REWIRE
Cybersecurity Skills Alliance

Co-funded by the
Erasmus+ Programme
of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R5.2.1 Third Annual Cybersecurity Skills Trends Report

Title	R5.2.1 Annual Cybersecurity Skills Trends Reports
Document description	3rd Annual Cybersecurity Skills Trends Report within R5.2.1
Nature	Public
Task	T5.2.1 Annual Cybersecurity Skills Trends Reports
Status	Final version
WP	WP5
Lead Partner	MRU
Partners Involved	All
Date	13/11/2024

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
ACSC	Australian Cyber Security Centre
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENISA	The European Union Agency for Cybersecurity
EU	The European Union
ECSF	European Cyber Security Framework
GDPR	General Data Protection Regulation
IoT	Internet of Things
MITM	Man-in-the-Middle
NCSC	National Cyber Security Centre (New Zealand)
PhaaS	Phishing-as-a-Service
RaaS	Ransomware as a Service
RDoS	Ransom Denial of Service
RFID	Radio-frequency identification

Table 1. List of abbreviations and acronyms

LIST OF TABLES

LIST OF FIGURES

REWIRE
Annual Cybersecurity Skills Trends Report

SUMMARY

The Third Annual Cybersecurity Skills Trends Report provides a comprehensive analysis of the cybersecurity skills landscape in the EU. The report serves as a critical resource for stakeholders, offering key insights into the growing cybersecurity skills gap and the evolving market demands. One of the central tools highlighted is the Cybersecurity Job Ads Analyzer, which uses machine learning to map essential competencies and align them with the ENISA framework, helping track high-demand profiles like Cybersecurity Architect and Cyber Incident Responder. The CyberABILITY platform further supports the sector by acting as a hub for skills, training programs, and certifications, aiding recruitment and career planning while contributing to standardizing roles across Europe.

The REWIRE stakeholder survey conducted in 2024 revealed the high demand for roles such as Chief Information Security Officers and Cybersecurity Architects, with crucial skills in business continuity, data privacy, and incident management. Despite a shortage of certified professionals, organizations invest in employee training, emphasizing the importance of certifications and cyber ranges.

The report also provides a detailed mapping of skills needed to address Operational Technology (OT), Information Technology (IT) threats and Shared-IT threats. With the rise of IoT integration, risks to OT systems have increased, necessitating skills in cyber threat intelligence and vulnerability assessments. IT threats, such as blockchain vulnerabilities and supply chain attacks, underscore the importance of securing network communications and ethical hacking. Over 75% of IT threats and over 80% of Shared-IT threats, like cloud misconfigurations, are covered by the REWIRE and ENISA skill frameworks, though areas like IoT security and AI-driven social engineering require further refinement.

Overall, the report emphasizes the need for continuous refinement of cybersecurity skill frameworks, strategic workforce development, and adaptive education to address the constantly evolving threat landscape. It calls for collaborative efforts across sectors to ensure the cybersecurity workforce is prepared for future challenges.

1. INTRODUCTION

In an environment where cybersecurity dynamics are constantly changing, a structured approach to tracking and analyzing trends is crucial. The 3rd Annual Cybersecurity Skills Trends Report, crafted by the Erasmus+ REWIRE project, represents a concerted effort to gather data on the shifting landscape of cybersecurity competencies systematically. The aim is to identify and anticipate future needs in the cybersecurity skill sector, laying a foundation for developing subsequent project deliverables.

The structure of the Report is organized into several sections:

Section 2 outlines REWIRE's methodology for tracking and analyzing trends in cybersecurity skills. This methodological framework is critical for ensuring that the data collected is robust and that the analysis is grounded in a repeatable, scientific approach.

Section 3 presents the results of the Stakeholder survey. It provides a perspective into what skills and professionals different businesses are currently in need of and looking for.

Section 4 offers an in-depth examination of the current demand landscape for cybersecurity skills. It meticulously articulates the findings and insights gleaned from the Cybersecurity Job Ads Analyzer and the CyberABILITY platform, both of which are instrumental in pinpointing existing skills gaps and assessing the state of cybersecurity competencies across the industry.

Section 5 analyzes cybersecurity threat trends. By understanding the trajectory of threats, one can infer the direction in which cybersecurity skills need to evolve to counteract these threats effectively.

Finally, Section 6 encapsulates the essence of the report by merging the identified cybersecurity threats with the requisite skills necessary for their mitigation. This synthesis informs curriculum development, training programs, and policy-making. It ensures that educational institutions, training providers, and policymakers are in lockstep with the practical needs of the cybersecurity realm, equipping professionals with the tools and knowledge to safeguard digital assets in an increasingly complex and vulnerable cyber landscape.

This report builds on the foundation from the initial report delivered in October 2022 and the second report delivered in 2023. By maintaining a pulse on the sector's progression, the REWIRE project ensures that its outputs remain relevant and stakeholders are equipped with the knowledge to make informed decisions in the rapidly evolving cybersecurity domain.

2. METHODOLOGY

The project team used diverse information sources to construct this report. Table 2 lists the information sources used or planned to be used in the future to support the creation of this report and its iterations.

Information source	Description	Status and Periodicity
Stakeholders' survey	The Survey was conducted to collect information about unfilled cybersecurity job positions, the most sought-after skills and the ability of education providers to train the needed professionals	The first results in 2021 – are reported in R2.2.2. Cybersecurity Skills Needs Analysis and in 1st Annual Cybersecurity Skills Trends Report within R5.2.1 Repeated every two years
Job Ads Analysis	This tool created by REWIRE team allows identifying which cybersecurity skills are required within an ad and creates appropriate mappings to the relevant cybersecurity roles	Implemented. First results in 2022. Repeated annually.
National, regional, European and industry risk and threat reports	Cybersecurity risk and threats reports of various actors (e.g., ENISA), governmental reports (UK, New Zealand, Australia, etc.) and similar are reviewed to provide insights on cybersecurity skills.	Implemented. Repeated annually.
Sectoral surveys and studies	Sectoral surveys and studies from various organizations (e.g., CrowdStrike, Sophos, Truesec, etc.) are reviewed in order to provide further insights on the subjects of cybersecurity skills	Implemented. Repeated annually.
The CyberABILITY platform	The CyberABILITY platform combines and presents information to interested parties on the 12 roles of the ECSF, professional courses, academic degrees, and certifications.	Implemented.

Table 2. Cybersecurity Skills Trend Report information sources

The initial methodological approach included two steps. First, a Stakeholders' survey was conducted to identify the most coveted skills and the capacity of educational institutions to educate the required professionals. Second, the results of Job Ads Analysis enabled the

recognition of certain skills necessitated in respective ads and established corresponding links to the pertinent roles in cybersecurity. A REWIRE stakeholder survey was conducted for this report, which aimed to identify key cybersecurity skills, assess educational preparedness, and explore cybersecurity training methods. Combined with secondary sources, these insights enrich the analysis, mapping emerging cybersecurity needs to training programs. This data-driven approach ensures the methodology aligns with current cybersecurity trends and addresses European workforce and educational gaps.

To complement the initial methodology, the CyberABILITY platform is introduced as a critical resource for addressing skill gaps in the cybersecurity sector. This platform uses tools like the Cybersecurity Jobs Analyzer to identify in-demand skills from job ads and the Cybersecurity Profiler to map training programs to specific roles, aligning with the European Cybersecurity Skills Framework (ECSF). These tools enhance the analysis of emerging cybersecurity threats by identifying the necessary skills and linking them to relevant educational and certification programs, ensuring a structured response to workforce needs.

This report compares sectoral surveys and studies and national threat trends reports to identify the latest cybersecurity threats that emerged over the last year. It then allows the analysis of the skills required to tackle emerging threats. For each skills trend report, the information derived from all these sources and any news identified then will be combined to produce relevant insights.

3. RESULTS OF REWIRE STAKEHOLDERS SURVEY

The REWIRE team developed the survey in July 2024 to gain comprehensive insights into the current demand for cybersecurity competencies and skills. The primary objectives were to identify crucial cybersecurity roles, determine the relevant skills associated with these roles, and evaluate how well higher and vocational education institutions prepare future professionals. The survey also aimed to explore effective methods for developing these competencies and assess which technologies best support these educational approaches.

Responses were collected from professionals across multiple sectors, including government institutions, higher education and research organizations, small and medium enterprises, cybersecurity companies, vocational education providers, non-governmental organizations, and large corporations. The survey notably included participants from Lithuania, Cyprus, the Czech Republic, Greece, and Serbia, along with other European countries such as Italy, Spain, Austria, Belgium, Latvia, Portugal, France, Finland, and Estonia.

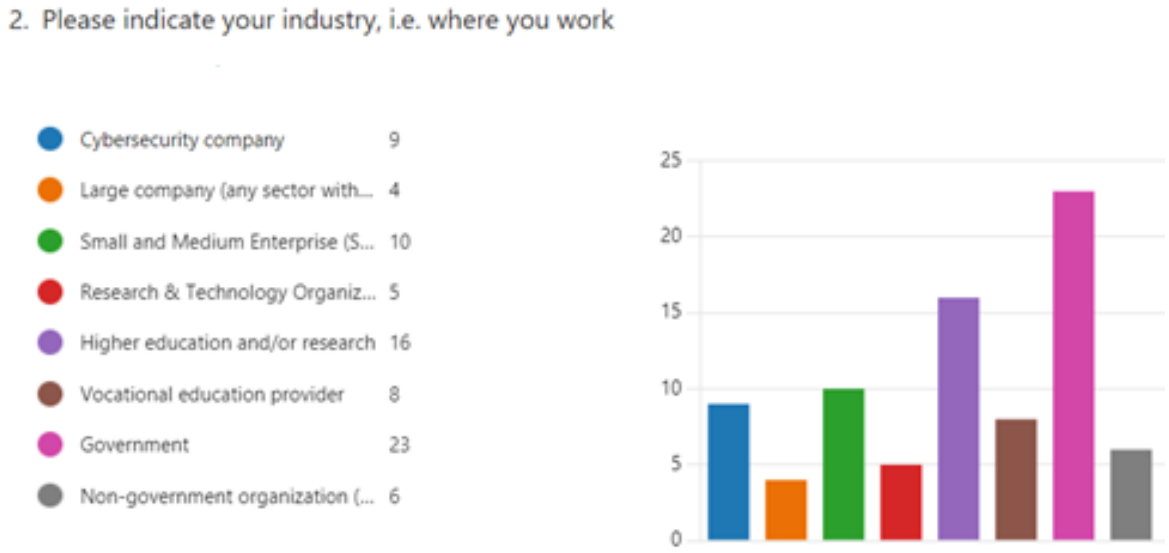


Figure 1. Distribution of respondents according to occupation

For example, the participants were asked to respond on the relevance of cyber ranges and other education platforms, cybersecurity sertifications, level of shortage of cybersecurity professionals, likeliness of investing in current employees, likeliness of outsourcing cybersecurity professionals, or alternatively, hiring (training) them in-house. The respondents were requested to identify the otganisation-level and country-level need of the specific ECSF roles which they consider relevant, provide their evaluation of the degree of need for additional cybersecurity professionals with the competencies in their countries and rate the level of impact of different factors on cybersecurity education on the national and European level.

The data reveals a significant consensus on the value of cyber ranges, with most respondents considering them highly relevant for cybersecurity training. This positive perception extends to cybersecurity certifications and related training programs, essential for validating and

standardizing industry knowledge. However, a pronounced concern about the shortage of certified professionals highlights a critical gap in the cybersecurity workforce. This concern is met with a strong commitment from organizations to invest in training their existing employees over the next two years, reflecting a proactive strategy to address the shortage of certified experts.

Opinions on outsourcing cybersecurity functions are varied. While there is a preference for in-house solutions, many organizations are also open to utilizing managed services. This mixed sentiment is balanced by a clear inclination toward hiring skilled cybersecurity professionals rather than developing new talent from scratch. Chief Information Security Officers and Cybersecurity Architects are consistently identified as high-demand roles. Cyber Incident Responders and Digital Forensics Investigators also show considerable demand across various regions. In contrast, roles such as Cyber Legal, Policy & Compliance Officers, and Cybersecurity Implementers display more inconsistent demand, varying significantly depending on the region.

The survey highlights a consistently high demand for expertise in business continuity, data privacy, data security, and digital forensics. These competencies are vital for maintaining organizational resilience and safeguarding sensitive information. Similarly, Incident Management, Information Systems, and Network Security are crucial, reflecting the need for effective response strategies and robust protection against cyber threats. Risk management and testing and evaluation are also highly sought after, emphasizing the need for professionals skilled in identifying and mitigating risks and performing security assessments.

In contrast, the demand for competencies such as law, policy, ethics, physical device security, and data analysis varies more widely across regions. This variability suggests that while certain areas, like business continuity and data protection, are universally critical, other competencies may be more context-dependent, varying according to regional and organizational priorities. The results indicate a strong and consistent need for skills addressing immediate and strategic cybersecurity challenges while reflecting diverse requirements across different locations and sectors.

Several factors impact cybersecurity education across Europe. The lack of coordinated efforts at the EU level is highly rated, indicating that fragmented and inconsistent policies across member states hinder the development of effective cybersecurity education frameworks. The economic impact of inadequate cybersecurity capabilities and awareness is also significant, reflecting insufficient preparedness's financial and operational challenges. Additionally, the need for improved social awareness and dedicated curricula and training is noted as having a high impact, emphasizing the importance of increasing public awareness and developing well-defined educational pathways. The COVID-19 pandemic's impact is rated as medium, suggesting it has influenced cybersecurity education but not as dramatically as other factors. Issues like gender imbalance in cybersecurity are viewed as having a lower impact but remain a relevant concern for diversity and inclusivity within the cybersecurity workforce.

The survey results indicate that while overall satisfaction with cybersecurity education is generally positive, there is room for improvement. Some regions are reported as having well-developed frameworks, while others show notable gaps. Key recommendations for enhancing cybersecurity education include increasing the number of study programs at both Bachelor's

and master's levels, offering tailored training programs for IT professionals, expanding the number of training providers and platforms dedicated to cybersecurity, and fostering collaboration within the EU. Specific certifications as part of educational and training programs are also recommended to ensure professionals meet recognized standards. These improvements aim to address existing gaps and elevate the overall quality of cybersecurity education across Europe.

At the national level, priorities for cybersecurity domains vary significantly. Business Continuity, Data Privacy, Data Security, Incident Management, and Information Systems and Network Security are consistently recognized as high priorities. Other domains, such as Data Analysis, Digital Forensics, and Intelligence Analysis, are also important but often receive medium priority ratings, indicating a balanced focus. Conversely, areas like Identity Management and Testing and Evaluation are given lower priority, reflecting a relative lack of emphasis or development.

4. STATUS OF CYBERSECURITY SKILLS AND SYSTEMATIC SKILL GAP

The Cybersecurity Job Ads Analyzer and the CyberABILITY platform are both vital in tackling the systematic skills gap in the cybersecurity sector. The Job Ads Analyzer leverages machine learning to evaluate job advertisements across Europe, providing a clear view of essential skills and competencies in demand and aligning them with the ENISA framework. This helps stakeholders identify and monitor the changing needs for roles like Cybersecurity Architect and Cyber Incident Responder. Complementing this, the CyberABILITY platform serves as a comprehensive observatory, mapping job market trends, training programs, and certifications while aligning educational offerings with industry requirements through tools such as the Cybersecurity Profiler and ECSF Explorer. Together, these platforms empower professionals, organizations, and educational institutions to bridge the skills gap effectively, ensuring that the workforce evolves in line with market needs and standards. Both are discussed in retail further.

4.1. JOB ADS ANALYSIS

In the third annual report, the REWIRE partners embark on the following approach to elucidate the landscape of the cybersecurity skills shortage, mainly the **Development of the Cybersecurity Job Ads Analyzer**[1]. This innovative application is designed to aggregate and examine job adverts. It incorporates a machine learning algorithm, which is instrumental in pinpointing and delineating the specific competencies sought in an advertised open cybersecurity job market. The analysers' sophisticated capabilities enable a granular analysis of the evolving demands of cybersecurity skills, thus providing invaluable insights into the current skills ecosystem. The insights developed via Job Ads Analysis are integrated within the CyberABILITY[2] platform, presenting the fuller picture of the skills required to respond to certain threats.

The Job Analyzer app integrates the ECSF key skills and knowledge describing the profiles by mapping them to the identified 31 REWIRE skills. Specifically, after analyzing the ENISA framework, we realized that the listed key skills and knowledge describing the profiles are uniquely phrased. This does not allow for depicting the relationships among the profiles through the connections of the same skills and knowledge. A way to overcome this issue is to group the knowledge and skills that represent the same concept but are phrased differently. Moreover, these lists require technical knowledge to be understood and can be demanding to be managed by non-experts in the sector. We refer to EWIRE Report R3.4.1[3] for more details.

[1] Ricci S, Sikora M, Parker S, Lendak I, Danidou Y, Chatzopoulou A, Badonnel R, Alksnys D. Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation. InProceedings of the 17th International Conference on Availability, Reliability and Security 2022 Aug 23 (pp. 1-10).
[2] https://rewireproject.eu/cyberability/
[3] REWIRE Consortium, "REWIRE Deliverable R3.4.1 - Mapping the framework to existing courses and schemes." Nov. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/11/REWIRE_R3.4.1_Deliverable-v7-Final.pdf

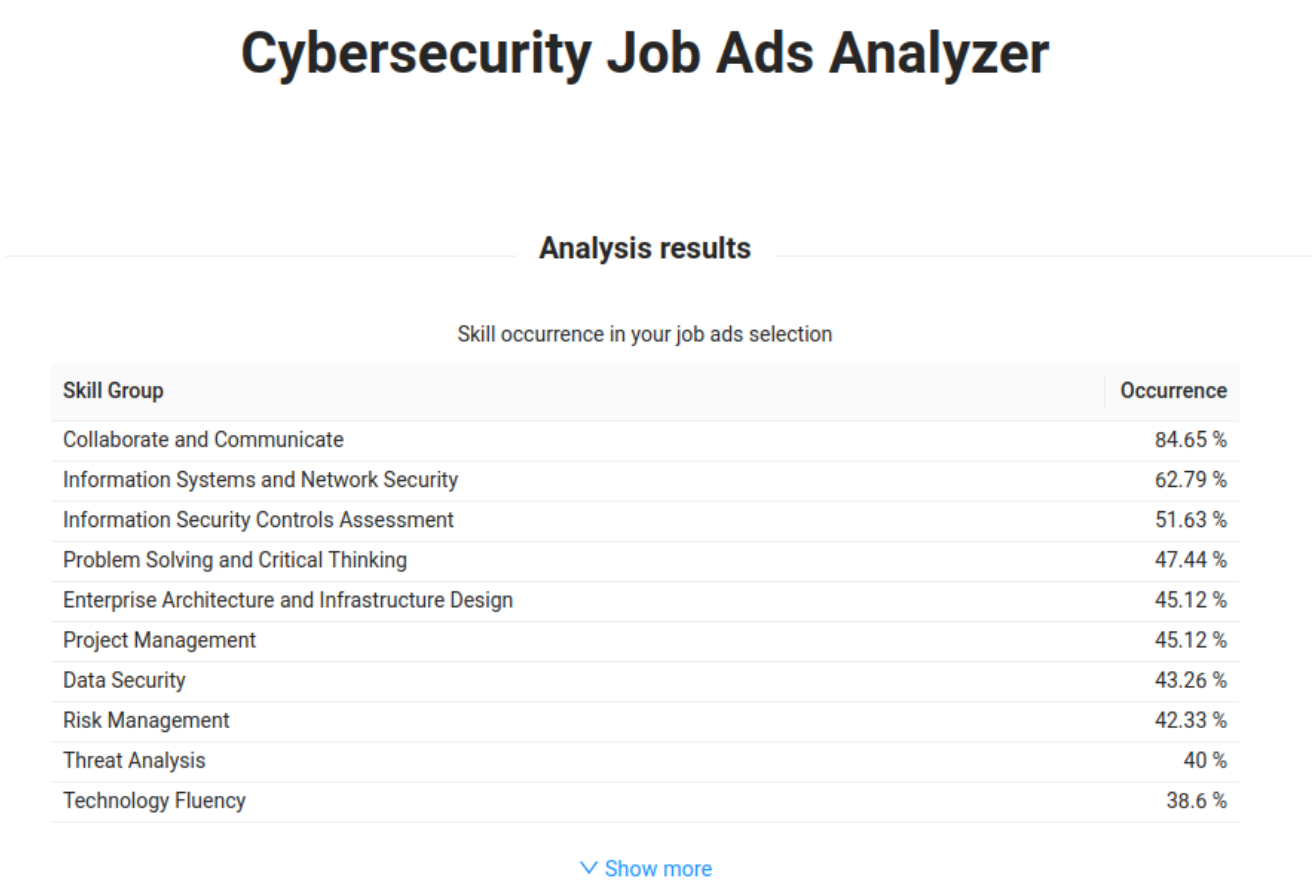


Figure 2. Example of Job Ads Analyzer result on Cybersecurity Architect job profile

At the moment of the submission of this deliverable, the Job Ads Analyzer included 1316 inserted jobs across 31 European States. The ML results can show the identified cybersecurity skills within the selected job adverts. For instance, Figure 1 shows the results of the ML algorithm on the 215 Cybersecurity Architect-related ads. While the ML algorithm may identify all 31 skills, their occurrences give a rough estimate of their importance from a market point of view for that role. Moreover, Table 3 compares the top 10 skills identified by the app and the one describing the Cybersecurity Architect in the ECSF framework. The highlighted skills (in blue) are common between the ECSF and ML market demand analysis.

Skills Groups in the ENISA Framework	Job Ads Analyzer
Collaborate and Communicate	Collaborate and Communicate
Data Privacy	Information Systems and Network Security
Data, Asset and Inventory Management	Data Security
Enterprise Architecture/ Infrastructure Design	Enterprise Architecture and Infrastructure Design
Information Security Controls Assessment	Information Security Controls Assessment

Law, Policy, and Ethics	Threat Analysis
Risk Management	Risk Management
Software Development	Data Security
Technology Fluency	Technology Fluency
Workforce Management	Project Management

Table 3. Comparison between ENISA and Job Ads Analyzer on top skills

Moreover, Figure 2 shows the skills occurrences for the cybersecurity architect job ads (in red) compared to the ones in the whole data set. For instance, the chart highlights that Enterprise Architecture skills are more required in cybersecurity architect-oriented ads.

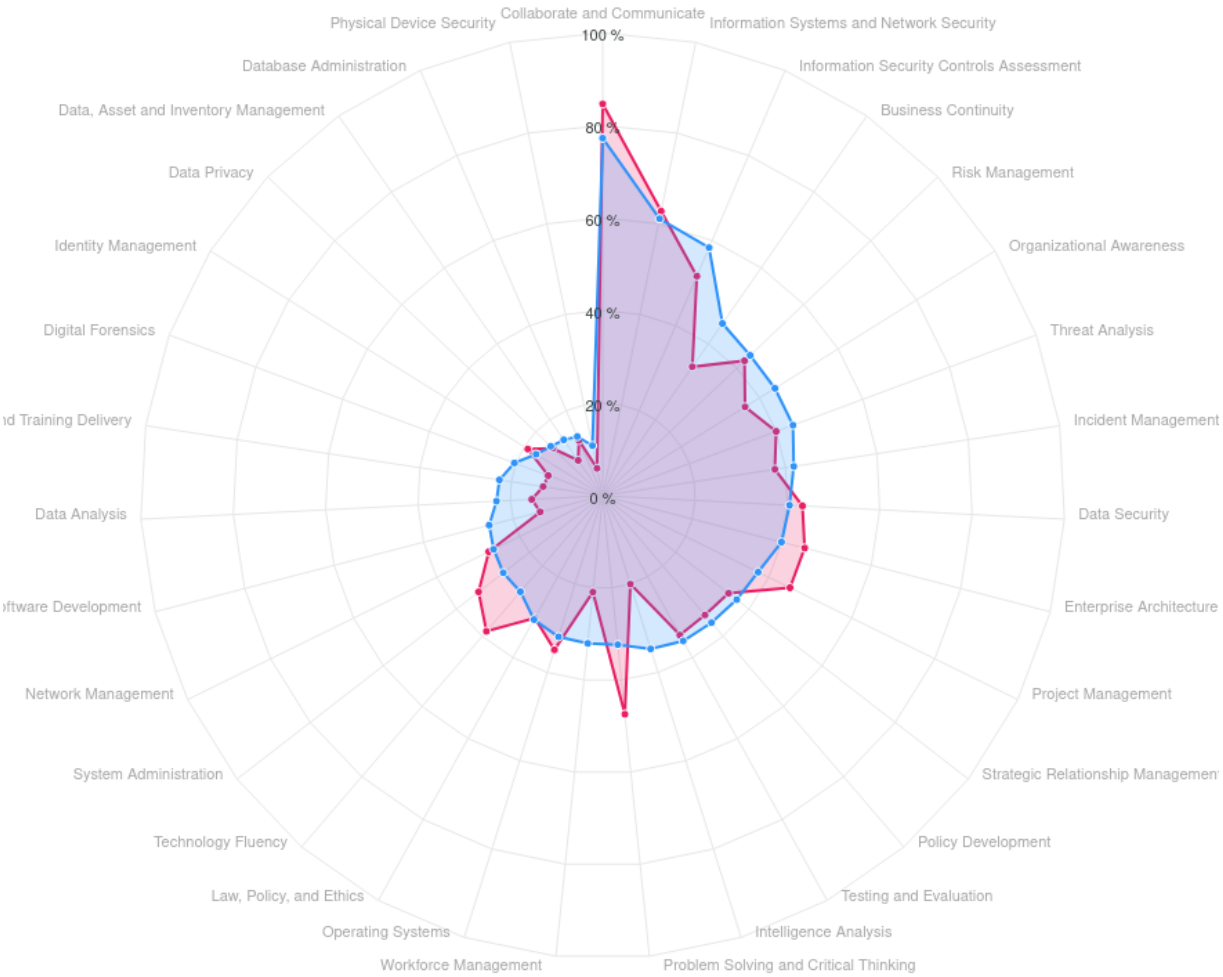
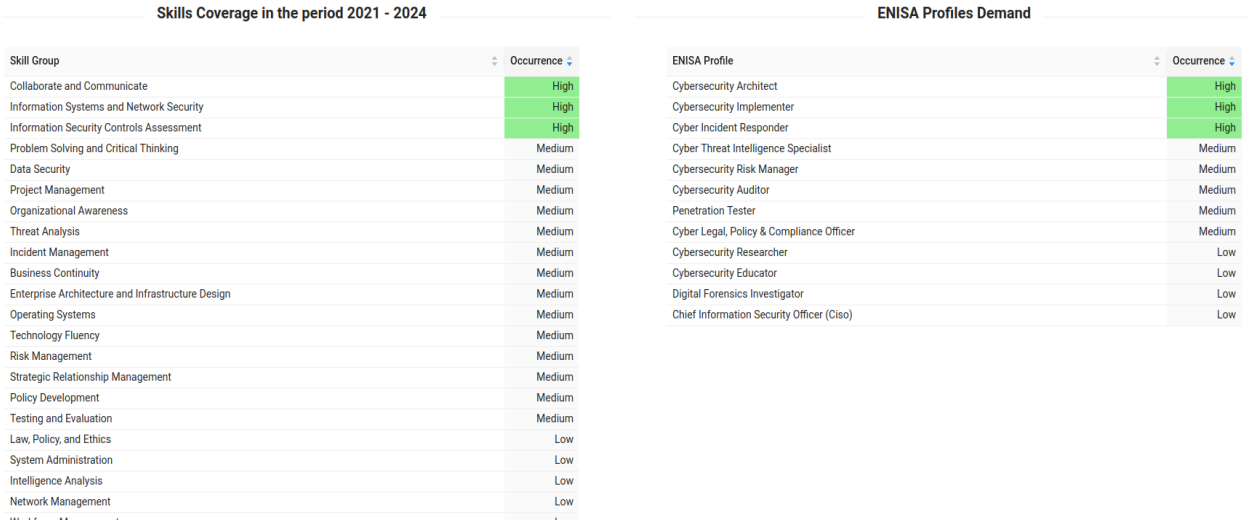


Figure 3. Comparison between skills occurrences in cybersecurity architect ads and the whole data set

The application allows analyzing which skills and profiles are the most requested in a time frame. For instance, Figure 3 depicts the skills and profiles analysis for the period 2020-2024, estimating that "Collaborate and Communicate", "Information Security Controls Assessment", and "Information Systems and Network Security" skills are highly requested as well as "Cybersecurity Architect", "Cybersecurity Implementer", and "Cyber Incident Responder" profile are the one in more demand.



Skills Coverage in the period 2021 - 2024

Skill Group	Occurrence
Collaborate and Communicate	High
Information Systems and Network Security	High
Information Security Controls Assessment	High
Problem Solving and Critical Thinking	Medium
Data Security	Medium
Project Management	Medium
Organizational Awareness	Medium
Threat Analysis	Medium
Incident Management	Medium
Business Continuity	Medium
Enterprise Architecture and Infrastructure Design	Medium
Operating Systems	Medium
Technology Fluency	Medium
Risk Management	Medium
Strategic Relationship Management	Medium
Policy Development	Medium
Testing and Evaluation	Medium
Law, Policy, and Ethics	Low
System Administration	Low
Intelligence Analysis	Low
Network Management	Low

ENISA Profiles Demand

ENISA Profile	Occurrence
Cybersecurity Architect	High
Cybersecurity Implementer	High
Cyber Incident Responder	High
Cyber Threat Intelligence Specialist	Medium
Cybersecurity Risk Manager	Medium
Cybersecurity Auditor	Medium
Penetration Tester	Medium
Cyber Legal, Policy & Compliance Officer	Medium
Cybersecurity Researcher	Low
Cybersecurity Educator	Low
Digital Forensics Investigator	Low
Chief Information Security Officer (Ciso)	Low

Figure 4. Skills coverage and ENISA profile demand

In the collection of job ads, users can choose whether the related job ads refer to more than one ECSF profile. Figure 4 depicts the correlation among profiles, where thicker edges represent stronger relationships, and larger node indicate higher demand for that profile. Job ad descriptions often match the Cybersecurity Architect and Cybersecurity Implementer profiles, as well as the Cyber Incident Responder and Cyber Threat Intelligence Specialist profiles. This suggests that the skills required for these job roles involve a combination of knowledge from those profiles.

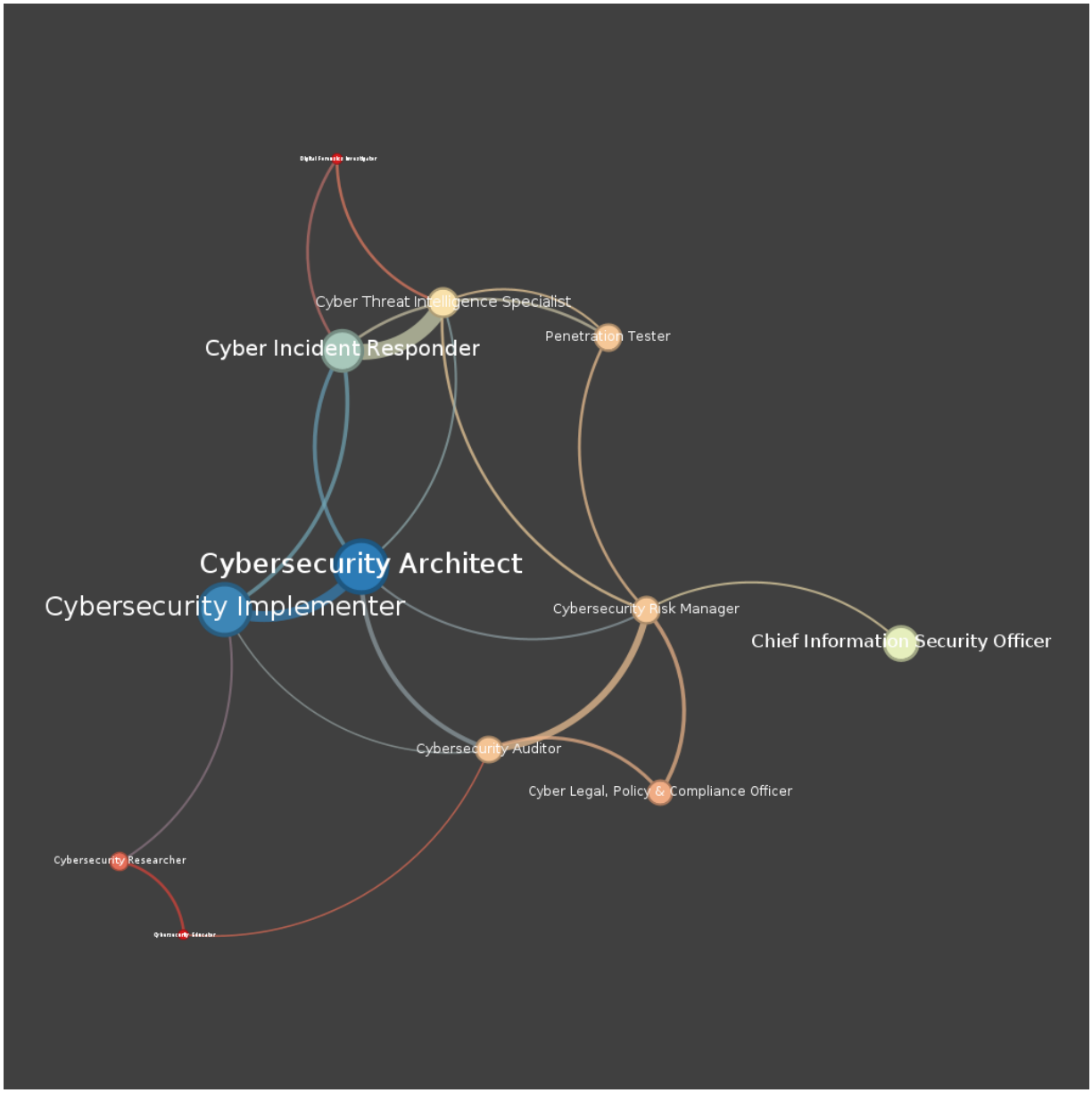


Figure 5. Correlation among ECSF profiles

Figure 5 depicts the correlation (i.e., edges) among skills weighted on the number of their appearance in the same ad. If one excludes “Communication and Collaboration" the most demanded skills together are 1) “Information Systems and Network Security" and “Information Security Controls Assessment" as well as 2) “Information Systems and Network Security” and " Enterprise Architecture and Infrastructure Design"

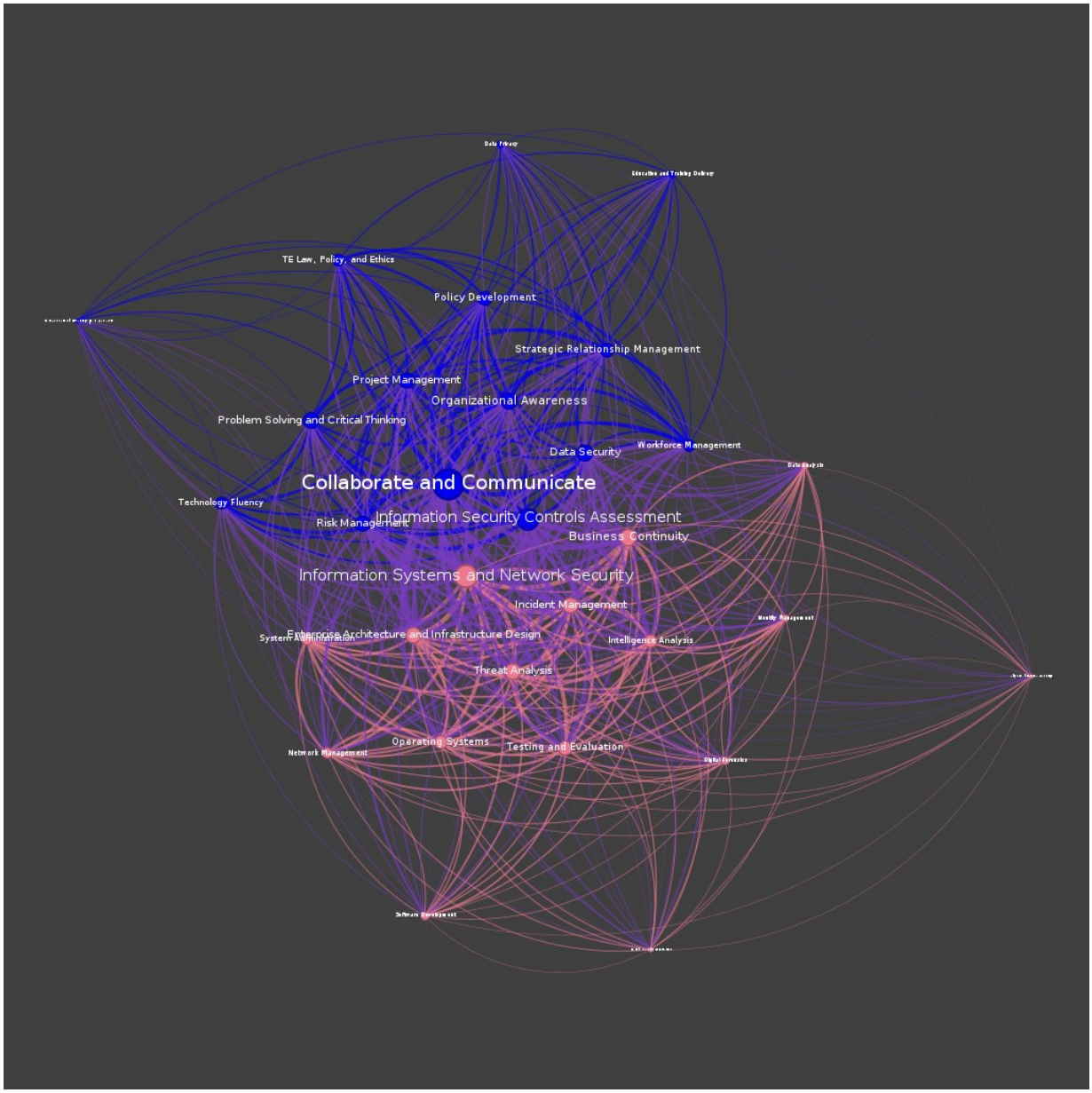


Figure 6. Skills correlation

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4.2. CYBERABILITY PLATFORM

The CyberABILITY platform[4] is designed to meet the growing demands of the cybersecurity sector. It is a comprehensive Cybersecurity Skills Digital Observatory, providing insights into the job market, key competencies, training programs, and certifications. The platform supports professionals, organizations, and educational institutions to stay informed about cybersecurity trends. Leveraging REWIRE project deliverables, CyberABILITY maps courses and certifications to a detailed framework. Key tools include:

- **Cybersecurity Jobs Analyzer**: Identifies specific cybersecurity skills needed for various roles, utilizing a job advertisement database and machine learning to align skills with real-world demands, integrating ENISA's framework.
- **Cybersecurity Profiler**: Maps curricula, training, and certifications to cybersecurity roles, assisting users in finding recommended courses and designing study programs in line with ENISA standards.
- **ECSF Explorer**: Offers an interactive tool for exploring the European Cybersecurity Framework (ECSF), showcasing profiles, key skills, and knowledge relevant to specific roles (see Figure 6).

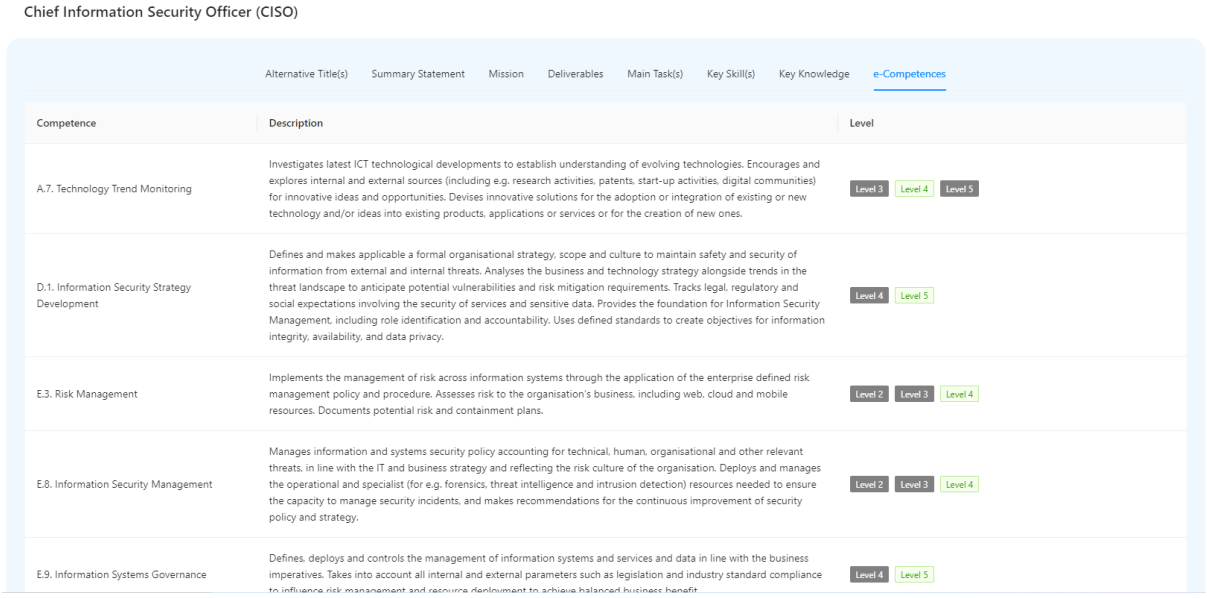


Figure 7. Example: E-competences required by CISO

In addition, the CyberABILITY platform is also based on The European Cybersecurity Skills Framework (ECSF), a tool designed to identify and define the tasks, skills, competencies, and knowledge required for various cybersecurity roles across Europe. It serves as the EU's reference for evaluating relevant skills, aligning with the Cybersecurity Skills Academy established by the European Commission. ECSF organizes cybersecurity roles into 12 profiles, detailing their responsibilities, skills, and interconnections. It promotes a shared understanding of critical competencies, facilitates skill recognition, and supports creating

[4] https://cyberability-platform.informacni-bezpecnost.cz/

cybersecurity-related training programs. The ECSF aims to standardize cybersecurity terminology and create a shared understanding between employers and educators across the EU. It helps identify critical skills needed for the workforce, supports the development of targeted learning programs, and aids policy-makers in addressing skills gaps. By clarifying essential professional roles and skills, ECSF assists non-experts and HR departments in recruitment and career planning. Additionally, it promotes harmonization in cybersecurity education and enhances the protection against cyberattacks by strengthening the European cybersecurity workforce.

The ECSF Explorer is an interactive tool for navigating the European Cybersecurity Skills Framework (ECSF).[5] The tool is integrated into the CyberABILITY platform, allowing users to explore various cybersecurity roles, including alternative titles, key responsibilities, required skills, and knowledge. Users can view the specific e-competences associated with each role, with colour-coded tags indicating the required competence levels. Green tags highlight the necessary levels for the role, while grey tags show other potential levels for that competence. This tool helps users better understand the qualifications and competencies needed for cybersecurity professionals.

[5] https://cyberability-platform.informacni-bezpecnost.cz/roles

5. CYBERSECURITY THREATS TRENDS

This chapter aims to conduct a comparative analysis of different sectoral surveys, studies, and national threat trends reports to identify the latest cybersecurity threats that emerged in 2023. It is important to track emerging threats in order to react to them and adapt the respective cybersecurity skills necessary to adapt to them.

The ENISA Threat Landscape Report of 2024 (ENISA report) indicates that the primary threats identified in 2023 remain the same.[i] The prime threats identified due to their prominence over the reporting period are ransomware, malware, social engineering, threats against data, threats against availability and integrity, disinformation – misinformation, and supply-chain attacks.

Ransomware is an attack in which threat actors seize control of a target's assets and demand a ransom to restore access or prevent public data exposure. This definition reflects the evolving ransomware landscape, where multiple extortion methods and motives beyond financial gain are increasingly common. Ransomware remains a top threat, with several high-profile incidents occurring during the reporting period. For another consecutive year, threats to availability, such as DDoS attacks and ransomware, ranked as the top cyber threats during the reporting period.[ii]

The UK NCSC reports that ransomware remains one of the most significant cyber threats to the UK, urging organizations to protect themselves. While cybercriminals typically steal and encrypt data, data extortion attacks—where data is stolen without encryption—are becoming more common. Between 2022 and August 2023, the NCSC received 297 ransomware reports, with 28 resulting in managed incidents. The top sectors affected were academia (50 reports), manufacturing (28), IT (22), finance (19), and engineering (18), though there's no clear targeting of academia. Sanctions on groups like EvilCorp and Conti have led criminals to diversify, while Ransomware as a Service (RaaS) lowers entry barriers, allowing smaller groups to adopt these tactics, impacting the cybercrime landscape.[iii]

However, most ransomware incidents do not rely on sophisticated attack techniques. Criminals often succeed because of poor cyber hygiene. Many organizations do not follow NCSC advice, resulting in many victims. If organizations do not implement proper protective measures, the threat will persist as attackers continue to exploit opportunities and maximize their profits.[iv]

ACSC reports that 10% of all incidents responded to were related to ransomware, which is consistent with last year. One hundred fifty-eight (158) entities notified ransomware activity on their networks, compared to 148 last year, marking roughly a 7% increase. The number of extortion-related cybersecurity incidents that ACSC responded to increased by about 8% compared to the last year. Over 90% of these incidents involved ransomware or other restrictions to systems, files, or accounts.[v]

According to ACSC, cybercriminals continually adapted their tactics to extract the highest payments from victims, evolving their operations to target Australian organizations. A global network of access brokers and extortionists drove this. The Australian Signals Directorate (ASD) responded to 127 extortion-related incidents, with 118 involving ransomware or other

forms of system, file, or account restrictions. Business email compromise persisted as a major method of cybercrime, while ransomware remained a highly destructive threat. Similarly, hacktivists' denial-of-service attacks disrupted the business operations of various organizations.[vi] A quarter of ransomware incidents also involved confirmed data exfiltration, known as 'double extortion,' where attackers demand payment for decrypting data and preventing its public release. Some ransomware actors claim to have exfiltrated data, but verifying these claims can be challenging until data exfiltration is confirmed or the authenticity of leaked data is established.[vii]

According to Crowdstrike, while ransomware remains a favoured tool for many big game hunting (BGH) adversaries, data theft extortion has become an increasingly appealing—and often simpler—monetisation method. This is reflected in the 76% rise in victims listed on BGH-dedicated leak sites (DLSs) between 2022 and 2023. Throughout the year, access brokers continued to capitalize by selling initial access to eCrime threat actors, with the number of advertised accesses increasing by 20% compared to 2022.[viii]

CrowdStrike reports that while ransomware makes up a small portion of overall malware detections, its impact is the most severe. It affects businesses across all sectors, with small- and medium-sized enterprises (SMEs) being the most frequent targets. In 2021, the Institute for Security and Technology's Ransomware Task Force found that 70% of ransomware attacks targeted small businesses, a trend consistent with CrowdStrike's data despite yearly fluctuations in incidents.[ix]

The record number of victims listed on dedicated leak sites (DLSs) in 2023 underscores big game hunting (BGH) as the most significant eCrime threat to organizations across all regions and industries. This increase is fueled by factors such as GRACEFUL SPIDER's zero-day exploitation campaigns, BGH actors targeting unmanaged devices (like edge gateways and VMware ESXi for encryption), and a growing trend of naming victims after data theft without deploying ransomware. CrowdStrike's Chief Adversary Officer (CAO) predicts that while ransomware will remain the primary extortion method through 2024, BGH adversaries will increasingly exploit stolen data to pressure victims into paying. This trend is expected to accelerate, particularly as new U.S. Securities and Exchange Commission (SEC) rules impact the disclosure of major cybersecurity incidents. In 2023, SCATTERED SPIDER's use of Alphv ransomware highlighted extortion's effectiveness. Previously focused on cryptocurrency theft and SIM swapping, the group now uses ransomware to expand its targets. Without law enforcement disruption, SCATTERED SPIDER is expected to remain a major threat to high-revenue private sector entities in Europe and North America through 2024.[x]

According to the New Zealand NCSC, some of the key themes we explore include the ongoing impact of cybercriminal activity and extortion. Ransomware continues to impose significant financial costs and demands extensive recovery efforts. Malicious cyber activity increasingly causes downstream effects, especially as Aotearoa, New Zealand's digital supply chain, grows deeper and more interconnected. Phishing and other social engineering tactics remain widespread and effective. However, emerging technologies like generative AI are poised to enhance the sophistication of these attacks, enabling more convincing and targeted lures, which could lead to a faster rate of compromise.[xi]

New Zealand's NCSC reports that 2022/2023 saw the most severe incidents classified as C3, primarily involving disruptive ransomware and extortion. Unlike the previous year, which had two C2 incidents, these C3 events had broader impacts, such as one compromise affecting multiple organizations' privacy and security. Criminal cyber activity, particularly ransomware and extortion, increased compared to previous years, with over one ransomware incident recorded per month. Half of these were C3-level, including one incident that forced critical infrastructure to activate business continuity plans, highlighting the threat of lateral movement into operational technology.[xii]

According to Sophos, In 2023, LockBit ransomware was the leading threat in small business cases handled by Sophos Incident Response. As a ransomware-as-a-service (RaaS), LockBit was the most widely deployed ransomware in 2022, accounting for nearly three times as many incidents as its closest competitor, Akira. Ransomware is also expanding beyond Windows systems, with developers creating cross-platform versions for macOS and Linux. In February 2023, a Linux variant of Cl0p ransomware was discovered, and Sophos has since observed it leaked versions of LockBit targeting both macOS and Linux platforms.[xiii]

Truesec says top-tier ransomware groups operate large teams of cybercriminals collaborating to breach networks and deploy ransomware. These syndicates represent the most sophisticated and varied threat to organizations. They invest heavily in custom tools, infrastructure, and employee salaries. Their preference is to target larger companies, seeking a substantial return on investment through multimillion-dollar ransoms, which only prominent victims are likely able to pay, making their time and financial investment worthwhile. [xiv]

Truesec reports that modern ransomware syndicates operate like organized businesses, with Russian groups often portraying themselves as "penetration testers" charging fees for poor cybersecurity, a narrative they sometimes internalize. These groups are financially driven, not thrill-seekers and their business models vary. Novice criminals use basic ransomware and simple tactics like password spraying, while advanced groups invest in ransomware-as-a-service (RaaS) and buy access from brokers, paying between 1,000 and 10,000 euros based on the target's size. Truesec's 2023 Threat Intelligence Report predicted a rise in ransomware due to Russia's isolation and economic struggles, leading more people into cybercrime. Since then, there has been a surge in new ransomware groups, with over 50% of cases in 2023 involving previously unknown actors. Rebranding and tensions between new and veteran criminals, particularly within the LockBit syndicate, make tracking difficult. As new actors improve, more skilled ransomware attacks are expected.[xv]

Malware, or malicious code or logic, is a broad term for any software or firmware designed to execute unauthorized actions that negatively affect a system's confidentiality, integrity, or availability. In 29% of cases, malware incidents impacted the general public, followed by infections in digital infrastructure at 25% and public administration at 11%. Additionally, 9% of observed malware events affected all sectors.[xvi]

UK NCSC reports that they identified 323,000 unique IP addresses with some form of vulnerability and 10,200 unique IPs with malware infections. UK NCSC distinguishes the top five malware families: avalanche-andromeda, Downadup, Camargue, snatch, and remnant.[xvii]

In May, the NCSC issued a joint advisory revealing details of 'Snake,' a sophisticated Russian espionage malware targeting Critical National Infrastructure in over 50 countries.

AI, particularly large language models (LLMs), is enhancing vulnerability detection, malware analysis, and faster release of indicators of compromise (IOCs). UK NCSC plans to use AI to detect mutated malware and identify patterns in services like blockchain-based DNS. In the long term, they aim to use ACD data to detect malicious behaviour across government systems.[xviii]

According to ACSC, in 2022–23, ASD collaborated with international partners to expose Russia's Federal Security Service for using 'Snake' malware in cyber espionage. Additionally, ASD highlighted the actions of a state-sponsored cyber actor from the People's Republic of China, who used 'living-off-the-land' techniques to compromise critical infrastructure organizations.[xix] CVEs have no expiration, as seen when ACSC observed cyber actors exploiting a 7-year-old unpatched CVE. Similarly, reports of WannaCry malware persist six years after its release, likely due to legacy systems being reconnected. These cases highlight the importance of timely patching and the risks of unpatched systems. In 2022–23, 57% of cybersecurity incidents affecting Australian critical infrastructure involved compromised accounts, assets, or DoS attacks, with data breaches and malware also significant.[xx]

As reported by the New Zealand NCSC, in the 2022/2023 year, the NCSC contributed to multiple cybersecurity advisories, publicly exposing sophisticated malicious cyber activity and offering guidance on detecting and mitigating its impact. At times, malicious cyber activity indirectly affects Aotearoa New Zealand's interests or poses a future risk. In such cases, the NCSC may collaborate with international partners to issue advisories identifying malware or specific tactics, techniques, and procedures (TTPs). These advisories help raise awareness of cyber threats and offer guidance to mitigate malicious activity.[xxi] In May 2023, we collaborated with international cybersecurity allies to reveal technical details about malware linked to Russia's FSB, particularly the Snake malware. While dominant ransomware-as-a-service (RaaS) providers gained strength, new variants and players emerged in 2022/2023. Innovations, especially in initial access and automated encryption, have increased. Cybercriminals are now targeting suppliers and developing malware aimed at hypervisors, which, if compromised, could impact multiple organizations relying on shared hardware.[xxii]

According to Crowdstrike, in 2023, coordinated international law enforcement operations targeted BGH actors, resulting in arrests, technical actions against their capabilities, cryptocurrency seizures, and sanctions on specific individuals. The disruption of HIVE SPIDER's Hive RaaS and MALLARD SPIDER's QakBot malware created gaps that were quickly filled by competing RaaS and MaaS actors, highlighting the resilience of the eCrime ecosystem when takedowns do not apprehend the individuals behind the operations.[xxiii] In 2023, adversaries shifted from using macros and ISO files for malware delivery, turning to malicious OneNote files after a Microsoft patch. Groups like LUNAR SPIDER and HONEY SPIDER adopted this method, but its use declined after Microsoft restricted certain file types. Adversaries then explored new techniques like malvertising, SEO poisoning, and spam campaigns using PDFs, HTML smuggling, and WebDAV. By late 2023, the malware was distributed through fake browser updates. Several macOS malware variants, such as AMOS and ShadowVault, also emerged, targeting passwords, cookies, and cryptocurrency wallets.[xxiv]

Crowdstrike notes that the rise of macOS malware and evolving delivery methods show the eCrime ecosystem's adaptability. Criminals often copy successful tactics, like using OneNote files, and will likely continue innovating in 2024. Trends in malware delivery will likely shift, with SEO poisoning, malvertising, and spam-based methods remaining popular. This assessment is based on observed trends since late 2022.[xxv]

According to Sophos, data theft is the primary goal of malware targeting small and medium businesses, with spyware like password stealers and keyloggers making up nearly half of detections. Attackers increasingly use web-based methods like malvertising and SEO poisoning to bypass security. In 2023, nearly half of detected malware focused on data theft, mainly through "stealers" that capture credentials, cookies, and keystrokes. While most malware can steal data, categorizing it by function is difficult. Around 10% targeted browsers or specific apps like Discord tokens. The Malware-as-a-Service (MaaS) model remains dominant, with AgentTesla leading in 2023, accounting for 51% of detections.[xxvi] Sophos reports that small businesses rely heavily on mobile devices for essential tasks, making them a target for cybercriminals. Android malware, especially spyware and "bankers," poses a major threat. Spyware collects personal data like SMS messages and call logs, which can be sold or used for blackmail. "Bankers" target financial apps, including cryptocurrency wallets, to steal account information and funds, often exploiting accessibility permissions. These malicious apps are often disguised as legitimate in app stores or shared via text message links.[xxvii]

Truesec has observed a rise in the automation of cyberattacks in recent years. Malware developers increasingly provide criminals with complete attack frameworks featuring user-friendly GUIs, making it easier for novices to carry out attacks. Hopes that AI-powered chatbots would be responsibly regulated to prevent cybercrime have been dashed. AI researchers are now releasing chatbots trained on dark web data, specifically designed to assist cyber criminals. These malicious AI bots can create advanced phishing campaigns, execute social engineering tactics, exploit vulnerabilities, and generate and distribute malware. This year, advanced threat actors are increasingly shifting away from specialized malware and exploiting legitimate hacking tools. Using existing tools within a target's environment allows these actors to remain low profile and undetected for years, avoiding using known toolkits and blending in with normal operations. Whether a threat actor infiltrates your systems from the outside or is an insider with network access, certain key capabilities can help you detect and remove even the most stealthy intruders, even if they don't deploy malware to steal data.[xxviii]

Social engineering refers to activities that exploit human error or behaviour to gain access to information or services. It manipulates victims into making mistakes or disclosing sensitive information, often through tricks like opening files, visiting websites, or granting system access. While these methods may involve technology, they rely on human interaction to succeed. Common attack vectors include phishing, spear-phishing, whaling, smishing, vishing, watering hole attacks, baiting, pretexting, quid pro quo, honeytraps, and scareware. Social engineering can be used for initial access or later stages of an incident, with notable examples including business email compromise (BEC), fraud, impersonation, counterfeit schemes, and extortion.[xxix]

ACSC reports that cybercriminals use social engineering to gain unauthorized access to systems or data by manipulating individuals. They may create a sense of urgency or impersonate a trusted source to convince victims to click on malicious links or files or disclose sensitive information, sometimes over the phone. Phishing is a common tactic used by cybercriminals to access systems by tricking victims into clicking malicious links or files. This can lead to personal data theft or malware installation. Despite growing awareness in Australia, more must be done to improve resilience. Always verify suspicious messages by checking official sources and avoid clicking links in unsolicited communications. Report any suspicious activity to ReportCyber and Scamwatch, and educate staff on corporate-focused social engineering risks.[xxx]

As observed by Crowdstrike, adversaries with various motivations and from different regions continue to employ phishing techniques that impersonate legitimate users to target valid accounts and other authentication data. Beyond stealing account credentials, CrowdStrike CAO has noted that adversaries also target API keys and secrets, session cookies and tokens, one-time passwords (OTPs), and Kerberos tickets throughout 2023.[xxxi] Identity-based techniques are central to SCATTERED SPIDER's tactics. In 2023, they executed sophisticated social engineering campaigns to access victim accounts. They used SMS phishing (smishing) and voice phishing (vishing) to collect credentials and manipulate help desk personnel for password or MFA resets. They often exploited prior intrusions at telecom companies to SIM swap targeted employees, allowing them to receive SMS with OTP codes. SCATTERED SPIDER primarily targets employees in information security and IT due to their access to security tools and occasionally targets those with access to company financial resources.[xxxii]

New Zealand NSCS reports that the key themes we examine include the ongoing impact of cybercriminal activity and extortion. Ransomware continues to impose significant costs and necessitates extensive recovery efforts. Malicious cyber activity increasingly affects the digital supply chain in Aotearoa, New Zealand, which is becoming more complex and interconnected. Phishing and other social engineering methods remain prevalent and effective. Additionally, emerging technologies like generative AI will likely enable more convincing and targeted lures, potentially accelerating the pace of compromises.[xxxiii]

According to Sophos, e-mail attacks are shifting from basic social engineering to more active engagement, utilizing a thread of emails and responses to enhance the believability of their lures. Attacks on mobile device users have surged, with social engineering scams exploiting third-party services and social media platforms, impacting individuals and small businesses. These attacks include business email, cloud service compromises, and pig butchering (shā zhū pán) scams. [xxxiv] Due to the modular nature of malware, fully categorizing it by functionality is challenging, as nearly all types can steal some form of data from targeted systems. This also excludes other credential theft methods, such as phishing via email, text messages, and other social engineering attacks. Additionally, targets like macOS and mobile devices are vulnerable to malware, potentially unwanted applications, and social engineering aimed at accessing users' financial data. In the past year, Sophos' messaging security team has encountered numerous new social engineering tricks designed to bypass conventional email defences. Rather than sending unsolicited attachments or links, more effective spammers often initiate a conversation first before making their move in follow-up emails.[xxxv]

According to Truesec, the expectation that responsible oversight would limit the use of AI-powered chatbots in cybercrime has not been met. Researchers are now releasing chatbots trained on the dark web to assist cybercriminals. These bots aim to create sophisticated phishing campaigns, execute social engineering attacks, exploit vulnerabilities, and distribute malware. Currently, several malicious chatbots are available, including one that helps with scripting and coding issues and another that assists in crafting effective phishing emails.[xxxvi] AI chatbots can aid in social engineering attacks, but using them for text translation is not significantly more innovative than using them for coding assistance. They can help proficient users translate more quickly, but the results are often unimpressive if employed merely as an advanced Google Translate.[xxxvii] Fake phone calls using AI-driven deep fake technology managed to deceive some staff, but most transfers were halted due to authorization procedures. This highlights how cybercriminals enhance social engineering attacks with voice cloning, which can effectively trick people. Soon, similar technology may also deceive visually. Moreover, SIM swapping enables criminals to make calls using the impersonated person's phone number.[xxxviii]

Threats against data

According to ENISA Threat Landscape 2024, A data breach, as defined by the GDPR, involves any security breach that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data (Article 4.12 GDPR). Technically, threats to data can be classified as either a data breach or a data leak, though these terms are often confused. A **data breach** is an intentional cyberattack by a criminal aiming to gain unauthorized access to and release sensitive or confidential data. In contrast, a **data leak** occurs unintentionally, often due to misconfigurations, vulnerabilities, or human error, leading to unintentional data exposure. Intentional data leaks are sometimes referred to as **data exposure**.[xxxix]

According to Sophos, Business email compromise (BEC), where cybercriminals take over email accounts for fraudulent or malicious activities, is a significant issue for small-to-medium businesses. While our sister publication, the Active Adversary Report, does not currently cover BEC, its authors estimate that 2023 BEC incidents were more frequently identified by our Incident Response team than any other incident type, except for ransomware. Stolen credentials, including browser cookies, can be leveraged for BEC, gaining access to third-party services like cloud-based financial systems or internal resources that can be exploited for financial gain. These credentials can also be sold by "access brokers" on underground forums, providing access to networks of small and medium-sized businesses, which Sophos has been tracking.[xl]

In 2023, nearly half of all detected malware was aimed at stealing data from its victims. Most of this malware falls under "stealers," designed to capture credentials, browser cookies, keystrokes, and other valuable data. This stolen data can be sold for profit or further exploited. Due to the modular nature of malware, it is challenging to categorize it strictly by functionality, as most malware can steal some form of data from targeted systems. Additionally, these detections do not account for other credential theft methods, such as phishing through email, text messages, and social engineering attacks. Other targets, like macOS and mobile devices,

are also vulnerable, with malware, potentially unwanted applications, and social engineering tactics particularly focusing on financial data.[xli]

Threats against the availability and integrity of data

ENISA Threat Landscape 2024 states that DDoS attacks target systems and data availability. While not a new threat, they remain a significant part of the cybersecurity landscape. These attacks occur when users cannot access data, services, or resources due to the exhaustion of system resources or overloading network infrastructure. Although DDoS attacks can be disruptive, their impact is often limited and symbolic.[xlii]

According to the New Zealand NCSC, information operations involve deliberately spreading misleading or harmful information to influence or undermine the authority of a targeted entity, typically a nationally significant organization, politician, or government. These operations frequently use inauthentic behaviour and misinformation, disseminated through commercial or public technology platforms like news websites or social media. Unlike traditional cyberattacks, information operations rarely compromise computer networks' confidentiality, integrity, or availability.[xliii]

Disinformation and misinformation (or information manipulation)

According to ENISA Threat Landscape 2024, foreign information manipulation and Interference (FIMI) refers to intentional and coordinated activities, often non-illegal, that threaten or have the potential to harm values, procedures, and political processes. FIMI can be conducted by state or non-state actors, including proxies both within and outside their territories. This report examines the threat irrespective of its source.[xliv]

As reported by the UK NCSC, AI has the potential to improve society, but at the NCSC, we know its risks, especially in trusting democratic systems. While the UK's use of paper ballots makes election interference harder, the next election will occur amid major AI advancements. The biggest threat is AI enhancing existing techniques, such as generating fake content, spreading disinformation with AI bots, and creating more sophisticated deepfakes. The UK government is committed to countering these threats, but the public must know about the changing risks. AI, often built using machine learning (ML), can unintentionally incorporate bias or misinformation due to flawed data. This vulnerability also opens the door to adversarial attacks, such as data poisoning, where attackers corrupt the data used to train AI systems.[xlv] In 2023, state-aligned actors have emerged as a new cyber threat to critical national infrastructure (CNI), adding to the ongoing risk from state actors. These groups typically engage in DDoS attacks, website defacements, and spreading misinformation. However, some have expressed intentions to cause more disruptive and destructive impacts on Western CNI, including in the UK. The NCSC remains focused on strengthening the resilience of the UK's CNI.[xlvi]

According to ACSC, security researchers have demonstrated how machine learning (ML) data sets can be attacked and "poisoned" with anomalous data, leading to misleading outputs. In 2016, Microsoft had to stop testing a chatbot after some users intentionally fed it misinformation and abusive content, causing it to generate offensive text.[xlvii]

Corwdstrike reports that Less direct forms of targeted intrusion involve efforts to compromise, disrupt, or leak data from government systems that support elections, such as those providing voter logistics or storing registration data. These tactics include DDoS attacks and website defacements, often used by hacktivists during politically charged periods. Political candidates, parties, donors, and advocacy groups are also vulnerable to hack-and-leak operations, which aim to discredit the targets. The most common and difficult-to-prevent form of election interference involves spreading misinformation or disinformation to influence public opinion before, during, and after elections. These information operations may undermine confidence in election outcomes, attack the integrity of candidates, or promote polarizing rhetoric. In some cases, they seek to cast the responsible threat actor in a favourable light by aligning with certain policy positions or promoting a message of cooperation.[xlviii]

Truesec states that a blurred line exists between Russian hacktivism, disinformation, and cybercrime. The Russian hacktivist group KillNet has carried out DDoS attacks in support of a darknet drug-selling site against a competitor. KillNet has also collaborated with a Telegram channel that monetizes disinformation by promoting pro-Russian narratives and crypto scams targeting Western conspiracy theorists. While hacktivism may seem like crowdfunded cyber vandalism, it is increasingly part of the larger threat posed by the post-truth disinformation ecosystem. [xlix]

Supply chain attacks

According to ENISA Threat Landscape 2024, Supply chain attacks have emerged as a cross-cutting threat, affecting multiple other types of cyber risks.[l]

UK NCSC reports that The NCSC's Incident Management team saw a 64% rise in reported cyberattacks in 2023, with 2,005 reports compared to 1,226 last year. Of these, 62 were deemed nationally significant, with four being particularly severe due to their impact on critical infrastructure supply chains. Since Russia invaded Ukraine, its cyber operations have expanded beyond military targets to include academics, think tanks, logistics hubs, and IoT devices. Small organizations are at risk, as simple interactions like malicious emails enable hostile actors to infiltrate networks. Supply chain compromises remain a major threat, exemplified by the SolarWinds breach attributed to Russia's SVR. The NCSC has strengthened cyber resilience by building trust groups and CISO communities, helping large and small organizations improve their defences through collaboration and shared guidance.[li] UK NCSC adds that the UK NCSC is improving online security for citizens and small organizations by reducing their need to act. Our Takedown Service has removed nearly 10 million malicious domains, preventing scams. We're also developing the Share and Defend capability to share data on malicious domains in real time with service providers, enhancing protection. This is being tested with major UK ISPs. Russia has also been hit by cyberattacks, with government and key sectors like energy and military frequently targeted. [lii]

According to ACSC, A malicious cyber actor can compromise multiple victims by targeting a single upstream or third-party supplier in an ICT supply chain attack, which involves two phases: first, attacking the supplier and then its customers. For instance, compromising a managed service provider (MSP) gives attackers privileged access to hundreds of customers or sensitive data, which they can exploit or use for extortion. This shows that even with strong

defences, a company's security is only as strong as its weakest link in the supply chain. Common techniques in ICT supply chain attacks include exploiting device misconfigurations, phishing, and using known vulnerabilities (CVEs).[liii]

Crowdstrike reports that in 2023, Democratic People's Republic of Korea (DPRK) adversaries, particularly LABYRINTH CHOLLIMA, increasingly exploited trusted relationships to conduct supply chain attacks. In three cases, LABYRINTH CHOLLIMA compromised the relationship between a technology vendor and its client, using supply chain attacks as an entry point. In March 2023, they compromised VoIP provider 3CX through an upstream attack on financial tech firm Trading Technologies. The attackers used trojanized 3CX apps to deploy information-stealing malware. In July 2023, they launched a similar attack, compromising a technology company's product to infiltrate its clients. CrowdStrike also observed LABYRINTH CHOLLIMA using a trojanized CyberLink media player in a campaign targeting specific geographies, indicating selective targeting. The motivations behind these compromises remain unclear, but LABYRINTH CHOLLIMA may cast a wide net to identify high-value targets for espionage or financial gain. Given the frequency of these incidents in 2023, additional supply chain compromises by this group are expected soon.[liv]

According to New Zealand NCSC, in 2022/2023, a key issue in the international landscape was targeting the security supply chain, particularly software and services critical to information security. In August 2022, LastPass revealed a breach of its proprietary information and source code, potentially setting the stage for future attacks on users' password vaults, which could grant access to valuable networks. That same month, Twilio, an SMS provider, reported a compromise targeting a subset of its customers, including Signal and Authy users. This suggests that attackers aimed to infiltrate the security supply chains of key organizations. As security services increasingly consolidate under a few cloud-based providers, they offer both enhanced security and a greater incentive for cyber actors to exploit them. These incidents likely prompted security improvements at similar companies while also serving as a proof-of-concept for other attackers.[lv] A supply chain compromise targets software, hardware, or IT service providers to exploit downstream customers, or when one organization holds data for others. Cybercriminals may extort both the victim and its customers. State-sponsored actors often use supply chains as entry points for attacks. The New Zealand NCSC works with critical infrastructure, providing alerts and guidance. In 2022/2023, the New Zealand NCSC assisted organizations affected by compromised providers, offering support and advice on improving digital supply chain security.[lvi]

Sophos reports that small businesses must be concerned about the security of services they rely on, as supply chain attacks are not limited to nation-state actors. In 2023, Sophos MDR responded to five cases where small businesses were attacked via exploits in a service provider's remote monitoring and management (RMM) software, with attackers using it to deploy tools and, in some cases, LockBit ransomware. Defending against attacks that exploit trusted software is challenging, especially when attackers can disable endpoint protection. Small businesses and their service providers must remain vigilant for signs of endpoint protection being turned off, which may indicate a supply chain vulnerability. A growing threat in 2023 involved attackers using vulnerable or malicious kernel drivers with valid digital signatures to bypass security measures and disable malware protection. These drivers operate at a low level, often running before security software, making them harder to detect. Supply

chain attacks involving third-party vendor services are an increasing concern, particularly among top ransomware groups.[lvii]

Content Management System (CMS) risk relates to a Content Management System (CMS) software. It refers to any unauthorized and malicious activity aimed at compromising the security of a CMS platform. CMS software is used to create, manage, and publish digital content on websites, and because it plays a central role in many websites, it is a common target for various types of cyberattacks. According to statistics available at that time, WordPress was estimated to be used by over 40% of all websites on the internet. The main attacks include Brute Force attempts, Vulnerability Exploitation, SQL Injection, Cross-Site Scripting (XSS), DDoS attacks, Malware infections, Phishing, and File Inclusion attacks.[lviii]

UK NCSC reports that data from the Vulnerability Reporting Service shows that most reported vulnerabilities are related to cross-site scripting, followed by information disclosure issues, often caused by CMS plugins. A key mitigation for many vulnerabilities is ensuring system owners regularly update their software and plugins to the latest versions.[lix]

AI (Artificial Intelligence) and generative AI-enabled

According to ENISA Threat Landscape 2024, recent observations reveal that state-linked groups from Russia, North Korea, Iran, and China are using large language models (LLMs) like ChatGPT for malicious activities, such as scripting, phishing, vulnerability research, and target reconnaissance. The main threat is not in new risks but in AI's ability to enhance existing techniques, enabling the large-scale distribution of fake, targeted narratives. These include manipulated social media posts, articles, memes, and photos. There have already been instances of doctored recordings falsely alleging election rigging or endorsing political candidates.[lx]

According to UK NCSC, as technology advances, so do the cybersecurity threats we face. Since the launch of ChatGPT, interest in Artificial Intelligence (AI) has surged, with AI now being a regular feature in the news. The NCSC has been researching AI security for years, collaborating with international partners and the UK's public and private sectors to harness AI's benefits while addressing associated risks. However, the NCSC also focuses on other critical technologies that receive less attention but are equally important for the future. These include semiconductors, cryptography (to protect data from future quantum computing threats), telecom security, socio-technical research, and radio frequency risks. The NCSC has provided expert advice for two national strategies the Department for Science, Innovation and Technology (DSIT) led to build resilience and safeguard national security. In the past year, the NCSC published 15 guidance pieces and 53 blogs and highlighted five major "cross-cutting" problems requiring significant collaborative efforts in its research problem book.[lxi] AI is advancing quickly, and cybersecurity must be integrated from the start to ensure systems are secure by design. Over the past year, we've highlighted AI risks, contributed to the government's AI agenda, and collaborated globally to promote secure foundations. While AI offers new cybersecurity opportunities, it also brings risks, particularly in machine learning (ML), which

can be vulnerable to biases and attacks like data poisoning. We are working with industry and academia to address these challenges and improve AI security.[lxii]

ACSC reports that in early 2023, AI tools became some of the fastest-growing consumer applications globally. AI enables machines to perform tasks requiring human intelligence, such as sorting data, automating tasks, and assisting in design. Machine learning (ML), a subset of AI, uses feedback to improve models for predictions, classifications, and uncovering patterns in data. AI's practical applications have expanded over the past three years, with costs dropping and accessibility increasing. Australians frequently interact with AI through online searches, shopping recommendations, and services like navigation and medical diagnostics. AI also powers customer service responses and predictive maintenance for industrial equipment. Despite its benefits, AI introduces new risks, including potential misuse. In 2022, researchers altered an AI model designed to catalogue therapeutic molecules, showing that it could generate over 40,000 potentially lethal molecules in six hours. Similarly, data poisoning can lead to harmful outputs, as seen in 2016 when a Microsoft chatbot was manipulated to produce offensive content. Cybercriminals could misuse AI for phishing, deepfake content, and even malware creation. Security researchers have demonstrated that AI can aid cyber intrusions, while defenders can also use AI for sorting data, detecting malware, and automating security tasks. When adopting AI, organizations should take a risk-based approach, ensuring the AI tool is secure, free from bias, and aligns with privacy laws. AI should support human decision-making, and oversight must be clearly assigned if issues arise.[lxiii]

According to Crowdstrike, in late 2022, generative AI became widely accessible, creating new opportunities for content creation and catching the attention of adversaries looking to exploit it. Generative AI has democratized computing, potentially lowering the barrier for less sophisticated threat actors. Two key areas where it may be used in cyber threats include developing or executing malicious computer network operations (CNO), such as creating scripts or code and enhancing social engineering and information operations campaigns. While it's difficult to assess the extent of its use in malicious CNO fully, there have been few confirmed cases of generative AI being used for such purposes in 2023. The limited visibility could be due to AI-generated content not leaving clear indicators or adversaries hiding its usage.[lxiv] In recent years, language models have advanced to generate stories and digital artwork, with Russia, China, and Iran showing interest in AI-generated deepfakes for influence operations. These predictions began to materialize in 2023. A Chinese campaign using AI-generated images gained traction on social media in September, and a hacktivist group used generative AI to create a spam tool for pro-Azerbaijan messaging.

As reported by New Zealand NCSC, with the rapid rise of technologies like generative AI, organizations looking to leverage these advancements must be ready to manage their use and address the privacy and security risks that come with their adoption.[lxv]

Truesec reports that it has observed a rise in automation within cyber attacks, with malware developers now offering complete attack frameworks via user-friendly GUIs, making it easier for less experienced individuals to conduct attacks. The hope that AI-powered chatbots would be responsibly regulated has faded. Some AI researchers are releasing chatbots specifically designed for cybercriminals trained on the dark web to assist with phishing, social engineering, vulnerability exploitation, and malware creation. A few malicious chatbots are available, helping criminals with coding problems and crafting more effective phishing emails. While

these tools may make cybercriminals more efficient, the likely impact will be faster and more effective attacks than with more advanced techniques. AI chatbots won't replace cybercriminals but will make experienced hackers quicker in executing attacks. Additionally, their use in tasks like social engineering or translation offers limited advancements over existing tools, often yielding only modest results. [lxvi]

Politically motivated attacks or hacktivism

According to ENISA Threat Landscape 2024, hacktivism has steadily expanded with the emergence of numerous new groups. Major events like national or European-level occurrences like the European Elections have motivated increased hacktivist activity during the reporting period.[lxvii]

UK NCSC reports that the global threat landscape is constantly evolving, making it critical for the NCSC, as the UK's technical cybersecurity authority, to monitor and address key threats, risks, and vulnerabilities. This year, state-aligned actors targeting critical national infrastructure (CNI), Russia's continued aggression in Ukraine, and risks from AI have heightened the need for NCSC interventions.

Key threats include:

- China: As a rising tech superpower, China poses a significant challenge to UK security. State-affiliated cyber actors use advanced capabilities to target critical infrastructure globally. The NCSC works closely with allies to address this growing cyber threat.
- Russia: Since Russia invaded Ukraine, cyber attacks, including DDoS and data wiper attacks, have targeted Ukraine. Despite this, Ukraine's resilience, supported by international partners, has mitigated the impact of these attacks.
- Iran: Iran continues aggressive cyber activities, including spear-phishing attacks and threats to individuals outside the country. The NCSC works with partners to counter these threats.
- North Korea (DPRK): North Korea uses cyber means to generate illicit revenue, evade sanctions, and strengthen its regime. Cyber thefts and attacks on institutions for financial gain and information are common.

The UK NCSC continues collaborating with the government and industry to address these global threats.[lxviii]

According to Crowdstrike, in contrast to the Russia-Ukraine war, where cyber operations played a direct role in the conflict, cyber activities in the Israel-Hamas conflict have not directly supported Hamas' military operations. While Iranian state-linked adversaries and proxies are likely involved, the full extent of their actions targeting Israel remains unclear. Identified incidents so far have not caused the major disruptions initially feared, potentially due to Iranian forces' unpreparedness or a desire to avoid escalation. CrowdStrike tracks two Iranian-aligned clusters, SpoiledMocha and Moonshuttle, connected to regional proxies like the Houthis and Hezbollah, though neither has been observed in the Israel-Hamas conflict. Pro-Iraqi Shia militia hacktivist groups have been active against Israeli entities, and further escalations could lead to more such activity, closely tied to geopolitical developments.[lxix]

In 2023, geopolitical conflicts like the Russia-Ukraine and Israel-Hamas wars drove significant hacktivist and targeted intrusion activity, especially from Iran- and Russia-linked adversaries. "Faketivists" tied to Iranian state actors and pro-Palestinian hacktivists targeted Israel's critical infrastructure and warning systems. After the October 7, 2023, outbreak of the Israel-Hamas conflict, pro-Palestinian hacktivist activity surged, with groups aiming to disrupt Israel's infrastructure and targeting countries seen as supportive of Israel. Meanwhile, no cyber activities linked to Hamas adversaries have been observed, likely due to resource or infrastructure issues.[lxx]

ACSC adds that hacktivism refers to individuals or groups that engage in malicious cyber activity to promote social or political causes, rather than for financial gain. These actors are typically less organized and resourced than other cybercriminals but can still cause significant harm through website defacements, social media hijacking, data leaks, or denial-of-service (DoS) attacks. In March 2023, the Australian Signals Directorate (ASD) reported that religiously motivated hacktivists targeted over 70 Australian organizations. Initial attacks focused on small-to-medium businesses through website defacement and DoS attacks, later escalating to critical infrastructure websites. Despite the disruptions, there was no operational impact on critical infrastructure. ASD provided support by identifying attack-related IP addresses and sharing indicators of compromise with partners.[lxxi] Technology has expanded the scope of information operations, with private contractors now systematizing the spread of information for strategic objectives. Like commercial spyware, these tools allow states and private organizations to engage in espionage. Some operations combine network exploitation, such as compromising opponents' email or social media, with inauthentic behaviour to manipulate public discourse.[lxxii]

According to Truesec, the 2022 Russian invasion of Ukraine triggered a surge in politically motivated hacking, or "hacktivism," with hackers on both sides aiming to disrupt their opponents' networks. This trend has since spread beyond the Ukraine conflict, becoming a tool for information operations globally. Sweden and Denmark have been targeted by sophisticated information operations to deepen divisions. Hacktivism has played a role in these efforts, particularly around the Quran burnings in Sweden, which were exploited by both Russia and Iran. There is also circumstantial evidence suggesting that Russia and Iran may have instigated the Quran burnings, which their proxy hacktivists then protested.[lxxiii] Hacktivism, especially through DDoS attacks, often uses rented services from criminal providers, requiring little skill. While the number of attacks hasn't increased since 2022, their intensity has, due to more powerful services. Larger groups like Anonymous Sudan are government-backed, while smaller hacktivists use basic tools. Russian hacktivism, such as KillNet, often overlaps with disinformation and cybercrime, promoting pro-Russian narratives alongside DDoS attacks.[lxxiv]

Based on the conducted analysis, the following **new threats** could be distinguished from the analysed reports:

The ENISA Threat Landscape 2024 lists CWE-798 **Use of Hard-coded Credentials** as a prominent issue, highlighting its role in facilitating unauthorized access and increasing the likelihood of system compromise. These credentials are often embedded directly into software or firmware by developers, creating an easy target for attackers. Once discovered, attackers can use these credentials to gain unauthorized access to systems, bypassing normal authentication mechanisms. This practice weakens security since the credentials are static

and not easily changeable by users or administrators, making them a persistent risk in environments where systems rely on them.[lxxv]

Out-of-bounds write attack (also known as a buffer overflow) occurs when a program writes data outside the boundaries of allocated memory. This happens due to improper validation of input data size or incorrect memory handling in the software. The vulnerability allows an attacker to overwrite adjacent memory locations with arbitrary data, which can lead to unintended behaviour, such as program crashes, corruption of data, code execution, and privilege escalation. This type of attack exploits vulnerabilities in software's memory management, typically found in programming languages like C and C++, which do not provide inherent bounds-checking for memory access. Out-of-bounds write vulnerabilities are often categorized under CWE-787 and are considered severe because they can lead to serious security breaches, including remote code execution and system compromise.[lxxvi]

Ransom Denial of Service (RDoS) is also distinguished as being on the rise. Threat actors have continued utilizing Ransom Denial of Service (RDoS) to carry out extortion-driven DoS attacks with financial motives. In an RDoS attack, vulnerable systems are identified and targeted, followed by actions that culminate in a ransom demand. There are two primary approaches to RDoS: Attack first: A DDoS attack is launched, and a ransom is demanded to halt it. Extort first: An extortion letter and proof of harm, typically a small-scale DoS attack, are sent with a ransom demand. RDoS attacks pose a greater risk than traditional DDoS attacks because they can be successful even without the attacker having significant resources. The simplicity of RDoS, combined with the use of DDoS-as-a-Service (also known as DDoS-for-Hire), has made this form of extortion more widespread. DDoS-as-a-Service allows attackers to easily initiate RDoS attacks, while making it difficult to trace their origin. In contrast, spreading malware requires more time and planning. RDoS tactics have evolved from double-extortion to quadruple-extortion. In triple-extortion, attackers encrypt and steal data, then threaten to launch a DDoS attack against the affected organization. Quadruple extortion escalates the attack further by involving business partners and clients, creating additional pressure on the victim and increasing the risk of business disruptions. According to Unit42, less than 2% of ransomware cases globally involve RDoS. Other more effective ransom attacks are preferred when the attacker's main objective is financial gain. Cloudflare also reported a decline in RDoS cases to 8% in Q3 2024. Meanwhile, Akamai noted that the gaming and gambling industries were prominent targets of DDoS attacks and triple extortion in 2023.[lxxvii]

6. CYBERSECURITY SKILLS REQUIRED TO ADDRESS IDENTIFIED THREATS

The purpose of this chapter is to map the main identified cybersecurity threats with the skills required to address the respective threats and link them with the 12 ECSF role profiles.

6.1. SKILLSKILLS AND THREATS MAPPING METHODOLOGY

The following methodology has been considered for mapping the identified threats to cybersecurity skills, according to three main axes:

- **Identification of threats and skills.** To perform this mapping, we relied on the updated list of cybersecurity threats, which was based on a comprehensive review of all threats documented in the year 2022, carefully evaluating their ongoing relevance to the current year, ensuring that they maintain their significance, and on a rigorous examination of most recent 2023 reports, meticulously sifting through their contents. It is also pertinent to emphasize that the requisite job profiles and the associated skills essential for this endeavour have already been thoughtfully detailed and provided within the scope of WP3 through the latest version of the cybersecurity skills framework.

- **Association of skills with threats.** To effectively address each identified threat, our approach involves an assessment of which precise skills are most pertinent for mitigating or countering these specific identified threats. For instance, threat analysis entails gaining deep insights into the threat's distinctive characteristics, tactics and techniques. We also delve into evaluating its potential impact, the vectors of attack and the vulnerabilities it exploits. Our methodology is firmly rooted in established best practices and practical expertise, ensuring a robust and well-informed threat migration and response strategy.

- **Assignment of weights for the mapping**. To make a systematic assessment, we have complemented the mapping by assigning numerical weightings for each skill coming from the ECSF role profiles, to quantify its significance in addressing each specific threat. These weightings are designed to accurately reflect the skill efficiency in mitigating the given cybersecurity threat. For this, we have utilized a scale ranging from 1 to 5, with a weight of 5 signifying the utmost importance and effectiveness in countering the cybersecurity threat.

6.2. MAPPING RESULTS

In this section, we detail the different tables that map the cyber threats across the three considered categories: Operational Technology (OT) Threats, Information Technology (IT) Threats, and shared Information Technology Threats, to the skills related to 12 ECSF role profiles. For clarity, we provide two tables for each threat category, the first table corresponding

to the first six role profiles and the second table corresponding to the second six role profiles from the ENISA cybersecurity skills framework. From these tables, we then elaborate on the skills that are the most relevant in addressing the identified threats and the job profiles associated with these skills. We also analyse the coverage of threats by skills for each of the three main threat categories and discuss some refinement of skills to properly address such threats.

6.2.1. OPERATIONAL TECHNOLOGY (OT) THREATS

Table 4 is a detailed reference for understanding the link between Operational Technology (OT) threats and the first 6 ECSF role profiles equipped to address them. Each cell within the table contains a curated list of skills associated with a specific job profile, highlighting the expertise required to mitigate Operational Technology (OT) cybersecurity threats effectively.

Integrating IoT devices into Operational Technology (OT) environments has heightened cybersecurity risks, as seen in a 2024 power grid attack and a 2023 manufacturing breach caused by compromised IoT devices. To mitigate these threats, it's crucial to implement cybersecurity best practices, secure network communications, and continuously assess vulnerabilities while monitoring issues and ensuring clear communication throughout the process.[lxxviii]

The mapping of skills with respect to OT threats shows the importance of several key skills from the ENISA cybersecurity skills framework. In particular, effective communication, coordination, and cooperation with internal and external stakeholders is crucial for addressing these cybersecurity threats. Ensuring seamless information sharing, and coordinating responses are essential to properly counter threats, such as those related to the cybersecurity workforce gap, the outsourcing of third parties for ICS architecture management, the remote access to the corporate network, the reliance on external servers for critical infrastructure, and the integration of IT and OT networks. Recognizing and categorizing types of vulnerabilities and their associated attacks are also required to enable proactive measures to secure such systems. Utilizing cyber threat intelligence (CTI) platforms and tools enables also staying well-informed about emerging threats and attack patterns. In addition, conducting ethical hacking, identifying and solving cybersecurity-related issues, and assessing cybersecurity vulnerabilities, contribute to addressing several others, such as those related to the vulnerabilities of ICS components, the use of outdated and obscure components and content management systems. These skills empower organizations to anticipate Operational Technology (OT) threats and manage the relevant risks in a more efficient manner.

The analysis of the first mapping reveals that all the Operational Technology (OT) threats are covered by at least two skills from the ENISA cybersecurity skills framework. In addition, some skills could be further refined to consider the threats' specificities. In particular, the threats related to the vulnerabilities of ICS components might be covered by more specific skills about the security of ICS systems, such as those linked to SCADA systems, PLCs and, more generally, to network protocols used in OT environments, contributing to a more precise response to such threats. Similarly, cybersecurity threats related to the outsourcing of third parties to manage and maintain the ICS architecture could be further covered by more refined skills on OT security frameworks and standards, as well as on specific industrial processes and technologies.

Overall, this mapping with respect to Operational Technology (OT) threats highlights, more specifically, amongst the twelve job profiles from the ENISA skills framework, the following ones: the penetration tester, the cyber threat intelligence specialist, the cybersecurity educator, the cybersecurity architect, and the cyber incident responder.[lxxix]

Table 4. The skills and knowledge required to effectively mitigate Operational Technology cybersecurity threats for the first set of the ECSF role profiles. Threats from 2024 are highlighted in bold.

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
OPERATIONAL TECHNOLOGY THREATS						
Out-of-bounds write attack	**Implement cybersecurity recommendations and best practices (weight: 4)**	**Recognize and categorize types of vulnerabilities and associated attacks (weight: 3)**			**Communicate, present and report to relevant stakeholders (weight: 4)**	
IoT Integration Risks in OT Environments	**Implement cybersecurity recommendations and best practices (weight: 4)**	**Secure network communications (weight: 4)**		**Assess risk factors (weight: 4)**		**Monitor the progress of issues throughout the lifecycle and communicate effectively (weight: 3)**
Cybersecurity workforce gap	Influence an organisation's cybersecurity culture (weight: 2.5) Motivate and encourage people (weight: 4) Guide, direct and motivate others. (weight: 4)	-	Understand, practice and adhere to ethical requirements and standards (weight: 4) Educate, monitor and assess the awareness of organization members and external parties on cybersecurity	Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4)	Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4)	Define, present and promote an information security policy for approval by the senior management of the organization (weight: 3)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
OPERATIONAL TECHNOLOGY THREATS						
			and privacy issues as needed. (weight: 5)			
Vulnerabilities of ICS components	-	Recognize and categorize types of vulnerabilities and associated attacks (weight: 3)	-	-	Use and apply CTI platforms and tools (weight: 4) Automate threat intelligence management procedures (weight: 3)	Coordinate the integration of security solutions (weight: 3.5) Monitor the progress of issues throughout the lifecycle and communicate effectively (weight: 3) Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3)
Content Management System (CMS) software	Implement cybersecurity recommendations and best practices (weight: 4)	Secure network communications (weight: 4) Manage and analyse log files (weight: 4), Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)	-	-	Coordinate the integration of security solutions (weight: 3)	-
Unpatched components	-	-	-	-	-	Plan and implement application and data provisioning (weight: 4) Monitor the progress of issues throughout the lifecycle and communicate effectively (weight: 3)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
OPERATIONAL TECHNOLOGY THREATS						
Utilizing outdated and obscure components	-	-	-	Assess risk factors (weight: 4)	-	Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3)
Outsourcing of the third parties to manage and maintain the ICS architecture	-	-	-	Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4)	Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4)	-
Remote access to the corporate network	-	-	Enforce and advocate the organisation's data privacy and protection program (weight: 4) Explain and communicate data protection and privacy topics to stakeholders and users (weight: 4)	-	Use and apply CTI platforms and tools (weight: 3)	Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
OPERATIONAL TECHNOLOGY THREATS						
Utilizing external servers for critical infrastructure architecture	-	Work on operating systems, servers, clouds and relevant infrastructures (weight: 4)	-	Communicate, coordinate and cooperate with internal and external stakeholders (weight: 2.5)	Use and apply CTI platforms and tools (weight: 4) Communicate, coordinate and cooperate with internal and external stakeholders (weight: 2.5)	-
Integration of IT and OT networks	-	Work on operating systems, servers, clouds and relevant infrastructures (weight: 4)	-	-	Use and apply CTI platforms and tools (weight: 3)	Guide and communicate with implementers and IT/OT personnel (weight: 4)

Table 5. The skills and knowledge required to effectively mitigate Operational Technology cybersecurity threats for the second set of the ECSF role profiles. Threats from 2024 are highlighted in bold.

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
OPERATIONAL TECHNOLOGY THREATS						
Cybersecurity workforce gap	Utilise existing cybersecurity-related training resources (weight: 3)	Communicate, present and report to relevant stakeholders (weight: 4)	Communicate, present and report to relevant stakeholders (weight: 4) Generate new	Communicate, present and report to relevant stakeholders (weight: 4)	-	Communicate, present and report to relevant stakeholders (weight: 4) Explain and communicate technical cybersecurity

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
OPERATIONAL TECHNOLOGY THREATS						
	Advise on appropriate solutions in the field of skills certification schemes, taking into consideration the needs of the interested parties (weight: 4) Convey complex information, concepts, or ideas effectively through verbal, written, and/or visual means and to different levels of audience (weight: 4) Gauge learner understanding and knowledge level and, provide effective feedback to students for improving learning (weight: 3)		ideas and transfer theory into practice (weight: 3) Communicate, present and report (weight: 3.5)			topics appropriately to a variety of stakeholders. (weight: 4)
Vulnerabilities of ICS components	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3)	-	-	-	Recognize and categorize types of vulnerabilities and associated attacks (weight: 2.5)	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4) Assess cybersecurity vulnerabilities (weight: 4)
Content Management System (CMS) software	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3)	-	-	-	-	Conduct ethical hacking (weight: 4) Identify and solve

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
OPERATIONAL TECHNOLOGY THREATS						
						cybersecurity-related issues (weight: 4)
Unpatched components	-	Develop code, scripts and programmes (weight: 3)	-	Build a cybersecurity risk-aware environment (weight: 2.5)	-	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4) Develop codes, scripts and programmes (weight: 3)
Utilizing outdated and obscure components	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3)	Develop code, scripts and programmes (weight: 3)	-	-	-	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Outsourcing of the third parties to manage and maintain the ICS architecture	-	-	-	-	-	-
Remote access to the corporate network	Apply network protection components and security controls (weight: 4.5)	-	Conduct network configuration and setup (weight: 4)	-	-	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Utilizing external servers for critical infrastructure architecture	-	-	-	Build a cybersecurity risk-aware environment (weight: 3)	-	-
Integration of IT and OT networks	-	-	Conduct network configuration and setup (weight: 4)	-	-	-

6.2.2. INFORMATION TECHNOLOGY (IT) THREATS

Table 6 and Table 7 provide a comprehensive mapping between Information Technology (IT) threats and the first and the second 6 ECSF role profiles. Each table cell provides a list of skills associated with a particular job profile that can be harnessed to counter the specific IT security threat outlined.

In 2024, significant cybersecurity threats emerged, including blockchain vulnerabilities and supply chain software attacks. For instance, hackers exploited a vulnerability in a decentralized finance platform's smart contract, resulting in a major cryptocurrency theft. Similarly, a supply chain attack occurred when malicious code was injected into a widely used software update, causing widespread disruptions. These incidents highlight the importance of applying security principles like least privilege and enforcing data protection to mitigate risks and enhance defences against such vulnerabilities.

The mapping of skills with respect to Information Technology (IT) threats also provides interesting elements regarding the key skills from the ENISA cybersecurity skills framework for addressing such threats. In particular, securing network communications is important to prevent multiple cybersecurity threats, including compromising communication equipment, network eavesdropping, traffic analysis, broken authentication, and man-in-the-middle attacks. Applying network protection components and security controls contributes complementarily to such prevention against DDoS attacks, POS intrusions, DNS cache poisoning, and DNS spoofing. Conducting ethical hacking, as already shown with the Operational Technology (OT) threats, enables identifying vulnerabilities at an early stage to prevent their exploitation through cybersecurity attacks, and enables addressing several threats, such as those regarding injection flaws, cross-site scripting, insecure deserialization, and more generally web application attacks and advanced persistent threats (APT). Using specific tools, techniques, and methods in relation to digital forensics helps in investing the root cause of an attack and in better quantifying its impact in link with threats such as vulnerabilities affecting mobile applications or ransomware campaigns. Skills regarding security and privacy infrastructures, technologies, and methods also permit addressing critical threats, such as privacy infringements and identity theft.

The analysis of this second mapping shows that around 75% of the Information Technology (IT) threats are covered by at least two skills from the ENISA cybersecurity skill framework. In addition, the refinement of some skills could contribute to better addressing some of the identified threats. More specifically, the threat related to large-scale attacks on IoT (medical devices) could benefit from skills more specific to medical device protection and regulations. Secure firmware development, data transmission, and lifecycle management, network segmentation, and real-time monitoring can further strengthen medical IoT devices' security. Also, the threats regarding social engineering are increased by the advances in the area of generative artificial intelligence. This requires further understanding of AI-driven social engineering tactics and better exploitation of methods and techniques for efficiently detecting and countering AI-enhanced attacks, such as advanced phishing and deepfake content. Also, the lack of protective monitoring could benefit from the efforts done in the area of software-

defined networking, with the new capabilities offered by these networking environments in terms of programmability and flexibility.

Overall, the mapping with respect to Information Technology (IT) threats highlights, more specifically, among the 12 ECSF role profiles from the ENISA skills framework, the following ones: the penetration tester, the cyber incident responder, the cybersecurity educator, the digital forensics investigator, and the chief information security officer.

Table 6. The skills and knowledge required to effectively mitigate Information technology cybersecurity threats for the first set of the ECSF role profiles. Threats from 2024 are highlighted in bold.

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
Ransom Denial of Service	**Implement cybersecurity recommendations and best practices (weight: 3)**				**Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4)**	**Conduct ethical hacking (weight: 4)** **Identify and solve cybersecurity-related issues (weight: 2)**
Use of Hard-coded Credentials	**Apply security design principles, e.g. least privilege (weight: 3)**		**Enforce and advocate the organisation's data privacy and protection program (weight: 4)**			**Dealing with problems (weight: 4)**
Exploitation of Blockchain Vulnerabilities	**Apply security design principles, e.g. least privilege (weight: 3)**	**Protect a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters) (weight: 4)**	**-**	**-**	**Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)**	**-**
Supply Chain Software Vulnerabilities	**Implement cybersecurity recommendations**	**-**	**Enforce and advocate the organisation's data privacy and protection program (weight: 4)**	**-**	**-**	**Dealing with problems (weight: 3)** **Monitor the progress of issues throughout**

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
	and best (weight: 3.5)					**the lifecycle and communicate effectively (weight: 4)**
AI (Artificial Intelligence) and generative AI-enabled	Apply security design principles, e.g. least privilege (weight: 3)	- Secure network communications (weight: 4)	-	-	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)	-
Malware exploits	-	Protect a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters) (weight: 4)	-	-	-	Monitor the progress of issues throughout the lifecycle and communicate effectively (weight: 3)
Ransomware	-	-	-	-	-	-
Privacy Infringement	Implement cybersecurity recommendations and best practices (weight: 3)	-	Enforce and advocate the organisation's data privacy and protection program (weight: 4) Explain and communicate data protection and privacy topics to stakeholders and users (weight: 4)	-	-	-
Identity theft	Implement cybersecurity recommendations and	-	Enforce and advocate organisation's data privacy and protection program (weight: 4)	-	-	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
	best practices (weight: 3)					
Compromising of communication equipment	-	Secure network communications (weight: 3)	-	-	-	-
Web applications attack	-	-	-	-	-	Plan and implement application and data provisioning (weight: 3)
Vulnerabilities in Mobile Applications and payment interfaces	Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 3)	Secure network communications (weight: 3)	-	-	-	-
Data Confidentiality, Integrity and Availability	-	Secure network communications (weight: 3)	Enforce and advocate the organisation’s data privacy and protection program (weight: 4.5)	Follow and practice auditing frameworks, standards and methodologies (weight: 4)	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)	Dealing with problems (weight: 3) Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3)
Eavesdropping and traffic analysis	-	Secure network communications (weight: 4)	-	-	-	-
DDoS	-	-	-	-	-	-
Social Engineering	Implement cybersecurity	-	-	-	-	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
	recommendations and best practices (weight: 3)					
POS intrusions	Apply security design principles, e.g. least privilege (weight: 3)	-	-	-	-	-
Miscellaneous errors	-	-	-	-	-	-
Lack of protective monitoring	-	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3.5)	-	-	-	Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 2.5)
Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)	Apply security design principles, e.g. least privilege (weight: 4)	-	-	-	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)	-
Large-scale attacks on IoT (medical devices)	Apply security design principles, e.g. least privilege (weight: 2.5)	-	-	-	-	-
Advanced Persistent Threats (APT)	-	Recognize and categorize types of vulnerabilities		-	-	Dealing with problems (weight: 2.5)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
		and associated attacks (weight: 3)				
Intellectual property theft	Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 3)	-	Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties (weight: 4) Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, aligning with the relevant audit plan(s). (weight: 3)	-	-	-
Denial of Service (Dos)	-	-	-	-	-	Conduct performance and resilience testing (weight: 4) Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
DNS Cache Poisoning	-	-	-	-	-	-
DNS Spoofing	-	-	-	-	-	-
Cybersquatting	-	-	-	-	-	-
Typosquatting	-	-	-	-	-	-
Adapting to risks from advances in employee computing technologies (e.g., increased prevalence of sensors, AI, etc.)	-	-	Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties (weight: 4)	Apply auditing tools and techniques (weight: 3)	-	-
Injection flaws	-	-	-	-	-	-
Broken authentication	-	Secure network communications (weight: 3.5)	-	-	-	Plan and implement application and data provisioning (weight: 2.5)
Broken access control	Apply security design principles, e.g. least privilege (weight: 2.5)	Secure network communications (weight: 4)	-	-	-	-
Cross-site scripting (XSS)	-	-	-	-	-	-
Man-in-the-middle attacks	-	Secure network communications (weight: 4)	-	-	-	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
INFORMATION TECHNOLOGY THREATS						
XML external entities (XXE)	-	-	-	-	-	-
Cryptojacking	-	-	-	-	-	-
Watering hole	-	-	-	-	-	-
Living off the land (LOTL)	-	-	-	-	-	-
Insecure deserialization	-	-	-	-	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3.5)	-

Table 7. The skills and knowledge required to effectively mitigate Information technology cybersecurity threats for the second set of the ECSF role profiles

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
AI and generative AI-enabled	-	-	-		-	-
Malware exploits	-	-	-	-	-	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 3.5)
Ransomware	-	-	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3)	-
Privacy Infringement	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 4)	-	Decompose and analyse systems to develop security and privacy requirements (weight: 3)	Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks (weight: 3.5)	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3)	-
Identity theft	Monitor evolving security and privacy infrastructures, technologies	-	Decompose and analyse systems to develop security and	Enable business assets owners, executives and other stakeholders to	-	-

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
	and methods (weight: 4)		privacy requirements (weight: 3)	make risk-informed decisions to manage and mitigate risks (weight: 3.5)		
Compromising of communication equipment	-	-	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 4)	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Web applications attack	-	-	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 4)	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Vulnerabilities in Mobile Applications and payment interfaces	-	-	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight:3)	Conduct ethical hacking (weight:3) Identify and solve cybersecurity-related issues (weight: 3) Assess cybersecurity vulnerabilities (weight: 4)
Data Confidentiality, Integrity and Availability	Monitor evolving security and privacy	-	Decompose and analyse systems to develop security and	-	-	-

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
	infrastructures, technologies and methods (weight: 4)		privacy requirements and identify effective solutions (weight: 3)			
Eavesdropping and traffic analysis	-	-	-	-	-	Develop codes, scripts and programmes (weight: 2)
DDoS	Apply network protection components and security controls (weight: 4)	-	-	-	-	-
Social Engineering	Apply network protection components and security controls (weight: 2.5)	-	-	-	-	Perform social engineering (weight: 4)
POS intrusions	Apply network protection components and security controls (weight: 3)	-	-	-	Work ethically and independently; not influenced and biased by internal or external actors (weight: 4)	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Miscellaneous errors	-	-	Identify effective solutions (weight: 3)	-	-	-
Lack of protective monitoring	-	-	-	-	-	-
Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)	-	-	-	-	-	-

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
Large-scale attacks on IoT (medical devices)	-	-	-	-	-	-
Advanced Persistent Threats (APT)	-	-	-	-	-	-
Intellectual property theft	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3)	-	Decompose and analyse systems to develop security and privacy requirements (weight: 4)	-	-	-
Denial of Service (Dos)	Apply network protection components and security controls (weight: 3)	Conduct network configuration and setup (weight: 3)	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 2.5)	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
DNS Cache Poisoning	Apply network protection components and security controls (weight: 3)	Conduct network configuration and setup (weight: 3)	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3)	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 3.5)
DNS Spoofing	Apply network protection components and security controls (weight: 3)	-	-	-	Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
					traces, logs, malware analysis, protocols, operating systems, etc) (weight: 2.5)	
Cybersquatting	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Typosquatting	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Adapting to risks from advances in employee computing technologies	-	-	-	Use monitoring tools to measure and evaluate the effectiveness of implemented cybersecurity controls and the achieved security levels. (weight: 3.5)	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Injection flaws	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Broken authentication	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
						cybersecurity-related issues (weight: 4)
Broken access control	-	Conduct network configuration and setup (weight: 3)	-	-	-	Conduct ethical hacking (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Cross-site scripting (XSS)	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Man-in-the-middle attacks	-	Conduct network configuration and setup (weight: 3)	-	-	-	-
XML external entities (XXE)	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)
Cryptojacking	-	-	-	-	-	Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3) Conduct ethical hacking (weight: 3)
Watering hole	-	-	-	-	-	Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3) Conduct ethical hacking (weight: 3)

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
INFORMATION TECHNOLOGY THREATS						
Living off the land (LOTL)	-	-	-	-	-	Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3) Conduct ethical hacking (weight: 3)
Insecure deserialization	-	-	-	-	-	Conduct ethical hacking (weight: 3) Identify and solve cybersecurity-related issues (weight: 4)

6.2.3. SHARED INFORMATION TECHNOLOGY THREATS

Tables 8 and 9 offer a detailed mapping between Shared-IT threats ECSF role profiles. Within each table cell, a compilation of skills attributed to a specific job profile is provided, illustrating how these skills can effectively address and mitigate the Shared-IT security threats at hand.

Cloud misconfigurations have emerged as a critical threat in 2024, with significant consequences highlighted by two major Microsoft incidents. In July, a faulty Azure configuration caused a major Microsoft 365 outage, disrupting services like Teams and OneDrive across the US. A subsequent global outage in August further underscored the impact of cloud misconfigurations, affecting users worldwide. This came on the heels of the April Paris Olympics, where fiber optic lines were sabotaged, leading to widespread disruptions. To mitigate such risks, it is essential to monitor evolving security infrastructures, manage and analyze log files, correlate cyber threat information, assess risk factors, and conduct thorough performance and resilience testing.

The mapping of skills with respect to Shared IT threats also highlights several major skills from the ENISA cybersecurity skills framework. In particular, following and practising auditing frameworks, standards and methodologies are essential for enforcing the security policy and maintaining secure and resilient infrastructures. This is required to properly address several cybersecurity threats, such as those affecting the supply chain or related to insider attacks. Collecting, analysing and correlating cyber threat information originating from multiple sources is also critical to address the lack of information sharing as well as deficiencies that may exist in incident reporting activities. It may also address threats regarding third-party attacks or prevent some breakdowns due to cybersecurity attacks. Coordinating the integration of security solutions is also a key requirement to guarantee the seamless integration of prevention, detection, and mitigation methods and techniques used in an organization and minimise the surface of attack on network infrastructures. Educating, monitoring and assessing the awareness of organization members and external parties on cybersecurity and privacy issues is another important factor contributing to preventing low awareness concerning security risks, and threats regarding compromised confidential or personal data. Analyzing and consolidating an organization's quality and risk management practices is another factor contributing to addressing threats with respect to resilience. These threats should also be addressed by regularly conducting performance and resilience tests to quantify an organisation's capabilities (technical and non-technical) to resist successful attacks.

The analysis of this third mapping shows a relatively high coverage, with more than 80% of the shared Information Technology threats covered by at least two skills from the REWIRE skill framework. Again, some of the considered skills could be refined with respect to the specificities of cybersecurity threats. For instance, the threat of falsified and stolen medical data may require some refinements about medical information systems and their security, but also, more generally, about specific healthcare regulations. This contributes to a better handling of risks related to data falsification and data theft in a medical context. Similarly, the threats regarding geopolitical instability risk could involve further specific skills with respect

to monitoring and analysing geopolitical events, complying with international cybersecurity regulations, and even engaging in cyber diplomacy to mitigate inherent risks.

Overall, this mapping with respect to shared Information Technology threats highlights more specifically, amongst the 12 role profiles from the REWIRE skills framework, the following ones: the chief information security officer, the cyber threat intelligence specialist, the cyber-security implementer, the cybersecurity auditor, and the cybersecurity implementer.

Table 8. The skills and knowledge required to effectively mitigate Shared-IT threats for the first set of the ECSF role profiles. Threats from 2024 are highlighted in bold.

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
Critical Infrastructure sabotage	**Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 4)**	-	-	**Assess risk factors (weight: 4)**	-	**Conduct performance and resilience testing (weight: 5)**
Cloud Misconfigurations	**Monitor evolving security and privacy infrastructures, technologies and methods (weight: 4)**	**Manage and analyse log files (weight: 3)** **Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)** **Develop code, scripts and programmes (weight: 4)**	-	**Assess risk factors (weight: 4)**	-	**Conduct performance and resilience testing (weight: 4.5)**
Politically motivated attacks or hacktivism	-	Recognize and categorize types of vulnerabilities and associated	-	Assess risk factors (weight: 4)	Collect, analyse and correlate cyber threat information	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
		attacks (weight: 4)			originating from multiple sources (weight: 4)	
Unpatched & outdated software	-	-	-	-	-	Coordinate the integration of security solutions (weight: 3) Monitor the progress of issues throughout the lifecycle and communicate effectively (weight: 3)
Low awareness	-	-	Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. (weight: 4)	-	-	-
Lack of incident reporting	-	Manage and analyse log files (weight: 3) Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3)	-	-	-	-
Lack of information sharing	-	Manage and analyse log files (weight: 3) Collect, analyse and correlate cyber threat	-	-	-	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
		information originating from multiple sources (weight: 3)				
Insider threats	Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 4)	-	-	-	-	-
Risks of emerging technologies like blockchain, AI, VR, quantum computing, intelligent automation, etc	Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams (weight: 4) Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks (weight: 4)	-	Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results in alignment with the relevant audit plan(s). (weight: 4)	Assess risk factors (weight: 4)	-	Coordinate the integration of security solutions (weight: 3)
Keeping up with changing regulatory requirements (e.g. GPDR, AI regulations, breach disclosure	Assist in communication of the enterprise architecture and standards, principles and	-	Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed	Follow and practice auditing frameworks, standards and	-	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
requirements etc.), or their ineffectiveness	objectives to the application teams (weight: 3) Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks (weight: 4)		evidence and document audit information and results, in alignment with the relevant audit plan(s) (weight: 4)	methodologies (weight: 4) Assess risk factors (weight: 3)		
Misinformation and disinformation sowing confusion among executives and the board about cyber risks	Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks (weight: 4)	Recognize and categorize types of vulnerabilities and associated attacks (weight: 3)	-	Follow and practice auditing frameworks, standards and methodologies (weight: 3)	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4)	-
Security misconfiguration	Apply security design principles, e.g. least privilege (weight: 4)	-	-	-	-	-
Third party related attacks	Implement cybersecurity recommendations and best practices (weight: 4)	-	-	-	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4) Automate threat	-

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
					intelligence management procedures (weight: 3)	
Infrastructure breakdown due to cyberattack		Work on operating systems, servers, clouds and relevant infrastructures (weight: 4)	-	Follow and practice auditing frameworks, standards and methodologies (weight: 3) Assess risk factors (weight: 4)	Automate threat intelligence management procedures (weight: 3)	Conduct performance and resilience testing (weight: 4)
Geopolitical instability risk	Apply security design principles, e.g. least privilege (weight: 4)	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4)	-	Follow and practice auditing frameworks, standards and methodologies (weight: 3)	-	-
Supply-chain resilience	Apply security design principles, e.g. least privilege (weight: 4)	Work on operating systems, servers, clouds and relevant infrastructures (weight: 2.5)	Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results,	Assess risk factors (weight: 4)	Use and apply CTI platforms and tools (weight: 3)	Conduct performance and resilience testing (weight: 4.5)

Identified threats	CHIEF INFORMATION SECURITY OFFICER (CISO)	CYBER INCIDENT RESPONDER	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	CYBER SECURITY AUDITOR	CYBER THREAT INTELLIGENCE SPECIALIST	CYBERSECURITY ARCHITECT
Shared-IT threats						
			in alignment to the relevant audit plan(s). (weight: 4)			
Blackmail due to compromised personal data	-	-	Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. (weight: 3) Enforce and advocate organisation's data privacy and protection program (weight: 4)		Coordinate the integration of security solutions (weight: 3)	-
Falsified or stolen medical data	-	-	-	Follow and practice auditing frameworks, standards and methodologies (weight: 3)	Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4)	-

Table 9. The skills and knowledge required to effectively mitigate Shared-IT threats for the second set of the ECSF role profiles

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
Shared IT threats						
Politically motivated attacks or hacktivism	-	-	-	Communicate, present and report to	-	Perform social engineering (weight: 3)

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
Shared IT threats						
				relevant stakeholders (weight: 4)		
Unpatched & outdated software	-	Develop code, scripts and programmes (weight: 4)	-	-	-	Develop code, scripts and programmes (weight: 4)
Low awareness	-	-	-	-	-	-
Lack of incident reporting	-	Communicate, present and report to relevant stakeholders (weight: 4)	-	Communicate, present and report to relevant stakeholders (weight: 4)	Collect information while preserving its integrity (weight: 4) Strictly and systematically follow the prescribed procedures. (weight: 3)	-
Lack of information sharing	-	Communicate, present and report to relevant stakeholders (weight: 4)	-	Communicate, present and report to relevant stakeholders (weight: 4)	Collect information while preserving its integrity (weight: 4) Strictly and systematically follow the prescribed procedures. (weight: 3)	-
Insider threats	Monitor evolving security and	Performs basic risk assessments for	-	Build a cybersecurity risk-aware	Work ethically and	-

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
Shared IT threats						
	privacy infrastructures, technologies and methods (weight: 4)	small information systems. (weight: 3)		environment (weight: 4)	independently; not influenced and biased by internal or external actors (weight: 4)	
Risks of emerging technologies like blockchain, AI, VR, quantum computing, intelligent automation, etc	-	Assess the security and performance of solutions (weight: 3)	-	Build a cybersecurity risk-aware environment (weight: 4)	-	-
Keeping up with changing regulatory requirements (e.g. GPDR, AI regulations, breach disclosure requirements etc.), or their ineffectiveness	-		-	-	-	-
Misinformation and disinformation sowing confusion among executives and the board about cyber risks	-	-	-	Identify sources of information that can be used for monitoring and measurement of cybersecurity controls. (weight: 2.5)	-	-

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
Shared IT threats						
Security misconfiguration	-	Conduct network configuration and setup (weight: 3)	-	-	-	Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 4) Identify and solve cybersecurity-related issues (weight: 4)
Third-party-related attacks	-	-	-	-	-	-
Infrastructure breakdown due to cyberattack	-	Contribute to the identification of risks that arise from potential technical solution architectures. (weight: 3) Suggest alternate solutions or countermeasures to mitigate risks. (weight: 3) Define secure systems configurations in compliance with intended architectures (weight: 4)	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions (weight: 3)	Oversee and control the implementation of prevention, security, and surveillance measures to assess their effectiveness and to make adjustments in case of unsatisfactory results. (weight: 4)	-	Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 4)
Geopolitical instability risk	-	-	-	Analyse and consolidate the organisation's quality and risk management practices (weight: 3)	Recognize and categorize types of vulnerabilities and associated	Assess cybersecurity vulnerabilities (weight: 3)

Identified threats	CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	CYBERSECURITY RISK MANAGER	DIGITAL FORENSICS INVESTIGATOR	PENETRATION TESTER
Shared IT threats						
					attacks (weight: 3)	
Supply-chain resilience	-	-	-	Analyse and consolidate the organisation's quality and risk management practices (weight: 3.5)	-	Assess cybersecurity vulnerabilities (weight: 3)
Blackmail due to compromised personal data	-	-	-	-	-	Identify and solve cybersecurity-related issues (weight: 3)
Falsified or stolen medical data	Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3)	-	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions (weight: 3)	-	-	-

To sum up, this chapter has systematically aligned the predominant cybersecurity threats with the requisite skills delineated across the 12 ECSF role profiles. This mapping not only clarifies the direct relationships between emerging threats and the specific skill sets needed to counteract them but also reinforces the strategic importance of continuous skills development in the cybersecurity domain. The insights generated from this analysis are crucial for developing a proactive and resilient cybersecurity workforce, capable of adapting to the rapidly evolving digital threat landscape.

CONCLUSIONS

The third annual Cybersecurity Skills Trends Report highlights several key insights into addressing the growing cybersecurity skills gap.

- The Cybersecurity Job Ads Analyzer, leveraging machine learning to analyze job ads across Europe, has proven to be an effective tool for mapping critical skills and competencies needed in the market. By aligning these skills with the ENISA framework, the Analyzer offers a comprehensive understanding of the evolving demands for roles like Cybersecurity Architect and Cyber Incident Responder, helping stakeholders track high-demand profiles over time.
- The REWIRE stakeholder's survey provided insight into the demand for cybersecurity skills, revealing the importance of certifications, cyber ranges, and targeted training programs. Despite the continued shortage of certified professionals, organizations are strongly committed to investing in employee training. High-demand roles include Chief Information Security Officers and Cybersecurity Architects, with key skills in business continuity, data privacy, and incident management remaining critical across regions.
- A detailed mapping of skills for addressing Operational Technology (OT) threats underscores the rising risks posed by IoT integration, exemplified by notable incidents in 2023 and 2024. Skills such as cyber threat intelligence, ethical hacking, and vulnerability assessments are essential to mitigate OT risks. The analysis shows that while ENISA skills cover most OT threats, some specific areas, such as ICS vulnerabilities, could benefit from further refinement.
- For IT threats, incidents such as blockchain vulnerabilities and supply chain attacks in 2024 emphasize the need for competencies in securing network communications, applying security controls, and conducting ethical hacking. While 75% of IT threats are covered by ENISA skills, refining certain competencies—such as those related to IoT security and AI-driven social engineering—could improve defenses.
- In dealing with Shared-IT threats, cloud misconfigurations, such as the Microsoft outages in 2024, highlight the critical need for auditing standards, threat analysis, and integrated security solutions. Over 80% of these threats are addressed by REWIRE skills, though some areas, like medical data theft, may require more specialized skills. Key roles in tackling Shared-IT threats include Chief Information Security Officers, cyber threat intelligence specialists, cybersecurity auditors, and implementers.

Overall, the report underscores the need for continued refinement of cybersecurity skills frameworks, investment in training, and a collaborative effort across sectors to address the evolving landscape of cyber threats.

REFERENCES

[i] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[ii] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[iii] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[iv] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[v] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[vi] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[vii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[viii] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[ix] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[x] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xi] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xii] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xiii] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xiv] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[xv] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xvi] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[xvii] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[xviii] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[xix] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

[xx] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[xxi] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xxii] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xxiii] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxiv] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxv] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxvi] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xxvii] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xxviii] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[xxix] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[xxx] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[xxxi] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxxii] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxxiii] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xxxiv] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xxxv] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xxxvi] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[xxxvii] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[xxxviii] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;

[xxxix] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[xl] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xli] Sophos 2024 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xlii]
[xliii] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[xliv]
[xlv] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[xlvi] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[xlvii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[xlviii] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xlix] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[l] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[li] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[lii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[liii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[liv] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lv] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[lvi] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[lvii] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[lviii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/

[lix] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[lx]
[lxi] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[lxii] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[lxiii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[lxiv] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxv] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[lxvi] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[lxvii]
[lxviii] United Kingdom National Cyber Security Centre Annual Review 2023, https://www.ncsc.gov.uk/collection/annual-review-2023
[lxix] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxx] The CrowdStrike 2024 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxi] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[lxxii] New-Zealand National Cyber Security Centre report 2022/2023, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf
[lxxiii] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[lxxiv] Truesec Threat Intelligence Report 2024, https://insights.truesec.com/hub/report/truesec-threat-intelligence-report-2024 ;
[lxxv] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[lxxvi] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[lxxvii] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[lxxviii] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[lxxix] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024