")

elif choix == '5':
    print("Goodbye !")
    break
```

---

**Listing 24** Python Application's Code Part 9

---

```
        else:
            print("Invalid choice, retry.")

            input("\nPress enter to continue...")
            print("\n" * 3)

if __name__ == '__main__':
    main()
```

---

# Appendix D : On The Use Of LLMs

This thesis was originally written in French, in an academic style that does not necessarily translate well to English. Chat-GPT, Gemini, and Mistral were used throughout this thesis to translate some paragraphs and to rephrase others. Multiple models were used because of the differences in the entropy of the LLM answer. The goal was always to choose the answer that was as close as possible, semantically and grammatically speaking, to the submitted text. The generated text is then modified to erase grammar errors that would not translate well between the two languages. The phrases are modified and verifications are made to ensure the LLM does not add unwanted ideas or remove others.

This unique prompt was used for translation:

translate to english : "<text to translate>"

Here is an example of the process:

The prompt :

"translate in english : "La mise en œuvre de la stratégie de remédiation des vulnérabilités liées à l'exposition internet des systèmes de l'hôpital a été un défi de taille, mettant en lumière les difficultés inhérentes à l'application de mesures de sécurité, même les plus élémentaires, dans un contexte réel.""

The LLM's answer :

"The implementation of the remediation strategy for vulnerabilities related to the internet exposure of the hospital's systems was a major challenge, highlighting the inherent difficulties of applying security measures, even the most basic ones, in a real-world context."

The final version after modifications :

"Implementing the remediation strategy for vulnerabilities related to the Internet exposure of the hospital's systems was a major challenge, highlighting the numerous difficulties of applying security measures, even the most basic ones, in a real-world context."

This unique prompt was used for rephrasing paragraphs in french:

reformule : "<text to rephrase>"

Here is an example of the process:

The prompt :

"reformule : "Enfin, Le partage de comptes entre employés d'un même prestataire est un autre fléau. Il arrivait que plusieurs techniciens d'une entreprise utilisent le même compte pour se connecter aux serveurs de l'hôpital. Cette pratique, en plus de questionner le respect des règles élémentaires de cybersécurité de cette entreprise, posait de sérieux problèmes en matière de traçabilité des actions effectuées sur les serveurs. En cas d'incident, il était, dans certains cas, très difficile de déterminer avec certitude quel employé avait réellement causé l'incident. Pour remédier à cela, une politique stricte d'authentification individuelle a été imposée. Chaque prestataire se voit désormais attribuer un compte personnel avec double authentification, et toute connexion à la plateforme est rigoureusement journalisée et filmée.""

The LLM's answer :

"Enfin, le partage de comptes entre les employés d'un même prestataire représentait un

autre problème majeur. Il arrivait que plusieurs techniciens d'une même entreprise utilisent le même compte pour se connecter aux serveurs de l'hôpital. Cette pratique, en plus de remettre en question le respect des principes fondamentaux de cybersécurité au sein de l'entreprise, entraînait des difficultés significatives en matière de traçabilité des actions réalisées sur les serveurs. En cas d'incident, il était parfois très compliqué de déterminer avec certitude quel employé était responsable. Pour résoudre ce problème, une politique stricte d'authentification individuelle a été mise en place. Désormais, chaque prestataire dispose d'un compte personnel sécurisé par une double authentification, et toutes les connexions à la plateforme sont systématiquement journalisées et filmées."

Same as the translation, additional modifications are made to the answer :

"Enfin, le partage de comptes entre les employés d'un même prestataire resté un fléau. Il arrivait que plusieurs techniciens d'une même entreprise utilisent le même compte pour se connecter aux serveurs de l'hôpital. Cette pratique, en plus de remettre en question les pratiques de cybersécurité au sein de l'entreprise, entraînait des difficultés significatives en matière de traçabilité des actions réalisées sur les serveurs. En cas d'incident, il était parfois impossible de déterminer avec certitude quel employé était responsable sans le concours de l'entreprise victime. Une politique stricte d'authentification individuelle a donc été mise en place. Désormais, chaque prestataire dispose d'un compte personnel sécurisé par une double authentification, et toutes les connexions à la plateforme sont systématiquement journalisées et filmées."