UMB

Enhancing the cybersecurity posture of Swiss Healthcare Institutions

C2SEC White Paper

Content

1 __ Executive Summary

Note at the beginning: this whitepaper has been originally issued our partner C2SEC.

Healthcare institutions in Switzerland and globally are prime targets for cyber threats due to their wealth of sensitive patient data and critical services. In the UK, nearly 80% of healthcare providers have reported a data breach since 2021 [1]. Also, data protection laws such as the European Union's General Data Protection Regulation (GDPR) [2] and Switzerland's Federal Act on Data Protection (FADP) [3] set high standards for data security and privacy. In 2022, The National Cybersecurity Centre NCSC recommended that all healthcare providers in Switzerland adhere to the minimum cybersecurity requirements [4].

This report delves into the external attack surfaces of 255 healthcare institutions across Switzerland. The key findings include:

- **10,000 + critical vulnerabilities identified, highlighting the need for a structured approach to vulnerability and asset management**. 78,005 security vulnerabilities are identified across healthcare institutions, with 13% of them have high and critical severity. This spotlights the pressing necessity for a structured approach to vulnerability, patch and asset lifecycle management, a mandatory NCSC requirement.
- **1,391 exposed login entries identified.** In addition, 7% of the institutions have more than 10 login entries. This illustrates **the challenges of user authentication management**, and particularly, how to enable multi-factor authentication (MFA) for all authentications, another mandatory item in NCSC's requirements.
- **A significant shift to cloud platforms is taking place.** 26% of the institutions have transitioned most of their digital assets to cloud platforms. Furthermore, there's a noticeable trend towards multi-cloud environments, with 45% of these institutions adopting multiple cloud services to boost operational flexibility and resilience.
- **In-depth case study of a leading university hospital** uncovers a vast digital asset presence encompassing 4,133 IP addresses and 6,529 subdomains that are hosted globally. This complexity demonstrates **the challenge of cybersecurity management when healthcare operations are integrated with larger educational institutions.**

The report then provides actionable recommendations to help healthcare institutions better align with NCSC's guidelines.

2 __ Introduction

Healthcare institutions in Switzerland and globally are at the forefront of cyber threats due to their repositories of sensitive patient information and the essential services they provide, making them prime targets for cyber-attacks.

March 2024 data of the U.S. Health and Human Services Office of Civil Rights (OCR) highlights 116 healthcare data breaches affecting over 13 million individuals [5]. In the UK, nearly 80% of frontline healthcare providers have experienced at least one data breach since 2021 [1]. A severe ransomware attack in May 2021 crippled Ireland's Health Service Executive (HSE), one of the country's largest medical systems, disrupting IT systems and forcing a return to paper-based records. [6].

Additionally, strict data protection laws such as the European Union's General Data Protection Regulation (GDPR) [2] and Switzerland's Federal Act on Data Protection (FADP) [3] enforce rigorous standards for data security and privacy. In 2022, The National Cybersecurity Centre NCSC recommended that all healthcare providers in Switzerland meet the minimum cybersecurity requirements [4]. These regulations pose considerable compliance challenges for Swiss healthcare entities, particularly those engaging with EU markets or managing EU citizens' data.

Effective management of external attack surfaces is the starting point for Swiss healthcare institutions to ensure regulatory compliance and maintain patient trust. This involves securing all internet-accessible assets such as web applications, cloud services, and network endpoints against unauthorized use. These assets are crucial in combating cyber threats. However, traditional security methods often fall short against sophisticated, evolving cyber threats and the growing digital presence of healthcare services, highlighting the need for more dynamic cybersecurity strategies.

C2SEC's Extended Security Posture Management (XSPM) platform offers a comprehensive overview of an institution's security stance, addressing external threats, cloud/SaaS vulnerabilities, and supply chain risks. This study uses the C2SEC platform to conduct an in-depth analysis of the external attack surfaces of Swiss healthcare providers, enhancing their cybersecurity with strategic insights and targeted actions to mitigate vulnerabilities.

3 __ Methodology

In our exhaustive analysis, we evaluated the cybersecurity posture of 255 healthcare institutions across all 26 Swiss Cantons [7]. This diverse group comprised seven prominent university hospitals, 36 cantonal and regional hospital groups, and a range of smaller clinics. Each institution, with its distinct domain identity as listed on the official website, was subjected to a thorough examination. Employing the cutting-edge, automated External Attack Surface Management (EASM) functionalities offered by the C2SEC platform, we embarked on a methodological journey throughout March 2024 to uncover the nuances of cybersecurity threats faced by these institutions.

The foundation of our approach was laid with non-intrusive scans of the primary root domains of each institution, a critical first step that enabled us to map the digital landscape without disrupting their operations. This initial phase kickstarted an intelligent workflow comprising data collection, normalization, and correlation, which facilitated a granular analysis of each institution's external attack surface. We then sifted through this data to identify, categorize, and analyze security vulnerabilities and gaps, adopting a holistic perspective to understand the myriad cybersecurity challenges confronting the Swiss healthcare sector.

To further enhance the depth of our analysis, we employed advanced algorithms and the latest cybersecurity frameworks to evaluate the severity and potential impact of the identified vulnerabilities. This included an assessment of risk factors associated with each vulnerability, considering factors such as the likelihood of exploitation and the potential consequences of a breach. Our methodology also integrated stakeholder feedback at various stages, ensuring that the analysis remained aligned with the operational realities and specific security concerns of the healthcare institutions.

By systematically dissecting the external attack surfaces of these institutions, our study aimed to not just catalog vulnerabilities but to provide a comprehensive understanding that could inform strategic cybersecurity enhancements. This methodical and data-driven approach was designed to empower Swiss healthcare institutions with actionable insights, enabling them to fortify their defenses against an increasingly sophisticated and dynamic cyber threat landscape.

4 __ The external attack surface

4.1 Asset Scale

The scale of digital assets an organization exposes directly influences its cyber risk profile; more assets equate to a broader attack surface. In our analysis of Swiss healthcare institutions, we specifically focused on IPv4 addresses and subdomains linked to their primary root domains, considering these as pivotal internet entry points and reliable indicators of the institution's overall attack surface.

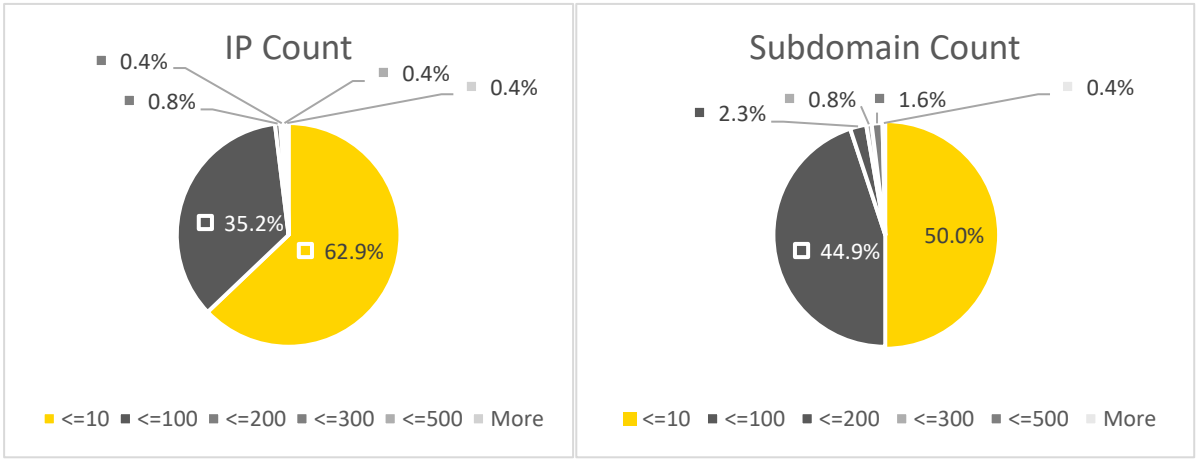

Figure 1: Distribution of Institution by Asset Size

Our comprehensive scans via the C2SEC platform unveiled a total of 7,831 IPs and 12,927 subdomains across the 255 surveyed institutions. The visualization in Figure 1 outlines the distribution of these entities according to their respective quantities of IP addresses and subdomains.

Analyzing the IP Count chart reveals that 160 institutions—62.9%—operate with 10 or fewer IP addresses, implying a strategy of either limited digital exposure or prudent cybersecurity practices. This majority predominantly consists of 144 clinics that offer limited or niche healthcare services, implying either a conservative digital approach or a strategic emphasis on cybersecurity. On the other hand, 35.2% of the surveyed institutions, including four university hospitals, 20 cantonal hospitals, and 66 clinics, exhibit a larger digital footprint, with IP counts ranging from 11 to 100, indicative of broader service offerings and a potentially more sophisticated digital infrastructure.

In terms of subdomain counts, the data paints a similar picture of diversity. While half of the institutions limit themselves to 10 or fewer subdomains, a substantial 44.9% oversee between 11 and 100 subdomains, hinting at greater online functionality and a more intricate web presence.

Despite the predominance of institutions with smaller digital profiles, there is an outlier with an exceptionally large digital footprint, exceeding 500 IP addresses and subdomains. This institution, as a university hospital,

represents a comprehensive healthcare operation with extensive services and patient interaction points. A detailed analysis of this case will be presented later in the report.

Furthermore, the data set incorporates critical elements of the institutions' foundational technology infrastructure, specifically, 396 email servers and 663 domain name servers (DNS). These figures not only reflect the operational requirements of the surveyed institutions but also represent aspects of the digital environment that require diligent management to ensure cybersecurity resilience.

Overall, the findings from these charts depict a sector characterized by diverse online engagement levels—ranging from modest, specialized operations to vast networks indicative of significant healthcare operations. This diversity underscores the necessity of cybersecurity strategies that are customized to address the unique digital footprints and infrastructure complexities of each institution.

4.2 Geo Location

Digital assets and data storage are directly impacted by the data regulations of the country they are located in. Hence, we analyzed the geographic locations of the IPs of the selected institutions. As illustrated by Figure 2, the assets are distributed over 17 countries where most institutions have assets in Switzerland while a few of them have assets in other countries. In specific, 93 institutions (including 4 university hospitals, 13 canton hospitals and 76 clinics) have assets in United States. Typically, the institutions rely on these oversea assets for CDN services from Cloudflare, IT support services from ServiceNow, and other cloud computing services from major cloud providers Azure, Amazon and Google.

Our analysis uncovered that eight institutions with small digital presence do not have any assets located within Switzerland. This small digital footprint aligns with the specialized nature of these clinics, which focus on niche healthcare services such as wellness, maternity care, and rehabilitation.

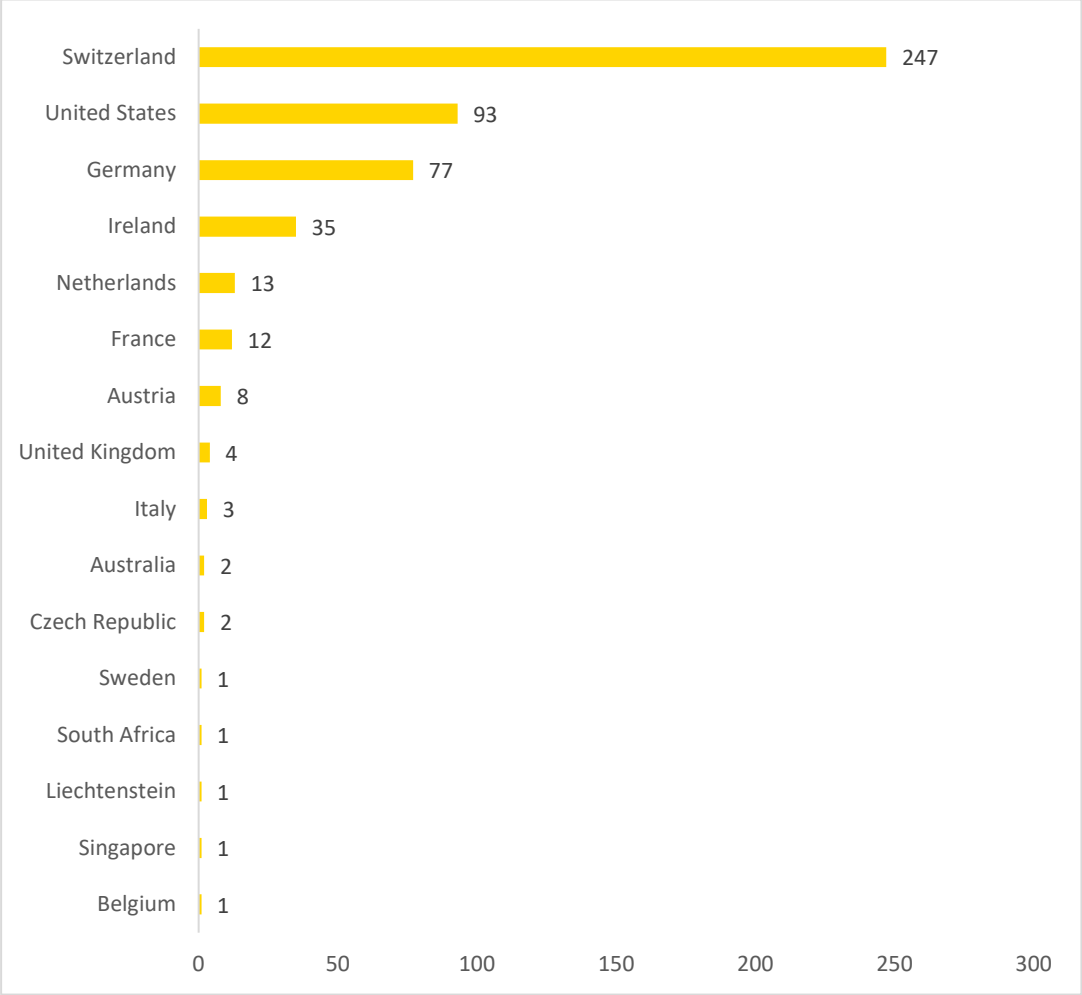

Figure 2: Asset Locations by Total Institutions

Furthermore, according to GDPR, we must monitor the security posture of assets not only in Europe but also outside Europe. Figure 3 shows the distribution of the proportion of non-EU assets for each institution.

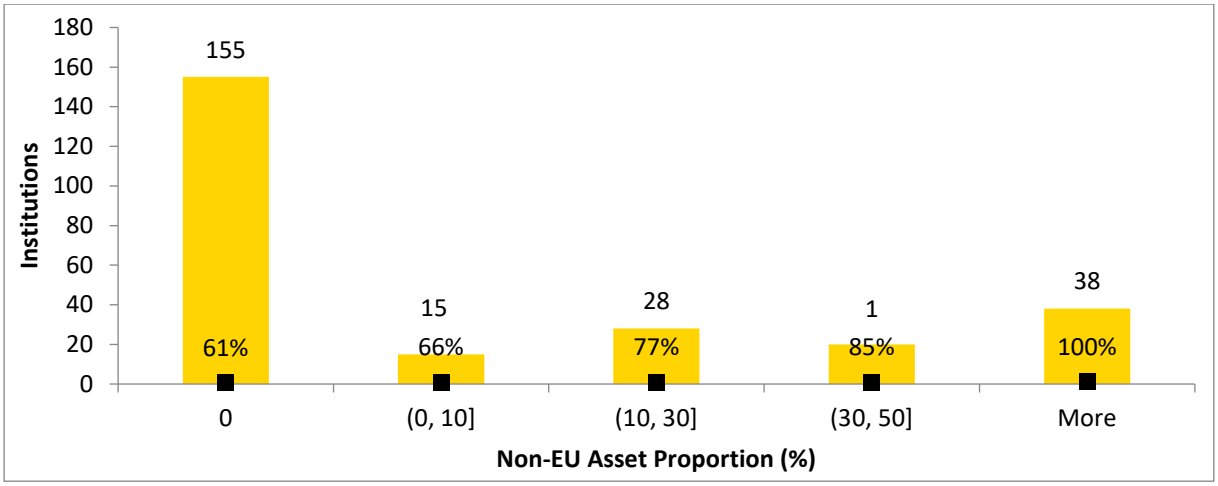

Figure 3: Histogram of Non-EU Asset

Our analysis unveiled a significant concentration 155 (61% of) healthcare institutions' digital assets in only Swiss regions, pointing to potential regional cybersecurity hotspots. Notably, the remaining 100 health institutions have assets located outside of Europe (including countries: United States, Australia, South Africa, Singapore) among which there are 38 institutions whose non-EU assets occupy over 50% of their total Internet assets. This suggests extended regulatory challenges, especially concerning HIPPA, GDPR compliance and international data protection laws.

4.3 Cloud Assets

The diversity in IP hosting and cloud service providers among the analyzed institutions reveals a fragmented cybersecurity landscape. This diversity, while beneficial for avoiding vendor lock-in, introduces complexities in maintaining a consistent and robust security posture and brings extra challenges for data protection.

We analyzed the IP host providers of these institutions and for each institution we identified the proportion of assets hosted in the major 25 cloud service providers on the Swiss market. Despite the scope being limited to these providers, the resulting analysis is indicative of the prevailing tendencies toward cloud technology adoption within the Swiss healthcare sector.

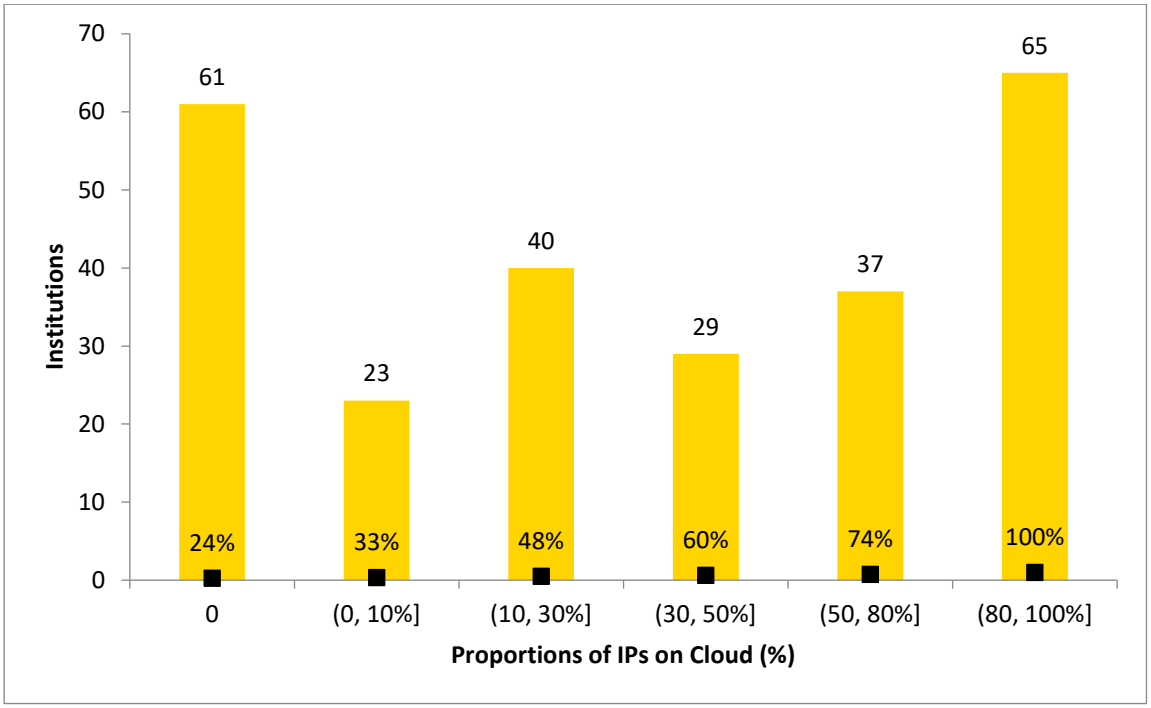

Figure 4: Cloud Asset Proportion

Figure 4 illustrates a definitive move towards embracing cloud services: a notable 26% of the surveyed institutions now entrust over 80% of their assets to cloud solutions. This transition to cloud-centric strategies highlights the sector's progressive shift in data management and security practices.

Conversely, a significant portion—24%—continues to operate with on-premises data center models, demonstrating the sector's diverse approaches to infrastructure deployment.

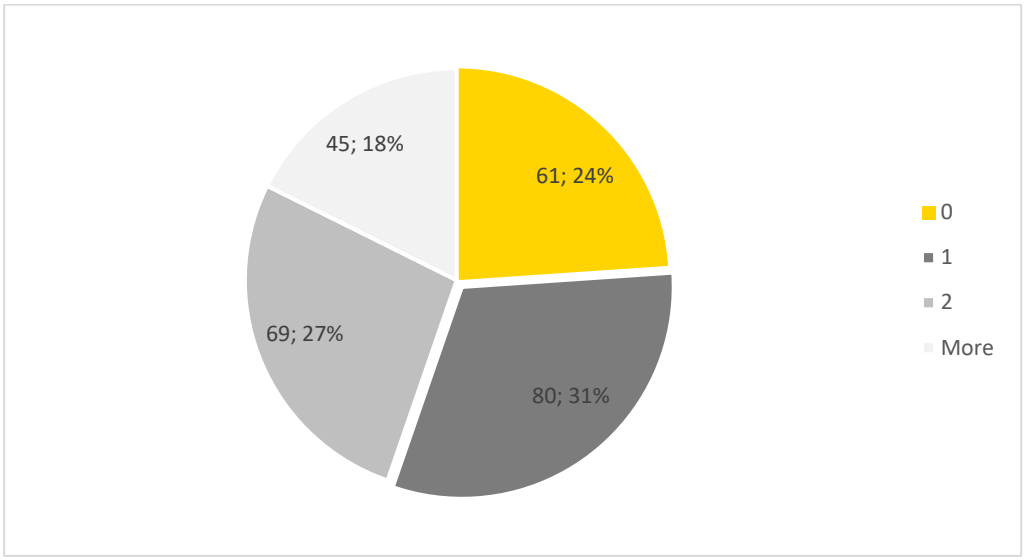

Figure 5: Number of Cloud Service Providers

Moreover, our analysis revealed that 45% of the institutions have embraced a multi-cloud strategy, as shown in Figure 5. Upon further examination, we discovered that this strategy spans the entire spectrum of healthcare providers, from the top-tier university hospitals to the smaller, specialized clinics, all taking advantage of services from multiple cloud providers. This widespread adoption underscores the industry's pursuit of greater operational flexibility and enhanced redundancy. However, this strategy also compounds the intricacy of risk management, introducing new challenges in orchestrating security across diverse cloud platforms and services.

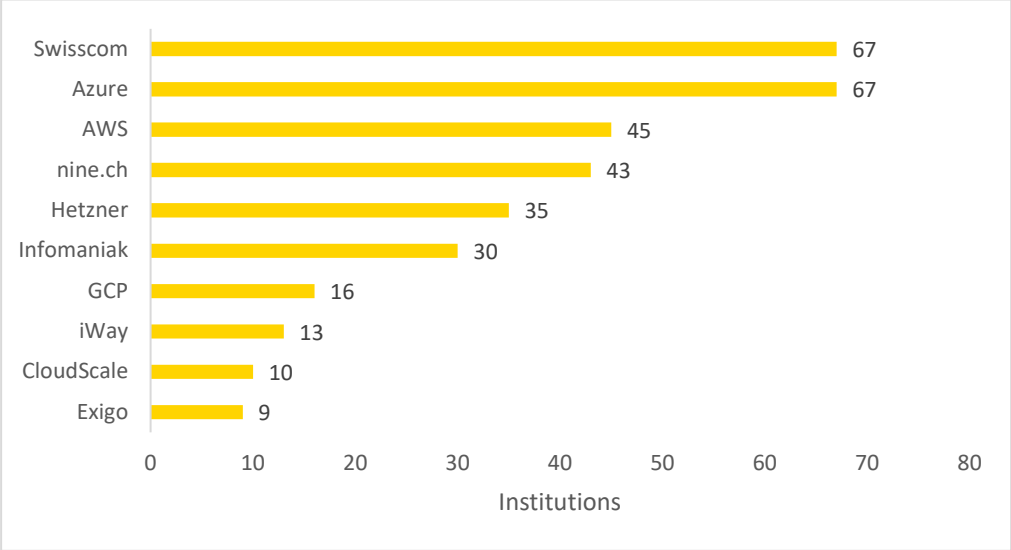

Figure 6: Top 10Cloud Service Providers

Delving deeper into the preferences among cloud service providers, Figure 6 highlights Swisscom as the leading local provider favoured by the surveyed institutions. Among the global cloud service providers, Azure emerges as the most utilized service, followed closely by AWS and then GCP. This preference pattern emphasizes the need for security assurance solutions in the Swiss healthcare sector to accommodate and seamlessly integrate with the services of all principal cloud providers.

4.4 Prioritized Assets

In order to facilitate prioritizing cyber risks by the external attack surface, C2SEC provides a metric “Asset Importance” to evaluates the criticality of each asset based on criteria such as its hostname, the technologies it employs, and the services it exposes, subsequently categorizing these assets into four levels of importance: Critical, High, Medium, and Low.

According to our analysis, reflected in Figure 7, of the total 12,930 hosts reviewed across the institution group, 17% are classified as critical. These critical assets are predominantly those involved in core operational functions, such as production systems and database management, necessitating heightened security measures.

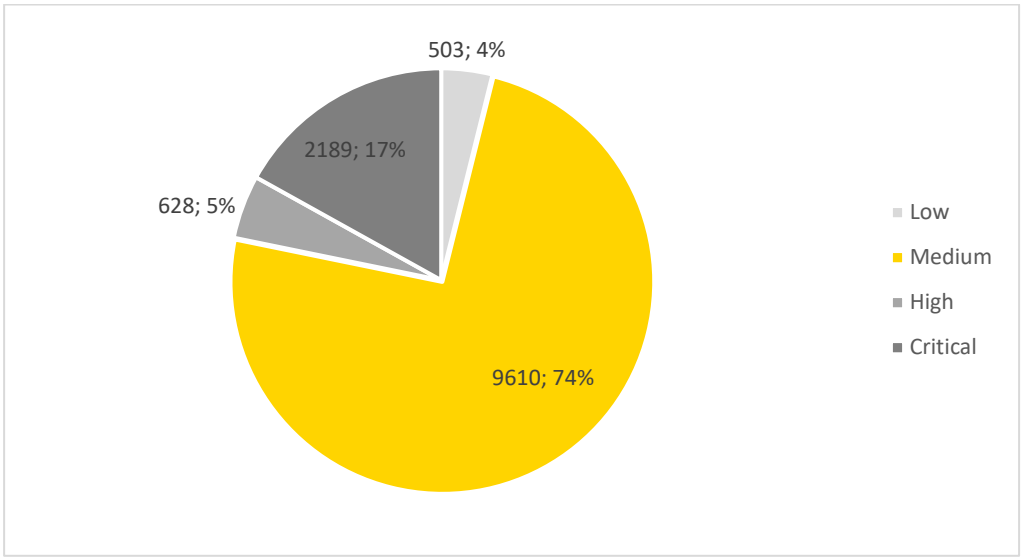

Figure 7: Asset Importance

4.4.1 Websites and Login Pages

A considerable segment of an institution's attack surface is comprised of its websites and associated applications, which are deemed significant assets. Our survey identified a range from 2 to 2,451 websites per institution, with a cumulative count of 7,142 websites exposed to the internet across all entities. Figure 8 illustrates that while the majority (59%) of institutions host fewer than 10 websites, there are 16 institutions with an extensive online presence, featuring over 50 websites.

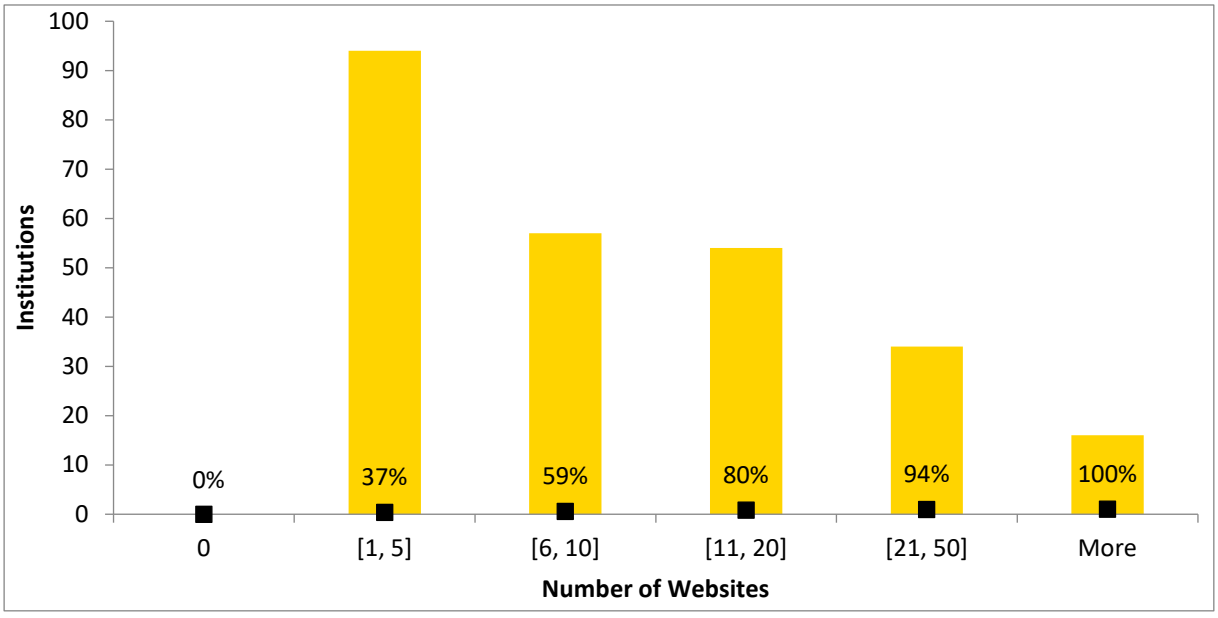

Figure 8: Website Count

Further scrutiny revealed 1,391 web pages specifically designed for user authentication, notably login pages where their hosting assets are deemed with critical importance. Figure 9 shows the histogram of Login page count for each institution. We observe that 29% of the institutions have no login pages exposed on the websites which implies that these organizations do not publish applications on their websites while 7% of the institutions have more than 10 login pages. The latter usually have dozens of websites published.

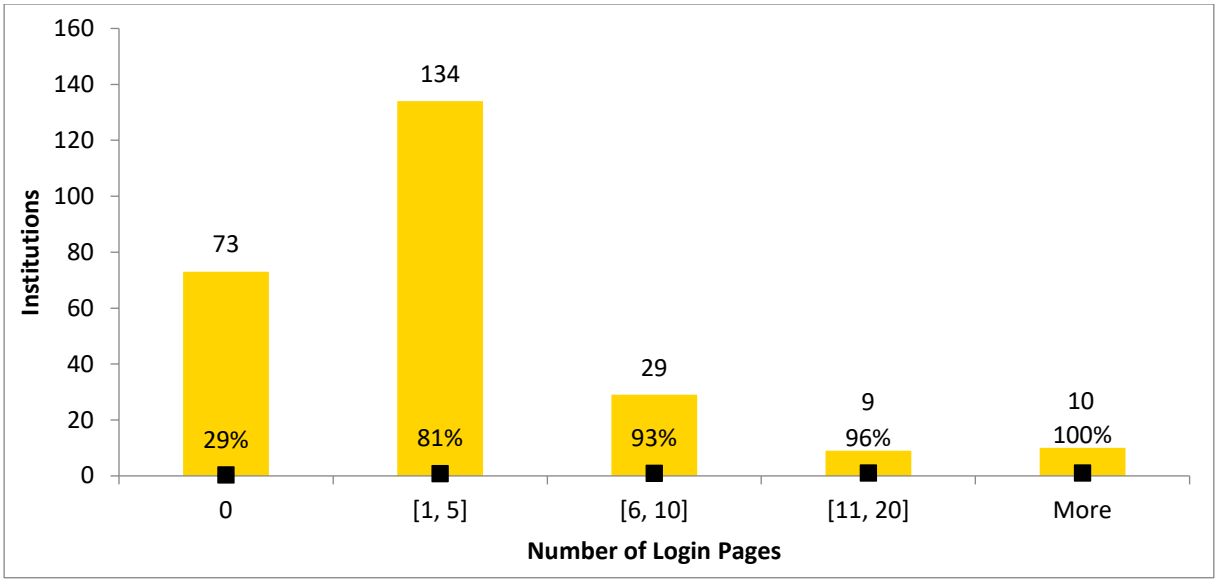

Figure 9: Login Page Count

These login pages are pivotal points within an institution's digital domain, serving as conduits to sensitive information and internal systems. Vulnerabilities in these pages, accessible through methods such as credential stuffing and phishing, make them prime targets for cyber incursions. Ensuring the security of these entry points is crucial for maintaining a robust cybersecurity posture and safeguarding against potential breaches.

4.4.2 Top web technology

An in-depth examination of web technologies utilized across these websites unearthed 393 distinct technologies, with the top 30 outlined in Figure 10. These popular technologies, while essential for building and maintaining modern websites and services, can also become vectors for cyberattacks if not properly secured or updated.

For instance, Apache and Nginx, two of the most widely used web servers, can be exploited through misconfigurations or unpatched vulnerabilities, allowing attackers to bypass security measures or execute malicious codes. Similarly, jQuery, a popular JavaScript library, can be leveraged by attackers if outdated versions containing known vulnerabilities are used, potentially leading to cross- site scripting (XSS) attacks.

Moreover, certificates issued by authorities like DigiCert are fundamental in establishing secure connections; however, if these certificates are improperly implemented or if attackers compromise them, the integrity and confidentiality of data in transit can be jeopardized. These examples underscore the importance of diligent management and updating of web technologies to protect against exploitation by cyber threats.

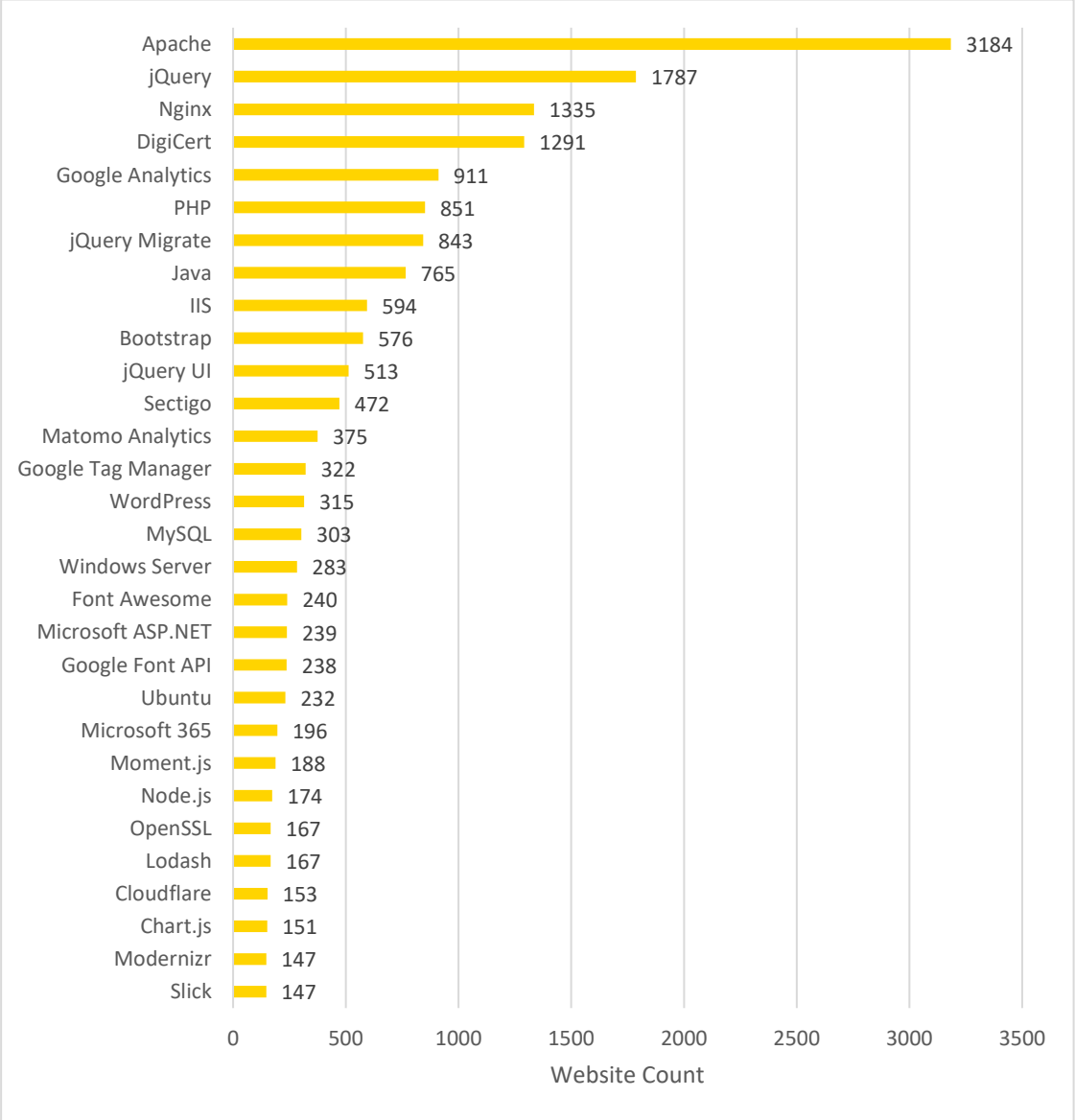

Figure 10: Top Web Technologies by Total Sites

5 __ Cybersecurity Gaps Analysis

5.1 Risk Index

The Risk Index (RI), as devised by C2SEC, serves as a dynamic metric to evaluate, and track the evolving security posture and associated cyber risks of an organization. This comprehensive index aggregates data across various dimensions of the attack surface, including the scale of assets, their geographical location, DNS configurations, email servers, presence of shadow IT, network integrity, IP reputation, encryption standards, patch management, and application security. Each of these components is assessed for its individual risk contribution, culminating in an overall RI for the organization calculated as a weighted average of these individual indices. The RI scale spans from 100 to 1000, with higher values indicating a proportionally increased level of cyber risk.

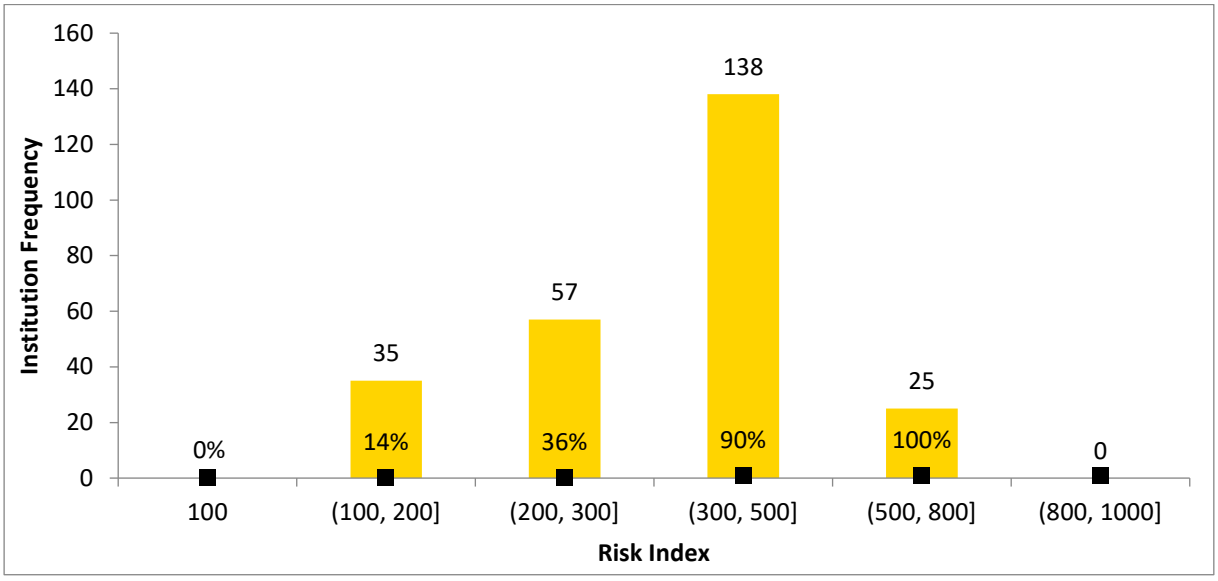

Figure 11: Risk Index

For the 255 healthcare institutions analyzed, RI scores ranged from 104 to 640. Detailed in Figure 11, our findings reveal that approximately 14% of these institutions demonstrate a robust security posture, with an RI of 200 or less, suggesting effective management of their cyber risk. Conversely, about 10% of the institutions exhibit significant vulnerabilities, reflected by RI scores above.

500. These entities, identified as having a heightened risk profile, necessitate urgent and focused cybersecurity interventions to mitigate potential threats and bolster their defences. We will take a closer look at two of them in the subsequent Section of Case Analysis.

A more granular analysis has unveiled that there is a correlation between the proportion of critical assets and the RI score as illustrated by Figure 12; specifically, a staggering 88% of those institutions with RI scores above 500 possess critical assets that account for more than half of their total assets. This insight draws a direct line between the criticality of an institution's digital assets and its susceptibility to cyber risk, emphasizing the need for a vigilant approach to cybersecurity in these high-risk environments.

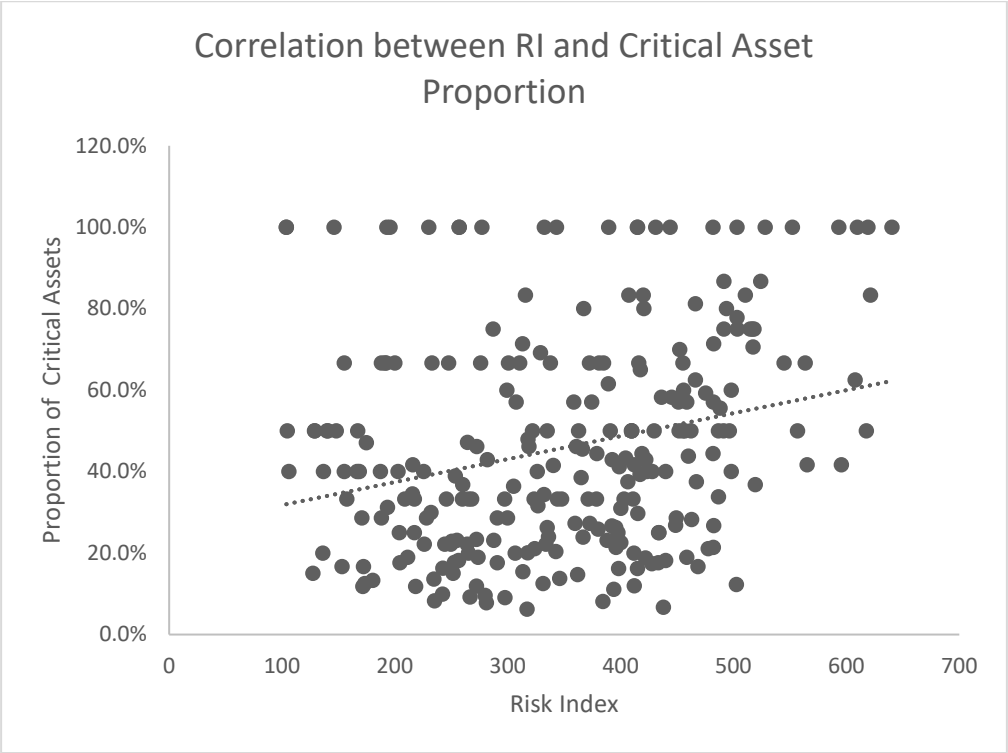

Figure 12: Correlation between Critical Assets Proportion and Risk Index

5.2 Security Issues

Cybersecurity issues identified from various risk components play a pivotal role in shaping an organization's attack surface and contribute to RI. These vulnerabilities serve as potential entry points for cyber attackers, directly influencing the magnitude and manageability of the attack surface. As such, the presence and severity of cybersecurity issues can significantly elevate the risk of unauthorized access, data breaches, and system compromises.

In total, C2SEC has unearthed 78,005 cybersecurity issues for the cohort of 255 health institutions, categorizing these issues according to their severity into Critical, High, Medium, and Low categories. The distribution of these issues by severity is illustrated in Figure 13, revealing a noteworthy finding: 13% of the identified issues are of high and critical severity. This subset of issues is particularly significant and warrants further investigation, as they represent the most immediate and potentially damaging threats to the cybersecurity posture of these healthcare institutions.

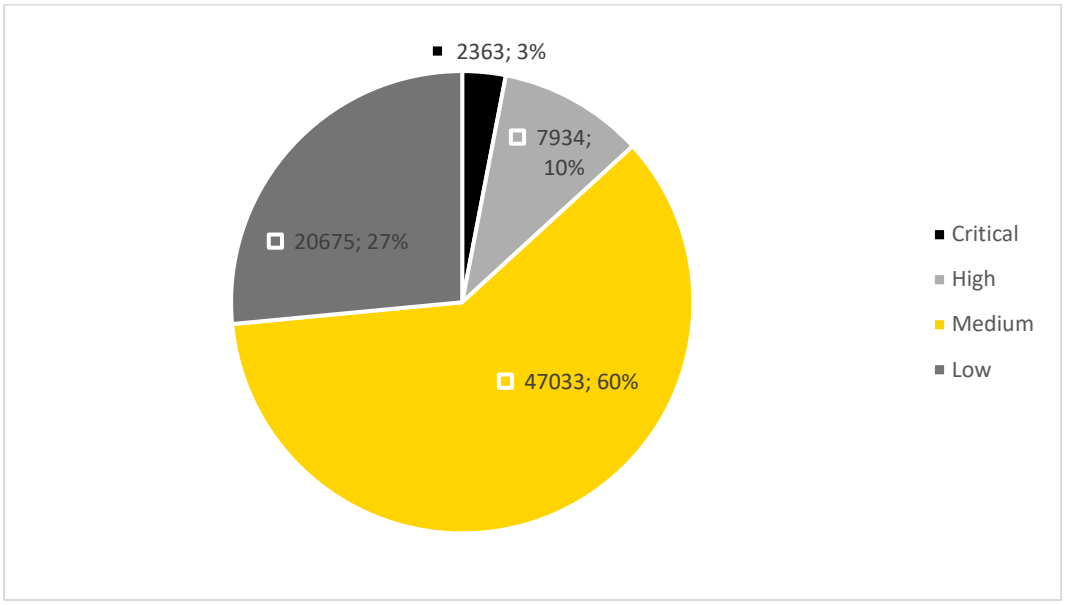

Figure 13: Issues by Severity

We then analyzed the number of issues with various severity for each institution. Specifically, the median number of critical issues per institution was identified as 3, whereas for high-severity issues, the median stood at 2. As depicted in Figure 14 through histograms, we observed that a significant majority, 86% (219 institutions), are grappling with critical issues, and 72% (184 institutions) are dealing with high-severity issues. It's noteworthy that for a large fraction of these institutions, the count of both critical and high-severity issues is less than 3. However, there are outliers in the data, with 3 institutions facing more than 50 critical issues and 9 institutions encountering over 50 high- severity issues, indicating areas of considerable concern within the cybersecurity management framework.

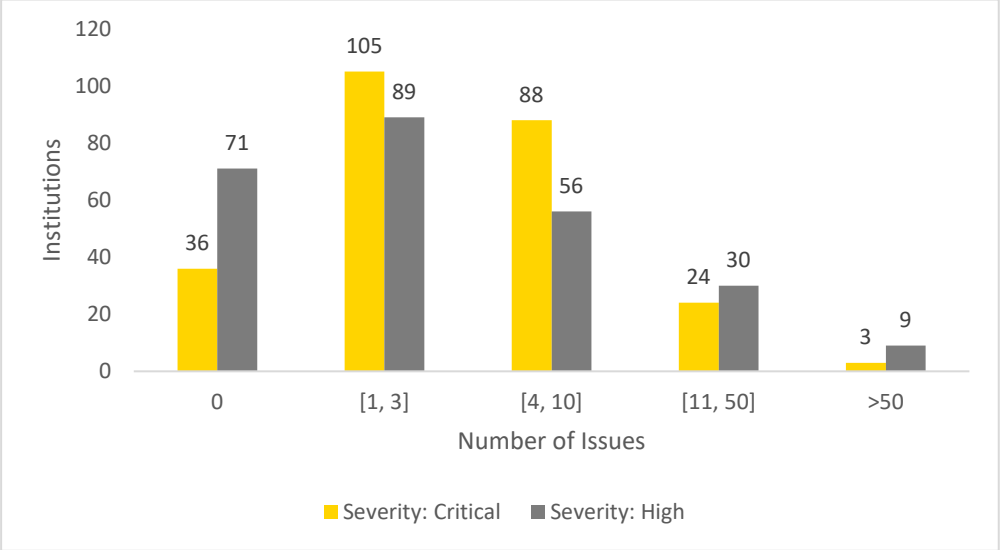

Figure 14: Login Page Count

Additionally, our analysis delved into the prevalence of critical issues across specific risk components of the external attack surface. Figure 15 highlights that the majority of institutions commonly face risks associated with network and application vulnerabilities, succeeded by concerns related to encryption practices and software patching deficiencies. This pattern underscores the critical areas where healthcare institutions are most vulnerable, pointing to network integrity and application security as primary focal points for immediate and effective risk mitigation efforts.

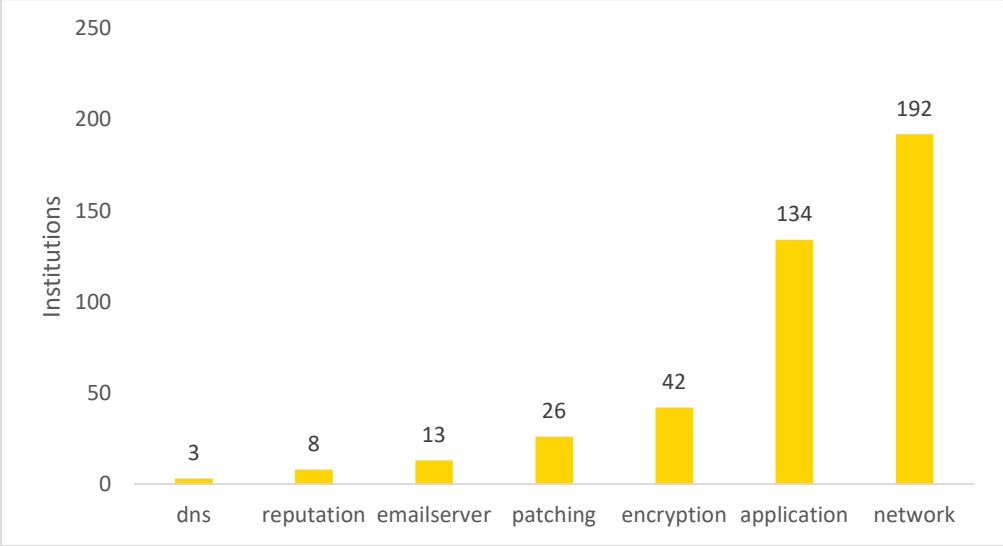

Figure 15: Number of Critical Issues of Components

Among the 315 unique critical issues pinpointed, Figure 16 delineates the top 10 critical vulnerabilities widespread across the institutions, notably highlighting the exposure of SSH services as the predominant issue. Such exposure paves the way for attackers to gain unauthorized entry into an institution's network, significantly compromising security. Moreover, the critical exposure of MariaDB emerges as another alarming vulnerability, threatening data integrity and necessitating robust protective measures. The list also includes exposures of crucial application panels, such as Typo3 (an open- source content management system) login page, VMware Horizon (a Virtual Desktop Infrastructure (VDI) product), and Drupal (an open-source content management system) login page, each presenting unique challenges to maintaining a secure digital environment. Two issues exposing web server configuration and development environment (PHP info) can also be invaluable to attackers. A further critical issue involves "Mismatched certificate names with login pages," an encryption problem that undermines the authenticity and security of communications, further complicating the institutions' efforts to protect sensitive data and maintain trust.

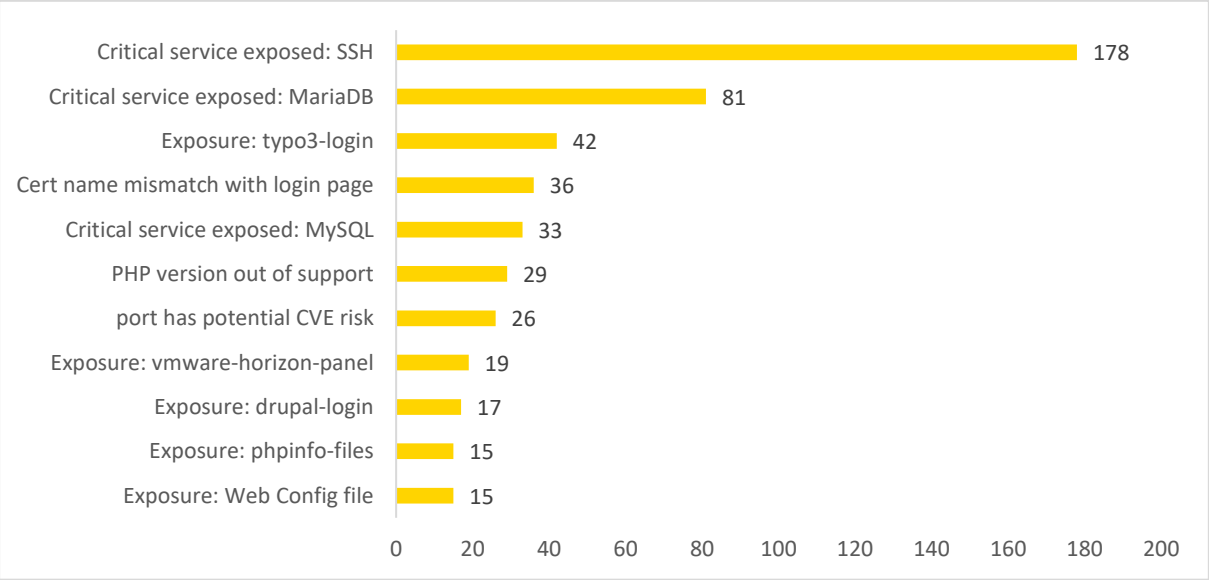

Figure 16: Top Critical Issues by Total Institutions

5.3 Network Ports and Services

Network misconfiguration remains a prevalent security vulnerability across various institutions, with exposed network ports and services posing significant risks. These vulnerabilities can be readily exploited by attackers to infiltrate a system or network. C2SEC's scanning efforts have uncovered 117 unique ports that host critical network services across 7,831 IP addresses. Table 1 showcases the top 10 most commonly open ports among these institutions. Notably, port 80 (HTTP) is universally exposed by all institutions, alongside port 443 (HTTPS) for secure web services, with only two exceptions lacking an open port 443. Other frequently encountered ports include 22 for SSH, providing secure access to remote servers, and 3306 for MySQL databases, in addition to various ports used for email services, primarily SMTP.

Port	Service	Institutions
80	HTTP	255
443	HTTPS	254
21	FTP	194
22	SSH	155
25	SMTP	147
3306	Mysql	105
8443	HTTPS	96
587	SMTP	91
465	SMTPs	86

Table 1: Top 10 Open Ports

5.4 Vulnerabilities

Software vulnerabilities, particularly those arising from patching issues, pose a substantial threat within the realm of attack surface management. These vulnerabilities are often cataloged as Common Vulnerabilities and Exposures (CVEs), a list of publicly disclosed computer security flaws. When organizations fail to apply patches to known vulnerabilities promptly, they leave open doors for attackers to exploit. These security gaps can be weaponized to gain unauthorized access, disrupt services, or steal sensitive data, making timely patch management a crucial aspect of maintaining a reduced attack surface.

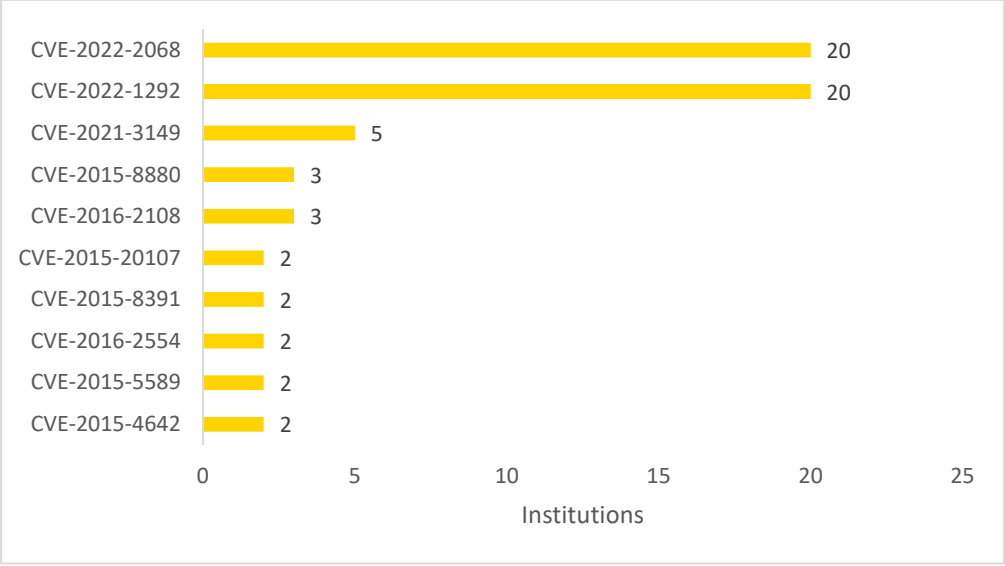

Figure 17: Top 10 Critical CVEs by Total Institutions

C2SEC's analysis of Swiss healthcare institutions has surfaced the total 50,750 patching issues which involve 1,270 distinct CVEs that remain unpatched, underscoring the challenges in patch management practices. Among these, 44 CVEs are identified as critical, each with a Common Vulnerability Scoring System (CVSS) score exceeding 9, with some even reaching the maximum severity rating of 10. As detailed in Figure 17, the top 10 most critical CVEs, such as CVE-2021-3149, CVE-2022-1292, and CVE-2022-2068, underscore recent security issues primarily within OpenSSL that could be exploited to remotely disrupt services. The remaining high-risk CVEs largely pertain to PHP vulnerabilities that can be manipulated for unauthorized privilege elevation and circumvention of security measures. Addressing these vulnerabilities is not just about applying patches; it's about understanding the potential impact, prioritizing remediation efforts, and consistently monitoring for emerging threats.

6 __ Case Analysis

In light of our comprehensive security posture assessment of Swiss healthcare institutions, we selected two exemplar cases for an in-depth analysis of their respective attack surfaces.

5.1 Institution with the Largest Asset Scale

The first case focuses on a leading university hospital in Switzerland, which boasts a significant number of digital assets. This institution does not have a standalone root domain; instead, it shares its digital infrastructure with the associated university. Leveraging the C2SEC platform, we executed a detailed scan of the university's primary root domain, uncovering a vast digital presence encompassing 4,133 IP addresses and 6,529 subdomains that extend beyond Europe, reaching into the United States (as shown in Figure 18). This complexity demonstrates the nuanced challenge of cybersecurity management when healthcare operations are integrated with larger educational institutions, highlighting the need for a synergistic cybersecurity strategy between the hospital and the university to forge a fortified defense against cyber threats.

Figure 18: Geo Locations

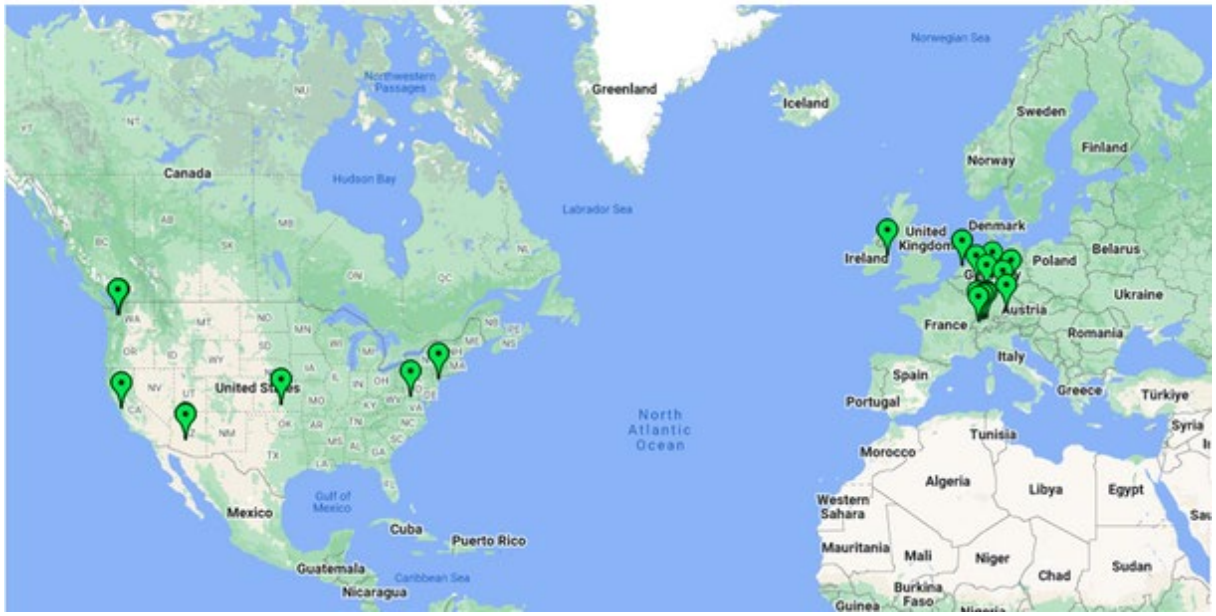

Figure 18: Asset GEO Locations

The expansive scale of the asset inventory and its geographical spread present substantial challenges in managing cybersecurity effectively. Overall, the institution has an RI value of 384 and about 8% of its assets are of critical importance. The posture matrix in Figure 19 illustrates the distribution of issue severity across varying levels of asset importance. Out of 40,092 identified issues, 412 that reside on critical assets demand urgent attention.

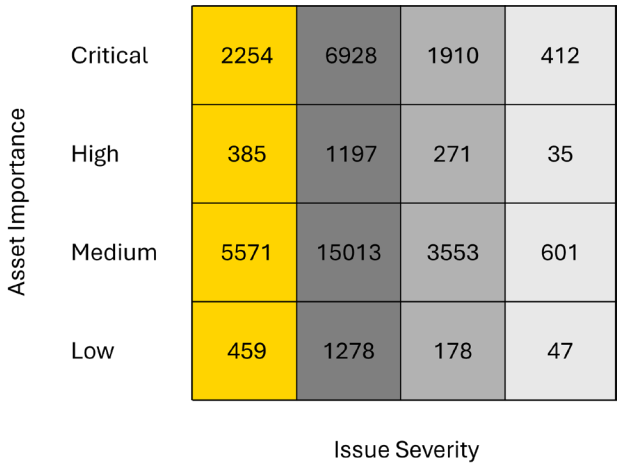

Figure 19: Security Posture Matrix of the Large Institution

In addition to the vulnerabilities associated with exposed network services like SSH and MySQL and common patching issues, we identified a significant number of issues (exceeding 50) related to exposed application control panels. These control panels, which include login pages, should typically be restricted to internal privileged users. Figure 20 highlights several examples of these vulnerabilities discovered within the organization's assets.

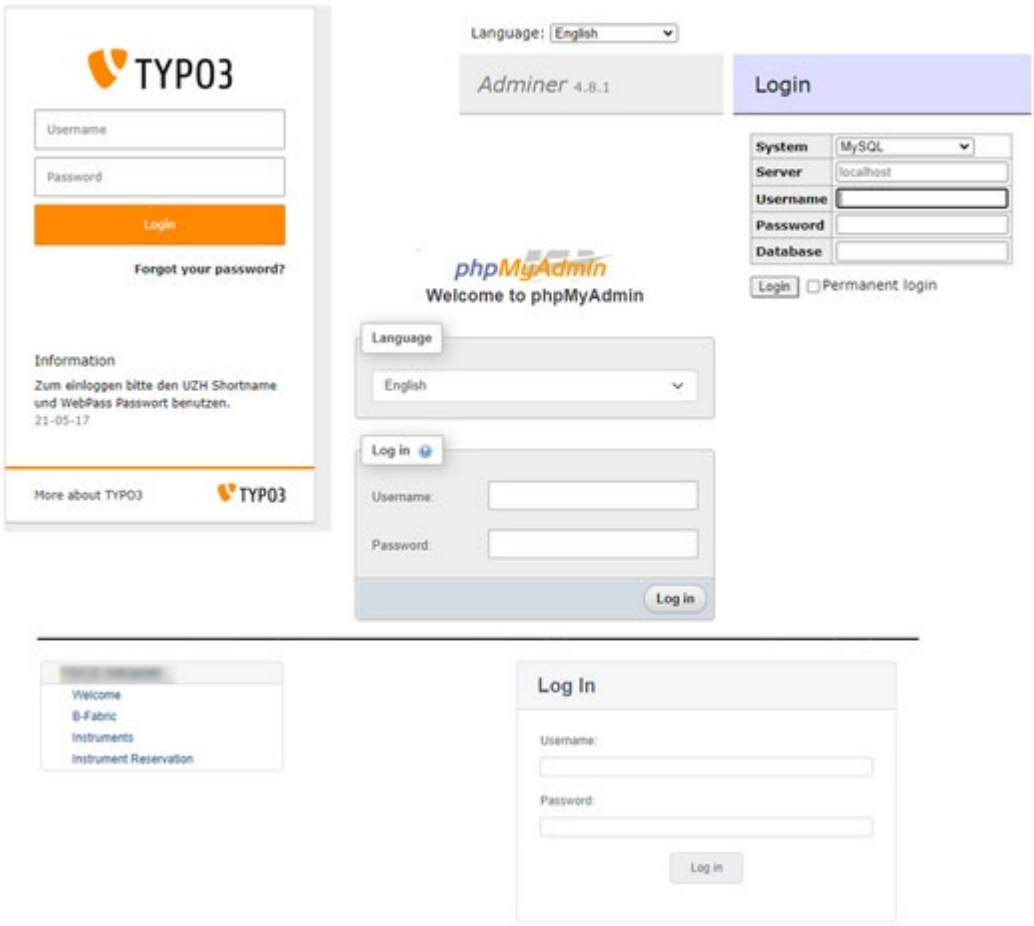

Figure 20: Examples of Exposed Control Panels

With the critical posture above, immediate action is required to enforce stringent access controls and employ robust encryption for application control panels to prevent unauthorized internal access. It's also recommended to implement a comprehensive vulnerability management program that includes regular scans, prompt patch management, and employee awareness training to mitigate the risk of exploitation.

5.2 Institution with Light Assets but Many Critical Issues

The second case study examines a mid-sized general hospital with a considerably lighter asset footprint—comprising merely 16 IPs and 60 subdomains—yet it's confronted with a disproportionately large number of critical security issues. Despite its smaller scale, it ranks high in vulnerability counts compared to other surveyed institutions.

In contrast to the first case, this hospital's Risk Index (RI) is alarmingly high at 565, coupled with a critical asset ratio of 41%. As depicted in Figure 21, this hospital must urgently remediate 72 critical security issues. Of these, while a handful relate to network and application vulnerabilities, the majority— exceeding 50—are associated with outdated components requiring patching. Specifically, these issues are linked to the use of an out-of-date OpenSSL version (1.1.1g from September 2018), all hosted on a single IP address. Given that OpenSSL is crucial

for secure network communications, neglecting to update this library exposes the hospital to severe cybersecurity threats.

Figure 21: Security Posture Matrix of the Mid-Size Institution

To enhance the hospital's security posture, a focused approach is needed. A targeted patch management strategy should be the first order of business, starting with an immediate upgrade of the outdated OpenSSL version to mitigate known vulnerabilities. Beyond patching, regular and automated vulnerability assessments should be implemented to ensure all software components are up to date.

7 __ Recommendations

The analysis conducted presents a compelling case for Swiss healthcare institutions to take immediate and specific actions to enhance their security postures. Aligned with the Swiss NCSC recommendations [4], below are actionable recommendations from this study:

1. Asset, Patch and Access Management

Asset Management: Develop a comprehensive inventory of digital assets and evaluate their importance to business operations, applying stringent security measures to the most critical ones.

Prioritize Patch Management: Institutions must establish a regimented patch management process, ensuring that all systems are kept up to date with the latest security patches.

Access Controls for Critical Control Panels: Enhance security for control panels and login pages by employing multi-factor authentication, strong password policies, and access restrictions based on roles.

2. Network Service, Web Application Security

Network Service: For critical services like SSH and MySQL that are exposed to the internet, it is critical to implement network-level security controls such as VPNs and firewalls, to secure these services.

Critical Web Application: Implement periodic automatic penetration testing to proactively identify and mitigate web application vulnerabilities.

3. Continuous Assessment

Perform continuous security evaluations to discover new vulnerabilities, focusing on high-risk areas such as exposed network ports and login interfaces.

4. 0day and N-day Exploitation Response

Develop, maintain, and periodically test a response plan to swiftly manage and mitigate the impacts of 0day and N-day attacks.

By following these recommendations, Swiss healthcare institutions can significantly reduce their attack surfaces and build a more secure infrastructure capable of repelling the increasingly sophisticated cyber threats they face.

8 __ Conclusion

Our study unveils a wide and complex attack surface across Swiss healthcare institutions, highlighting significant disparities in asset inventories, the severity and types of cybersecurity issues they face. These findings spotlight the substantial gaps that healthcare institutions must bridge to meet NCSC's guidelines effectively. The challenges are particularly acute in areas such as asset management, patch management, and securing access to control panels and login entries. Moreover, these challenges are intensified by the sector's rapid shift towards cloud environments.

This situation underscores the critical need for a systematic approach that includes automated asset discovery and management, comprehensive security posture assessments, prioritized risk mitigation, and continuous monitoring. For the healthcare sector to improve its security posture, adopting such proactive and dynamic approaches is not just an option—it is an imperative for safeguarding patient data and maintaining trust in the digital age.

Moving forward, it's crucial to understand that managing the external attack surface is just the beginning of comprehensive security posture management. As healthcare institutions continue to shift their infrastructures towards cloud and SaaS services, an extensive approach becomes imperative. This expansion should include in-depth penetration testing, cloud security posture management, SaaS security management, and thorough supply chain risk management. The C2SEC platform is specifically designed to help health institutions enhance their operational security and ensure compliance with relevant regulations, providing robust support as they navigate the complexities of digital transformation.

9 __ About UMB

Time is one of the most valuable resources in the world. And complexity eats up time. UMB wants to free up this time by making life easier. Under the motto "The Art of Creating Time", the IT service provider UMB AG, which is part of the BKW Group, gives its customers time for bold ideas and innovations in order to keep prosperity, health, development and the environment in balance.

With "Leading Edge" competencies in the areas of Business Advisory, AI & Data, Network, Platform Building, Security, Cloud, New Work, Communication and SAP, UMB has the experts for the digitalisation of its customers' business processes. The company has already received several awards as the best employer.

Established in 1978, UMB today has over 900 employees, 42 of whom are apprentices.

UMB AG
Hinterbergstrasse 19
6330 Cham

Tel: +41 58 510 10 10
info@umb.ch
www.umb.ch

10 __ About C2SEC

C2SEC is a global cybersecurity technology provider with clients in North America, Europe and APAC. Our clients include financial institutions, high-tech companies, insurances, industry conglomerates, health institutions, etc.

For healthcare institutions committed to safeguarding their digital future, C2SEC offers the comprehensive solution needed to understand, manage, and mitigate cybersecurity risks effectively. Contact us today to explore how C2SEC can transform your institution's approach to cybersecurity, ensuring a secure and compliant digital healthcare environment. For more information, please visit https://www.c2sec.com or contact

C2SEC S.A.
Rue de Lausanne 44 Genève
1201 Switzerland

Renato Martignoni renato@c2sec.com
+41 79 214 77 19

11 __ References

1. The Technology Lifeline: Charting Digital Progress in Healthchare. SOTI, 2023.
2. European Commission. (2016). General Data Protection Regulation (GDPR). https://ec.europa.eu/info/law/law-topic/data-protection_en
3. "Federal Act on Data Protection (FADP)." Available at: https://www.fedlex.admin.ch/eli/cc/2022/491/en
4. Recommendations on cybersecurity in the healthcare sector. NCSC, 2022
5. https://healthitsecurity.com/news/healthcare-data-breaches-are-piling-up- 3-months-into-the-year
6. https://cybernews.com/security/irish-health-service-executive-data-leak
7. Swiss hospitals and clinics. https://quel-hopital.ch/suisse/

12 __ Disclaimer & Copyright

Disclaimer

The information in this report is for reference only. While C2SEC INC/SA endeavors to ensure the accuracy of the information, no express or implied warranty is given by C2SEC INC/SA as to the accuracy of the information. Users are encouraged to conduct their own enquiries to verify any particular piece of information provided in this report. C2SEC INC/SA shall not be liable for any loss or damage suffered as a result of any use or reliance on any of the information provided in this report.

Copyright

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.