CyberHubs

Cybersecurity Skills Needs Analysis report Slovenia.

Co-funded by
the European Union

About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

Full partners

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | Athens University of Economics and Business | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | SEPE | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Associated partners

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union

Cybersecurity Skills Needs Analysis report - Slovenia, 2024, final version.

Deliverable D2.1: “Cybersecurity skills mismatches analysis”.

Authors: Andreja Lampe (ZIT), Ines Vlahović (ZIT), Tomaž Čebela (ZIT), dr. Muhamed Turkanović (UM FERI), Nika Jeršič (UM FERI)

Editors/Reviewers: Marie Montaldo (DE), Paul Aertsen (Breyer Publico)

Revision History			
Version	**Date**	**Modified by**	**Version**
0.1	15/07/2024	Ines Vlahović (ZIT), Tomaž Čebela (ZIT), Muhamed Turkanović (UM FERI), Nika Jeršič (UM FERI)	Draft version
0.2	04/10/2024	Ines Vlahović (ZIT), Andreja Lampe (ZIT), Muhamed Turkanović (UM FERI), Nika Jeršič (UM FERI)	Ready for a review
0.3	09/10/2024	Marie Montaldo (DE)	Review
0.4	22/10/2024	Ines Vlahović (ZIT), Nika Jeršič (UM FERI)	Updates based on the feedback
0.5	25/10/2024	Paul Aertsen (Breyer Publico)	Final review
1	28/10/2024	Ines Vlahović (ZIT)	Initial published version

Table of contents

List of Tables

List of Charts

Executive Summary

Introduction

This document provides a detailed analysis of the current state and future needs of cybersecurity skills and roles in Slovenia. It synthesizes data from various sources to offer a comprehensive understanding of the status, gaps and opportunities in the Slovenian cybersecurity workforce.

Objective

The primary aim of this report is to analyse and understand the cybersecurity skills landscape in Slovenia. By leveraging data from desk research, questionnaires, job vacancy analysis, and expert panels, the document identifies critical mismatches between the supply and demand of cybersecurity skills in the country. Additionally, the findings will contribute to the development of a tailored Cybersecurity skills strategy for the country, addressing both current and future needs for cybersecurity roles and the existing educational offerings.

Approach

The report was developed using a mixed-methods approach, combining detailed desk research on demand and supply, an analysis of job vacancies, a comprehensive questionnaire distributed to key stakeholders, and insights gathered from experts. Each phase of the research provided data that was analysed to form the overall conclusions. The methodology adopted in this study encompasses several key components. First, an extensive review of relevant literature, including scientific publications, labour market reports, and databases, was undertaken to identify essential cybersecurity roles and skill sets. Second, a detailed analysis of job postings was carried out to gauge the market demand for cybersecurity professionals. Third, data was collected from industry stakeholders via comprehensive questionnaires, focusing on both current and anticipated future requirements for cybersecurity skills. Fourth, a supplementary review of the available educational programs and training opportunities in the cybersecurity domain was conducted. Lastly, expert panels were convened to explore emerging trends and provide validation for the quantitative findings. The entire approach is aligned with European frameworks, notably the European Cybersecurity Skills Framework (ECSF), which serves as a valuable guide for outlining the critical missions, tasks, and competencies required of cybersecurity professionals. This structured approach ensures a robust foundation for profiling the most in-demand skills and knowledge within the field.

Results

The study revealed a significant shortage of cybersecurity professionals, skills and educational programs. The introduction of new regulations, such as the NIS-2 directive, is expected to increase the demand for cybersecurity professionals, compounding the current gap. Additionally, the rise of remote job postings and the acquisition of Slovenian ICT companies by foreign owners is exacerbating the local talent shortage. s.

The key findings are:

- **Cybersecurity role gaps and needs:**
  - There is a significant shortage of cybersecurity professionals in Slovenia, particularly in critical roles like Cybersecurity Implementer/Expert, (Chief) Information Security Officer/ Manager, Incident responder and Penetration Tester.
  - Specialized roles like Digital forensics investigator and Cybersecurity auditor are also in rising demand, but there is a lack of niche expertise to fill these roles.
  - The industry's lack of awareness about the benefits of specialized roles in non-ICT companies contributes to the overall shortage of versatile and highly skilled cybersecurity professionals.
- **Cybersecurity, IT related, soft and organizational skills gaps and needs:**
  - There is a growing demand for both cybersecurity skills and IT-related skills.

    - Gaps are also identified in organizational and soft skills, which are essential for integrating cybersecurity into broader business practices.
- **Training and educational deficiencies:**
    - Companies are inclined to upskill internal employees.
    - Despite the presence of educational programs, there is a noticeable gap in advanced and niche cybersecurity training, particularly in fields like AI-driven cybersecurity and legal compliance.
    - Lifelong learning programs are identified as critical for staying ahead in cybersecurity, but current offerings remain insufficient.

Conclusions

The study identifies several key challenges and opportunities for addressing Slovenia's cybersecurity skills gap. The following conclusions highlight the urgent need for targeted education and training, the importance of lifelong learning and industry collaboration, and the roles that should be prioritized for future development to ensure a sustainable cybersecurity workforce in the country.

Key roles for future development: The Cybersecurity Implementer/Expert, (Chief) Information Security Officer/ Manager, Incident responder and Penetration Tester roles remain the most critical for immediate focus due to the consistent growth in demand. At the same time, specialized roles such as Cybersecurity auditor, Cyber threat intelligence Specialist, and Digital forensics investigator should also be prioritized for long-term skill development.

Urgency to address skills gaps: The study confirms the urgent need to address the cybersecurity skills gap in Slovenia. The focus should be on creating targeted education and training programs that address both technical and soft skills, which are crucial for effective cybersecurity operations in both ICT and non-ICT companies.

Strategic focus on lifelong learning: Lifelong learning programs need to be expanded and refined to ensure they are keeping up with the latest technological developments and emerging threats.

Recommendations for industry collaboration: The findings suggest that collaboration between industry and educational institutions is essential. A coordinated effort is needed to ensure that training programs meet real-world demands, both in terms of immediate job needs and future skill trends. Policymakers and educational institutions must work together to increase the availability of specialized training programs and ensure that future professionals are well-equipped to tackle the growing challenges of the cybersecurity landscape. Establishing a national CyberHub is essential for collaboration and developing a long-term, sustainable cybersecurity workforce.

1 Introduction

1.1 Cybersecurity skills in Slovenia

In Slovenia, cybersecurity has become an increasingly important topic, particularly following recent cyberattacks on the websites of Slovenian ministries and numerous cases of personal cyber fraud. These incidents have raised public awareness of the potential damage cyber threats can cause and highlighted the importance of cybersecurity, even for non-IT companies.

However, there is a significant shortage of cybersecurity professionals, and as a result, most cybersecurity services are provided by IT companies with specialized expertise. The biggest challenge the industry is facing is the lack of skilled personnel. Although a few training companies and universities offer cybersecurity courses, the number of available spots each year is limited, making it difficult to meet current and future demands. Another challenge is that these educational programs have only been available for a few years, which is why many companies have resorted to training their own employees to develop cybersecurity expertise.

As a result, the current focus is predominantly on developing technical skills and knowledge, with less emphasis on organizational and soft skills. On the other hand, students who pursue cybersecurity education typically secure jobs even before completing their studies, largely due to strong collaborations between universities and IT companies.

There are organizations actively promoting cybersecurity among young people and raising awareness of the growing need for talent in this field. However, there is currently no central body that unites all companies and associations under one umbrella to address cybersecurity skills development comprehensively.

1.2 Research approach

The project involved a comprehensive research process focused on both the demand and supply of cybersecurity skills, incorporating job vacancy analysis, a questionnaire, and input from an expert panel. After completing each phase of desk research, the gathered data was carefully analysed to form the foundation for the overall conclusions. This analysis provided critical insights into the alignment between the current and future needs for cybersecurity professionals and the availability of relevant education and training programs.

The research methodology was aligned with the well-established European Cybersecurity Skills Framework (ECSF) and applied a multi-method approach. This included both quantitative and qualitative data collection from various sources, with the primary aim of identifying current and emerging requirements for cybersecurity roles and skills within Slovenia. The approach mirrors the methodology that was used in other European countries, such as Belgium, Estonia, Greece, Hungary, Lithuania, and Spain, which are part of the CyberHubs initiative.

The findings of this gap analysis are crucial for informing national cybersecurity strategies. By pinpointing where the supply of education and training falls short of meeting future needs, this research supports the development of targeted country-specific strategies that align future learning programs with the evolving demands for cybersecurity skills.

1.3 Reading guide

This document compiles data from each research section, with conclusions drawn for each area. An overall conclusion is then formulated, integrating insights from all sections.

2 Desk research (demand)

This chapter is about the desk research on the demand for roles and skills needed by organisations in Slovenia. The findings highlight the increasing demand for specialized roles and a wide array of technical and soft skills needed to meet the challenges posed by digital transformation and cybersecurity threats. This chapter sets the stage for a comprehensive understanding of the key drivers shaping the cybersecurity workforce in Slovenia.

2.1 Data collection

The data collection process involved a comprehensive search using mostly Slovenian institutional repositories from universities and government bodies, such as IKTHM, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), NIO, DKUM and DKUL. The selected items include a mix of internal documents from organizations, national cybersecurity reports, academic theses, and strategic frameworks, presented in table 1. This diverse selection ensures a well-rounded understanding of the evolving demands and requirements in the cybersecurity field.

Data collection in numbers	
Literature	14 papers/ articles included in analysis
Labour market desk research	21 labour market reports
Labour market databases	11 labour market databases

Table 1: Data collection in numbers.

2.2 Overview of the national context

In this section various facets that characterize the national context relevant to the study were explored. Each aspect includes several topics, though the list is not exhaustive, and other pertinent topics can be incorporated as needed.

2.2.1 Politics and agencies

The government is actively engaged in bolstering national cybersecurity through a comprehensive strategy. A national strategy for cybersecurity (slv. Strategija kibernetske varnosti) is in place, complemented by a digital strategy that encompasses cybersecurity (slv. Digitalna Slovenija 2030).

Several key actors are involved in the national cybersecurity landscape. The primary public organizations include:

1. **URSIV:** The established national cybersecurity authority.
2. **SI-CERT:** The existing and operational Computer Emergency Response Team.
3. **Ministry of Defence (MORS):** Includes a dedicated cybersecurity department and the newly established Cyber Range.
4. **SeKV:** A relevant body in the cybersecurity domain, connecting ICT companies offering cybersecurity expertise and cybersecurity experts.
5. **Universities:** Engage in cybersecurity research and education, like University of Maribor, University of Ljubljana, University of Primorska and Gea college.
6. **EDIH:** European Digital Innovation Hubs, contributing to the cybersecurity ecosystem.

There are significant national campaigns, foundations and initiatives in the field of cybersecurity:

- **Women4Cyber Slovenia**, aimed at promoting the involvement of women in the cybersecurity field.
- **SICEH**, association of Slovenian certified ethical hackers,
- **Kibertalent**, promoting cybersecurity for younger generations

Funding opportunities are available, particularly through ARIS (Public Agency for Scientific Research and Innovation of the Republic of Slovenia) project calls focused on cybersecurity themes, including the Targeted Research Programs (CRP) financed by ARIS in collaboration with MORS or URSIV.

2.2.2 Laws and regulations

The regulatory landscape for cybersecurity in Slovenia is shaped by both national and European legislation.

National Legislation

1. **ZInfV (2018)**: The Information Security Act, enacted in 2018, is a cornerstone of national cybersecurity regulation.
2. **ZInfV-1:** A new law specifically addressing critical infrastructure protection is currently being prepared that Is based on NIS2 directive.
3. **Indirectly Related Legislation**:
    - **ZVOP2**: The Personal Data Protection Act, which aligns with GDPR.
    - **ZEPEP**: The Act on the Protection of Critical Infrastructures.
    - **ZEKOM2**: The Electronic Communications Act, which also touches upon cybersecurity aspects.

Implementation of EU Legislation

Slovenia ensures that European Union regulations are transposed and implemented at the national level. Until specific national laws are enacted, EU regulations are directly applicable and provide the regulatory framework. Once national laws are developed, they often expand upon and elaborate these EU directives and regulations to fit the national context.

2.2.3 Market

Slovenian cybersecurity market consists of both large and smaller providers. In total, 84 companies from the IT sector are recorded to provide, implement or develop services and products from the field of cybersecurity. Table 2 presents the percentage of IT services offered by recorded companies. Many companies involved in cybersecurity are from the IT services sector, representing 33.33% of the total. These companies provide various IT services that include cybersecurity as a critical component of their offerings. The IT solutions sector follows, accounting for 19.44% of the companies. These firms primarily focus on developing and implementing secure IT infrastructures and systems. Telecommunications companies make up 8.33% of the market. These companies typically offer secure communication services and managed security services to their customers. IT consulting firms, comprising 5.56% of the market, provide strategic advice on cybersecurity risk management and policy development. Other sectors such as IT and telecommunications, cybersecurity consulting, IT and electronics, IT and consulting, cryptocurrency, research and education, quality and security certification, industrial services, IT and authentication, cybersecurity solutions, IT and appliances, IT and document management, research and development, management consulting, IT and design, healthcare technology, software development, and IT and software development each represent 34.34% of the market. These sectors contribute to the overall diversity and specialization within the cybersecurity landscape.

Industry	Percentage (%)
IT Services	33.33%
IT Solutions	19.44%
Telecommunications	8.33%
IT Consulting	5.56%
Other	34.34%

Table 2: Percentage of IT services offered by recorded companies.

In terms of offering cybersecurity services, presented in table 3, a significant portion of companies, 11.11%, specialize in securing IT infrastructure. This includes implementing robust security measures to protect IT systems and networks. Network security is the focus for 9.72% of the companies, where they provide solutions to safeguard network communications and prevent unauthorized access. Cybersecurity consulting is another prominent role, with 6.94% of the companies offering expert advice on cybersecurity strategies, risk management, and policy implementation. Managed security services, secure software development, and secure IT solutions are each provided by 5.56% of the companies, helping organizations proactively monitor and manage their security posture. These companies focus on developing secure software applications and implementing comprehensive IT security solutions, respectively.

Other services such as threat management, system security, threat detection, cybersecurity research, secure IT systems, secure communication solutions, secure digital solutions, penetration testing, secure healthcare IT systems, system security assessments, security assessments, secure document management, wallet security, secure authentication solutions, risk management, cybersecurity certification, secure communication services, cloud security, secure networking solutions, advanced cybersecurity solutions, IT security audits, cybersecurity risk management and policy advisory, cybersecurity audits, secure IT services, cybersecurity strategy, secure data management, network security solutions, system monitoring, secure IT systems and network security, secure network services, and comprehensive cybersecurity solutions are represented by 55.55% of the companies. These roles illustrate the broad spectrum of services and specializations within the cybersecurity field.

Cybersecurity Service	Percentage (%)
Secure IT infrastructure	11.11%
Network security	9.72%
Cybersecurity consulting	6.94%
Managed security services	5.56%
Secure software development	5.56%
Secure IT solutions	5.56%
Other	55.55%

Table 3: Percentage of cybersecurity services offered by recorded companies.

Presented in table 4, almost half of the companies (48.15%) have between 0 and 10 employees, indicating a large number of small businesses or startups. A quarter of the companies (25.93%) fall into the 11-50 employee range. Larger companies with more than 100 employees are less common, with only 1.23% having between 1001 and 5000 employees.

Employee Range	Percentage (%)
0-10	48.15%
11-50	25.93%
51-100	11.11%
101-500	11.11%
501-1000	2.47%
1001-5000	1.23%

Table 4: The distribution of companies based on the number of employees.

Presented in table 5, a significant portion of companies (45.24%) have an income of up to 1 million euros. Companies earning between 1 million and 5 million euros make up 23.81% of the representative sample. Interestingly, there are no companies in the 50 million to 100 million euros range, while 4.76% of companies have incomes ranging from 100 million to 1 billion euros.

Income Range (€)	Percentage (%)
0-1M	45.24%
1M-5M	23.81%
5M-10M	7.14%
10M-50M	19.05%
50M-100M	0.00%
100M-1B	4.76%

Table 5: The distribution of companies based on income range.

2.2.4 Society

As of June 24, 2024, Slovenia's population totals 2,123,949 registered citizens.

The demographic breakdown is as follows:

- Male Population: 939,969
- Female Population: 980,707

Age distribution:

- Average Age: 44.2 years
  - 0-14 years: 14.7%
  - 15-64 years: 63.5%
  - 65 years and older: 21.8%

The insights from the Digital Economy and Society Index (DESI) 2024, as presented in Table 6, offer a comparative analysis of the digital skills of individuals in Slovenia relative to the EU average.

Indicator, All individuals (aged 16-74)	EU average (% of individuals)	EU ranking	Slovenia average (% of individuals)	Slovenia ranking
Internet use	90.27	17th	89.41	19th
At least basic digital skills	55.56	17th	46.70	23th
Above basic digital skills	27.32	16th	18.88	25th
E-Government users (last 12 months)	75.01	22nd	78.37	20th

Table 6: DESI 2024 index for digital skills in Slovenia.

2.2.5 Technology

Significant research on new technologies, particularly in cybersecurity, is being conducted by several key institutions, like University of Maribor, University of Ljubljana, University of Primorska and Gea college. These institutions are actively involved in research and development projects, often collaborating on national and international levels. ARIS CRP

supports numerous actors in the field of cybersecurity research, encouraging a broad spectrum of projects and initiatives in the field of cybersecurity.

The Slovenian government is actively investing in technological developments, including cybersecurity, through several key agencies and ministries:

- **ARIS (Agency for Research and Innovation Slovenia)**: Provides funding and support for research and innovation projects.
- **Ministry of Public Administration (MDP)**: Invests in digital infrastructure and e-government initiatives.
- **Ministry of Economic Development and Technology:** Focuses on fostering technological advancements in various economic sectors.
- **Ministry of Defence (MORS)**: Includes investments in cybersecurity and related technological developments, such as the Cyber Range.

2.3 Literature

In the search for relevant literature on cybersecurity roles and skills, thirteen articles and reports were identified and selected for analysis. These sources span a range of publications, including internal documents, national reports, academic theses, and strategic frameworks. The literature reviewed offers comprehensive insights into the current and future landscape of cybersecurity roles and skills in Slovenia.
A frequency analysis was performed:

- Type of Publication:
  - Internal Documents: 3
  - National Reports: 4
  - Academic Theses: 5
  - Strategic Frameworks: 1
- Institution:
  - University of Maribor: 4
  - University of Ljubljana: 3
  - University of Primorska: 3
  - Gea College: 3
- Focus Area:
  - Current Landscape: 6
  - Future Landscape: 3
  - New Technologies: 4
- Year of Publication:
  - 2020: 2
  - 2021: 4
  - 2022: 3
  - 2023: 4

The number of publications in the mentioned literature focusing on cybersecurity is larger than the presented numbers. However, the literature primarily focuses on implementing and developing cybersecurity solutions and analysing cybersecurity practices and was not in the scope of this report.

2.3.1 Roles

The literature on cybersecurity roles highlights the evolving and critical nature of these positions in ensuring national and organizational security. Key findings include (Dušek, 2022; Kocbek & Lampe, 2021; Kompara, Nemec Zlatolas, Hölbl, Welzer Družovec, Bošnjak, et al., 2022; Kompara, Nemec Zlatolas, Hölbl, Welzer Družovec, Taneski, et al., 2022; Maček et al., 2018; Markun, 2023; Prislan, 2012; Štrucl, 2021; Urajnar, 2023; Zupančič, 2020):

- Current Demand:

- **Cybersecurity Manager and Cybersecurity Officer (CISO)**: These roles are crucial in organizations for overseeing the entire cybersecurity framework, ensuring compliance with regulations, and managing risks and incidents. The CISO is emphasized for their strategic role in safeguarding information systems and ensuring organizational resilience against cyber threats.
- **Cybersecurity Professionals**: There is a growing demand for specific cybersecurity professionals, especially in for roles like **penetration testers, risk managers, auditors and threat intelligence specialists**.

- Future Demand:
  - **Digital Transformation Manager and Data Scientist**: As part of broader ICT roles, these positions are expected to grow in importance, driven by the need to integrate cybersecurity into digital transformation initiatives and data-driven decision-making.
  - **Cybersecurity Educators and Trainers:** The establishment of networks of secondary schools and universities focusing on cybersecurity education is projected to create new roles aimed at developing future cybersecurity professionals.

2.3.2 Skills

The literature underscores the importance of a diverse set of skills for cybersecurity professionals, categorizing them into technical and non-technical competencies:

1. **Technical Skills**:
   - **Cybersecurity Competence Catalogue**: The development of detailed competence levels for various ICT roles highlights essential technical skills such as risk management, cybersecurity architecture, and understanding of domain-specific technologies.
   - **Incident Management and Compliance**: Skills related to managing cybersecurity incidents, ensuring compliance with legal frameworks, and protecting information systems are emphasized as critical for effective cybersecurity management.
2. **Soft/Transversal Skills**:
   - **Strategic Management and Customer Orientation**: Beyond technical skills, strategic management capabilities and understanding customer needs are essential for roles like the Digital Transformation Manager. These skills help align cybersecurity initiatives with broader business objectives.
   - **Communication and Awareness**: Effective communication and raising awareness about cybersecurity risks are necessary to enhance the overall security posture of organizations. Professionals must be adept at educating and informing stakeholders about potential threats and best practices.
3. **Organizational Skills**:
   - **Collaboration and Stakeholder Engagement**: The ability to collaborate with various stakeholders, including public-private partnerships, is crucial for leveraging scarce resources and ensuring comprehensive cybersecurity measures.
   - **Leadership and Risk Management**: Leadership skills in managing cybersecurity teams and overseeing risk management processes are highlighted as vital for CISOs and other high-level cybersecurity roles.

2.4 Labour market reports and databases

To search for studies and reports on the topic of cyber security in Slovenia and the EU, an analysis of five key research papers published between 2012 and 2023 was performed. These papers cover a range of topics, including legal regulations, local community security, national strategies, employee cyber risk management, and perspectives on information warfare and cybercrime. The reports were sourced from various academic databases and repositories, including DKUL (Digital Library of the University of Ljubljana), DKUM (Digital Library of the University of Maribor) and Urbana Informatika.

2.4.1 Roles

The analysis of high-demand roles in cybersecurity, as outlined in various studies and strategic documents, highlights notable trends in the present and projected future demand for specific positions. These trends are systematically summarized in table 7, which consolidates insights from various sources. The roles are listed in the first column, while the subsequent columns display the percentage of demand currently, in two years, and beyond five years. For instance, the demand for the role of Chief Information Security Officer (CISO) is expected to increase significantly from 30% to 60% over the next five years. Similar upward trends are observed across other roles such as Architects, Penetration Testers, and Threat Intelligence Specialists. This data reflects the growing importance of these positions in ensuring cybersecurity in the evolving digital landscape. (DIGITAL SLOVENIA 2030: An Overarching Strategy for Slovenia's Digital Transformation by 2030, 2023; Napovedovanje Potreb Po Kadrih Na Digitalnih Profilov, 2023; Gergorić & Lampe, 2021; Urajnar, 2023)

Role	Current Demand (%)	Demand in 2 Years (%)	Demand in >5 Years (%)
Chief Information Security Officer (CISO)	30	50	60
Architect	25	40	50
Penetration Tester	25	40	55
Risk Manager	20	30	35
Threat Intelligence Specialist	25	35	45
Auditor	25	35	50
Educator/Trainer	20	30	40
Researcher	15	20	25
Digital Forensics Investigator	10	20	30

Table 7: Demand for crucial roles presented in literature.

2.4.2 Skills

Table 8 illustrates the importance of various technical skills in Slovenia compared to the European Union (EU) as a whole, based on employer preferences. The table highlights that in Slovenia, there is a slightly higher demand for comprehensive technical expertise across all listed skills. For example, the demand for System Management in Slovenia is 65%, compared to 62% in the EU. Similarly, Cybersecurity Planning is valued by 62% of Slovenian employers, slightly above the EU average of 60%. (Gergorić & Lampe, 2021; Kocbek & Lampe, 2021; Kompara, Nemec Zlatolas, Hölbl, Welzer Družovec, Taneski, et al., 2022)

Importance of Technical Skills, based on employers preferences in Slovenia in comparison with EU in general.		
Skill	**EU (%)**	**Slovenia (%)**
System Management	62	65
Cybersecurity Planning	60	62
Business Continuity, Disaster Recovery, and Incident Management	55	57
Security Program Management	50	52

Personnel Security	48	50
Security Operations	46	48
Social and Behavioural Privacy	43	45
Data Privacy and Security	58	60
Usable Security and Privacy	54	56

Table 8: Importance of technical skills in Slovenia, compared to EU average.

Table 9 highlights the importance of soft skills, with Communication and Teamwork being particularly valued in Slovenia, like the European Union. Critical Thinking and Problem Solving are especially crucial, with a slightly higher emphasis in Slovenia compared to the EU averages. (Gergorić & Lampe, 2021; Kocbek & Lampe, 2021).

Importance of Soft Skills, based on employers' preferences in Slovenia in comparison with EU in general.		
Skill	**EU (%)**	**Slovenia (%)**
Team and client communication	58	60
Teamwork	55	57
Critical Thinking	70	72
Problem Solving	72	74
Creativity	50	52
Ethics	45	43
Independence	48	49
Self-Management	54	56
Leadership	38	37
Responsibility/Reliability	53	55

Table 9: Importance of soft skills in Slovenia, compared to EU average.

2.5 Conclusions

Slovenia's national context in cybersecurity is characterized by a strong governmental framework, comprehensive legislation, a dynamic market, and a commitment to technological advancement. The current and future landscape indicates a growing need for skilled cybersecurity professionals, supported by targeted education and training initiatives. In the short term (next 2 years), the focus is on enhancing digital skills and increasing the number of cybersecurity professionals. In the medium term (3-5 years), the integration of cybersecurity into digital transformation and data-driven initiatives is crucial. In the long term (beyond 5 years), sustaining a robust cybersecurity ecosystem through continuous research, development, and strategic management will be essential.

3 Questionnaire

This chapter delves into the findings from a questionnaire that was distributed to both IT and non-IT companies across Slovenia. The purpose of the questionnaire was to gather insights into the current and future needs of these organizations with respect to cybersecurity roles and skills. It aimed to identify the specific cybersecurity positions that are in demand, the skills and competencies these roles require, and how companies are currently addressing the training and development of their cybersecurity personnel.

3.1 Data collection

The survey was distributed in the following ways:

- By email to CCIS ICT Association members and to all ICT companies in Slovenia.
- Additionally, the survey was sent by email to one hundred CIOs of the largest companies in Slovenia, ensuring input from key decision-makers in the industry.
- Through social networks by both partners CCIS and UM.
- On official websites of UM.

This multi-faceted approach ensured a broad and comprehensive reach across various organization types and sizes.

3.2 Results

Within thirty-six survey responses, that are presented in chart 1, most respondents come from either specialized cybersecurity organizations or ICT companies that require in-house cybersecurity professionals. A significant portion also comes from private and public sector organizations across various industries.

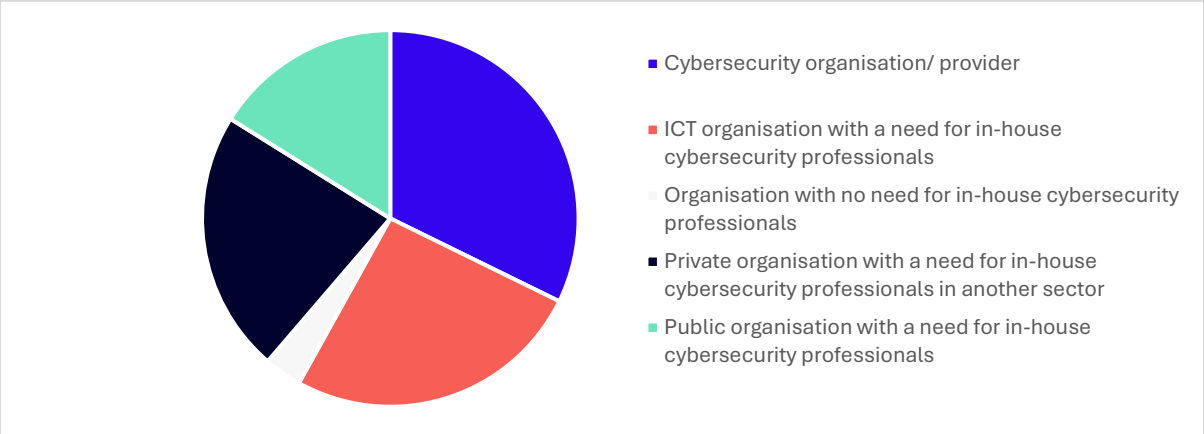

Chart 1: Survey question "To what category does your organisation belong?".

By sending the survey to CIOs of the largest companies from Industry, the analysis captures insights from key decision-makers, enhancing the survey's relevance and impact. Additionally, medium, small, and micro companies are almost evenly represented, ensuring a balanced perspective across different organizational sizes (see chart 2).

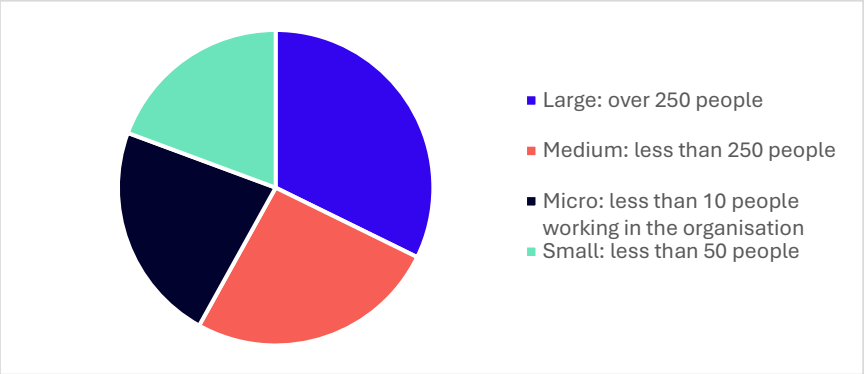

Chart 2: Survey question "What is the size of the organisation?".

The results indicate a broad and inclusive survey distribution, reaching various organizational types and sizes. This comprehensive approach ensures that the analysis reflects diverse perspectives on cybersecurity needs, aligning with the survey's goal of capturing a wide range of insights for a holistic understanding of the industry and its needs on the national level.

3.2.1 Cybersecurity roles

Chart 3 shows that most of the cybersecurity workforce is concentrated in execution roles, with Cybersecurity implementer/expert and Incident Responders having the highest numbers. (Chief) Information Security Officers also have a presence, while more specialized roles, such as Digital Forensics Investigators and Cybersecurity Auditor, have significantly fewer employees, indicating either niche expertise or lower demand for these positions.

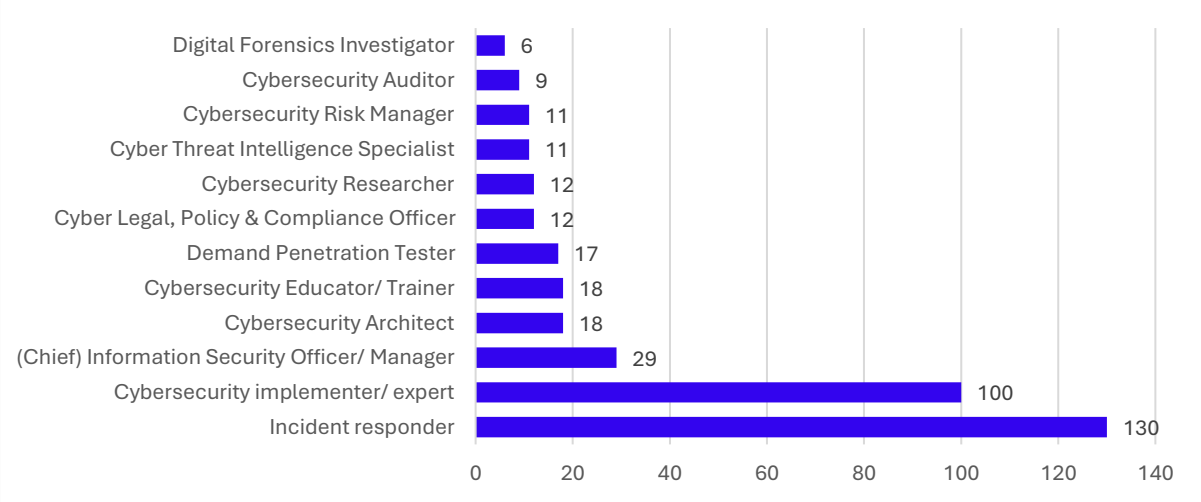

Chart 3: Survey question "Number of employees per role working NOW".

Two most "popular" and needed cybersecurity roles are Cybersecurity implementer/expert and Incident responder.

This is the reason analysis is divided to two parts, first analysing just these two roles and secondly analysing the rest of roles.

Currently there is more than one hundred experts in Cybersecurity implementer/expert and Incident responder based on survey and is expected to **more than double** the number in 5 years. Chart 4 indicates a consistent and growing demand for both roles across all times. The biggest growth in demand is projected for Cybersecurity

implementer/expert. This highlights the critical and ongoing importance of these roles in managing current and future cybersecurity challenges.

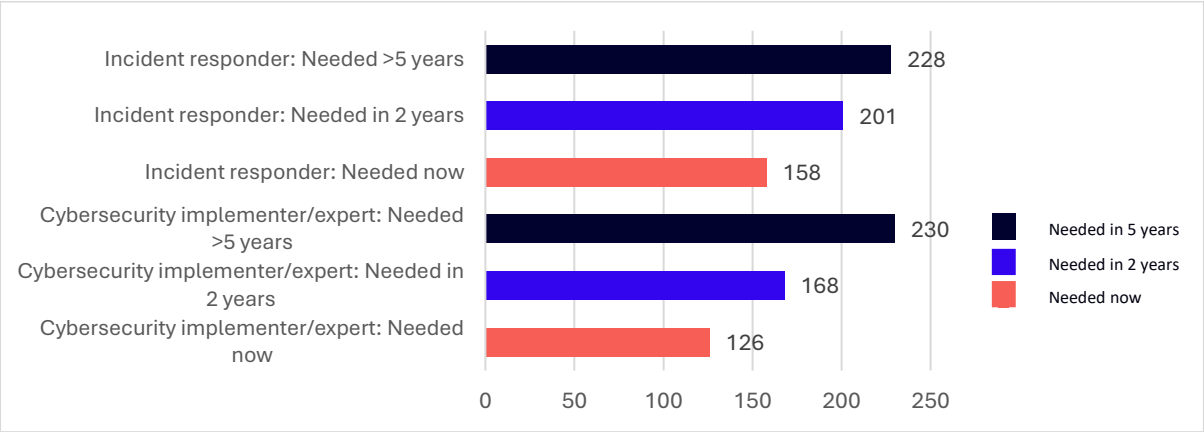

Chart 4: Survey question "Demand for people in roles Cybersecurity implementer/expert and Incident responder".

Chart 5 demonstrates a consistent growth in demand across all roles, underscoring the importance of investing in each area of cybersecurity. However, to effectively prioritize resources and efforts, it is crucial to assess not only the overall

demand but also the specific roles experiencing the highest volume and the fastest growth. This combined perspective will help identify which roles are most critical in addressing current and future cybersecurity challenges.

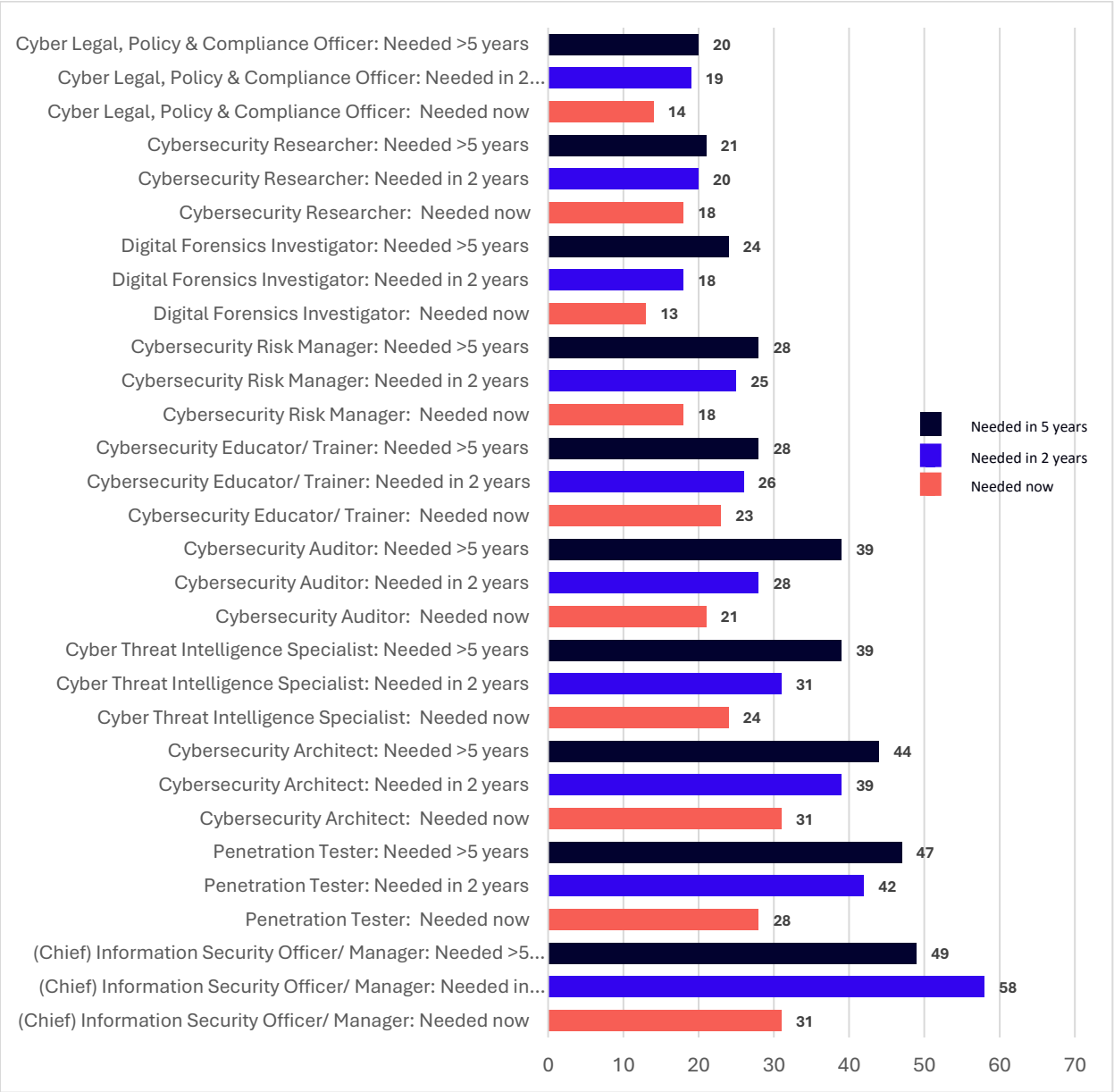

Chart 5: Survey question "Demand for people for all other roles".

In terms of **absolute numbers**, the roles with the highest demand are (Chief) Information Security Officers, Penetration Tester, and Cybersecurity Architect, followed closely by Cyber Threat Intelligence Specialist and Cybersecurity Auditor. This high demand suggests that organizations are placing a strong emphasis on leadership roles to manage overall security strategies, as well as on technical experts to test and secure systems from vulnerabilities. The need for Penetration Testers and Architects reflects the focus on proactive defence and building secure infrastructures, while the demand for Cyber Threat Intelligence Specialists shows the importance of gathering and analysing data to anticipate and counteract cyber threats. Cybersecurity Auditors are critical for ensuring compliance with regulations and standards, emphasizing the growing need for organizations to maintain transparency and adhere to increasingly complex security laws.

From a **higher growth perspective** in chart 6, roles such as Cybersecurity Auditor, Digital Forensics Investigator, Cyber Threat Intelligence Specialist show high growth potential with more than triple increase of the number from now. Roles Penetration Tester, Cybersecurity Risk Manager and Cybersecurity Architect are more than doubling the number of people from now. This substantial growth in these key roles underscores the expanding scope of cybersecurity, where organizations are not only focusing on strengthening their defences but also on identifying and mitigating risks, ensuring regulatory compliance, and developing advanced strategies to combat sophisticated cyber threats.

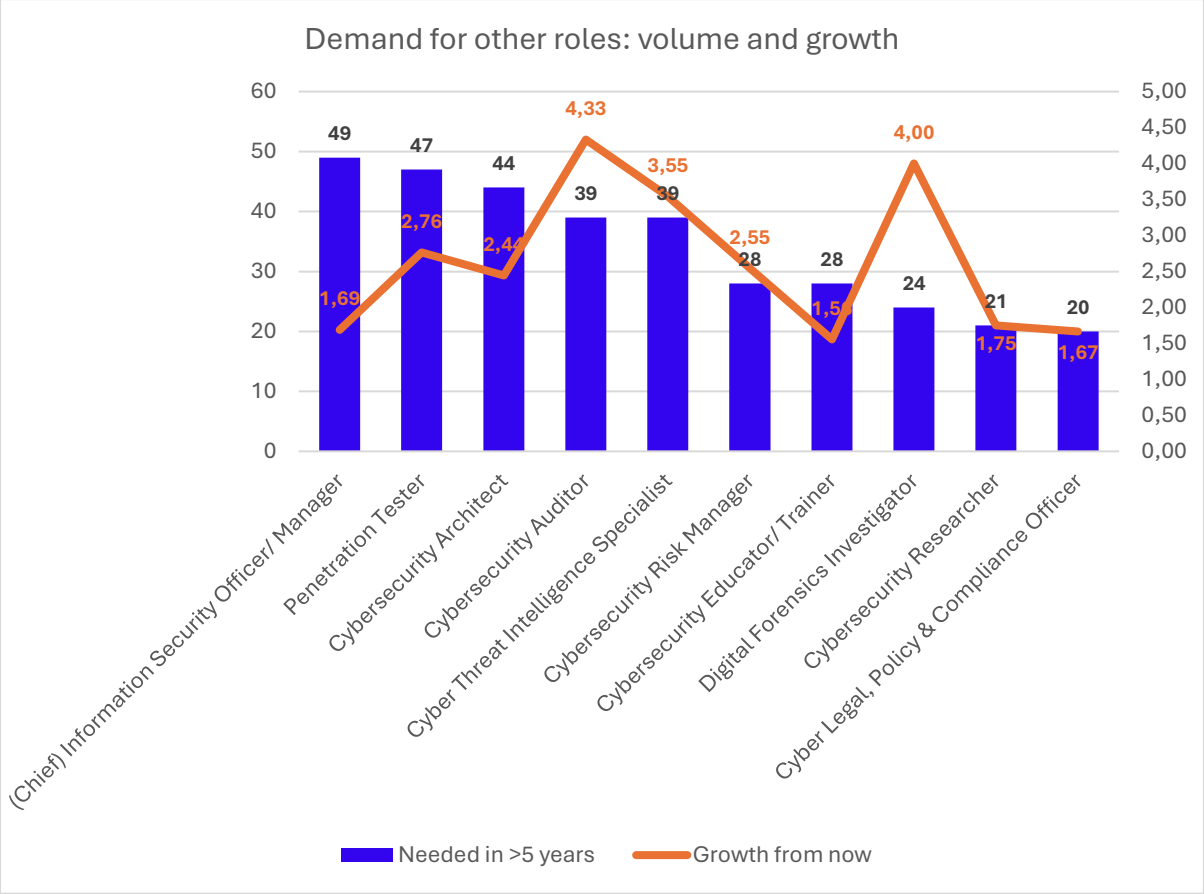

Chart 6: Survey question "Demand for all other roles from volume and growth perspective".

Combining both perspectives, the priority should be placed on:

- Cybersecurity implementer/expert and Incident responder.
- Cybersecurity Auditor, Cyber Threat Intelligence Specialist and Penetration Tester.
- Cybersecurity Architect, Digital Forensics Investigator, (Chief) Information Security Officer/ Manager.

3.2.2 Skills for cybersecurity professionals

In the following charts, 7 and 8, respondents were asked to rate the importance of various topics. For the purpose of ranking results, the responses "Lot of need" and "Substantial need" were combined. The graphs In this chapter illustrate the varying levels of demand across different cybersecurity skills.

With regards to **cybersecurity skills**, the most prominent demand, reflected by the red bar indicating "Lot of need" and blue bar indicating "Substantial need" is for skills related to Communications Security, Cloud Security, Information Systems & Network Security/ Cyber Resiliency, Incident Management and Access Controls/ Identity Management.

These areas show consistently high demand across organizations, signalling a critical need for expertise in securing emerging technologies and protecting sensitive data.

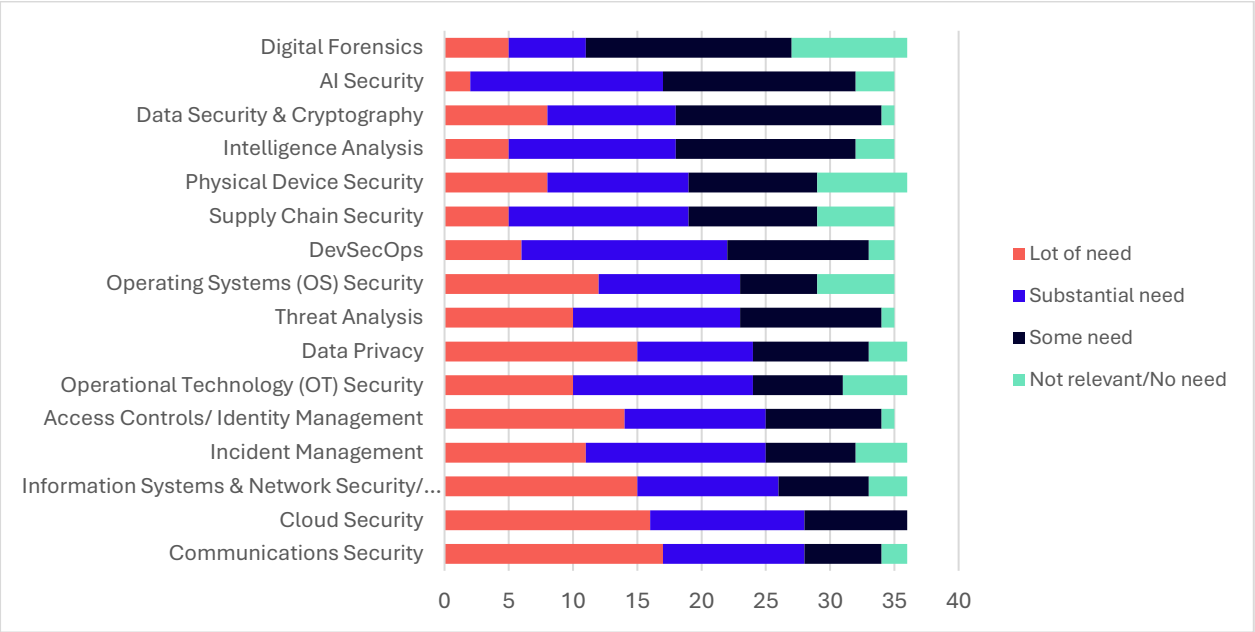

Chart 7: Survey question "Cybersecurity skills needs".

With regards to **IT related skills**, the most important skills are System Administration & Integration, Network Management, Software Development & Computer Languages, Enterprise Architecture & Infrastructure Design and Operating Systems.

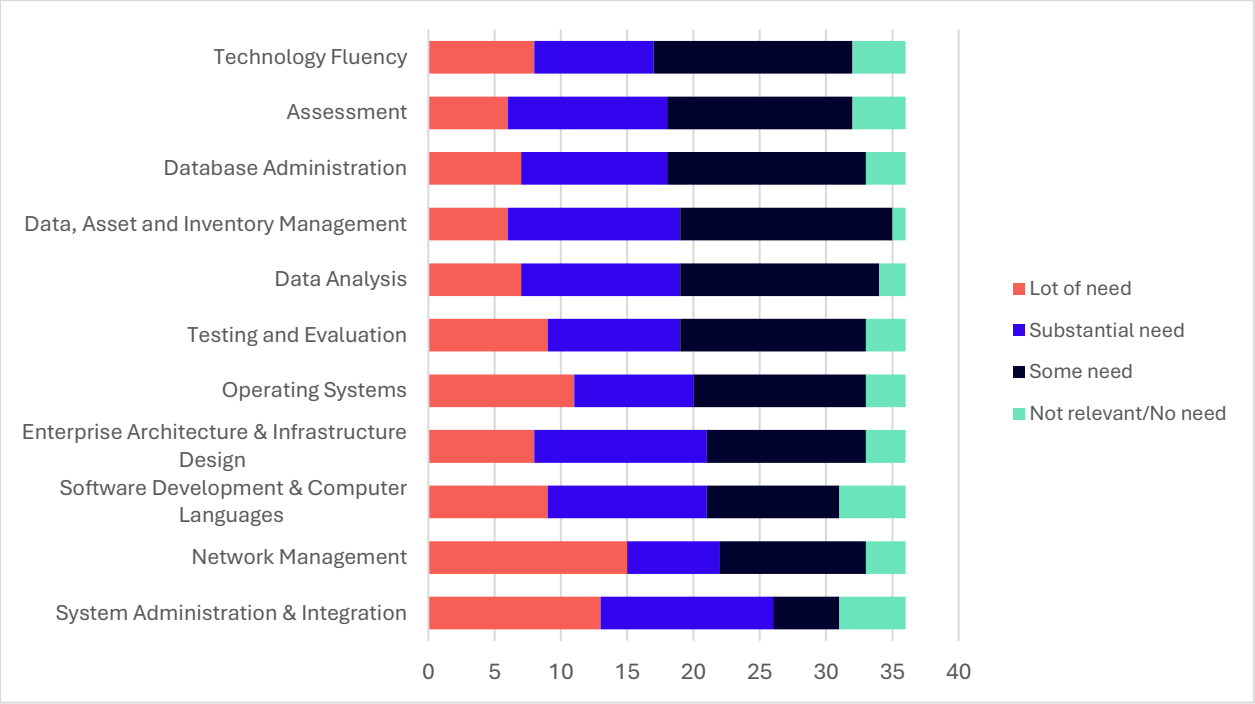

Chart 8: Survey question "IT related skills needs".

Regarding **organization-related** skills in chart 9, key areas are Risk Management, Business Continuity, and Process, highlighting the critical awareness of cybersecurity's role in maintaining "business as usual". However, there is a growing sentiment that certain skills are not as essential.

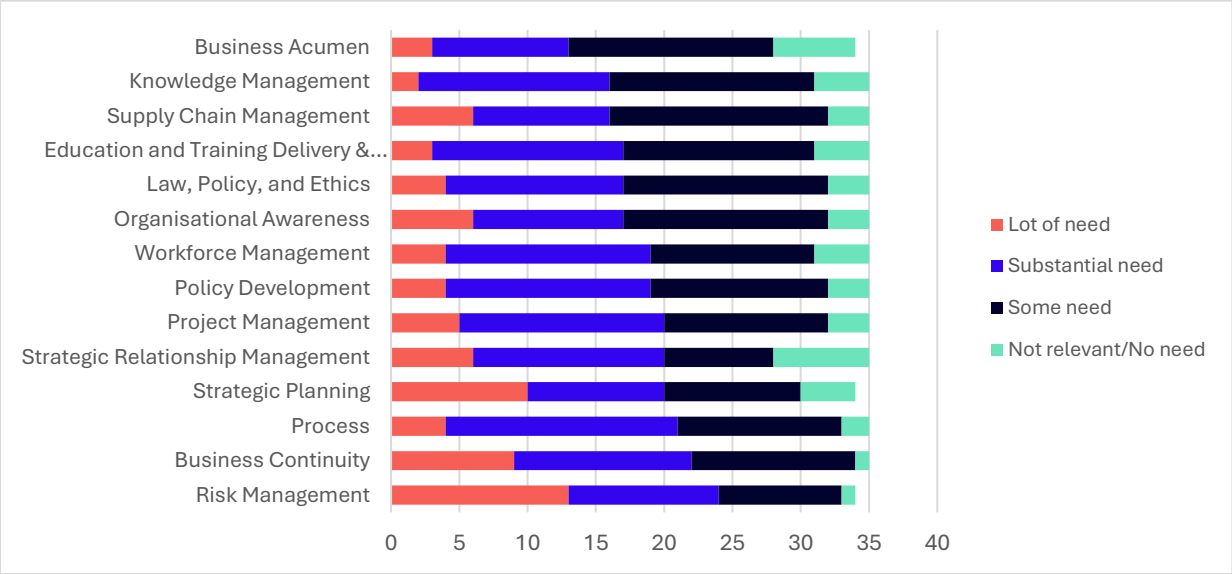

Chart 9: Survey question " Organisation related skills needs".

Regarding **soft/transversal** skills in chart 10, the needs distribution is much more balanced. While Problem-solving stands out as the most needed skill when combining "Lot of need" and "Substantial need," other categories rank highly based solely on "Lot of need," including Willingness to Learn, Acting Responsibly, Communication, and Ethical Behaviour. However, compared to other skill areas, there is a growing sentiment that certain skills are becoming less essential.

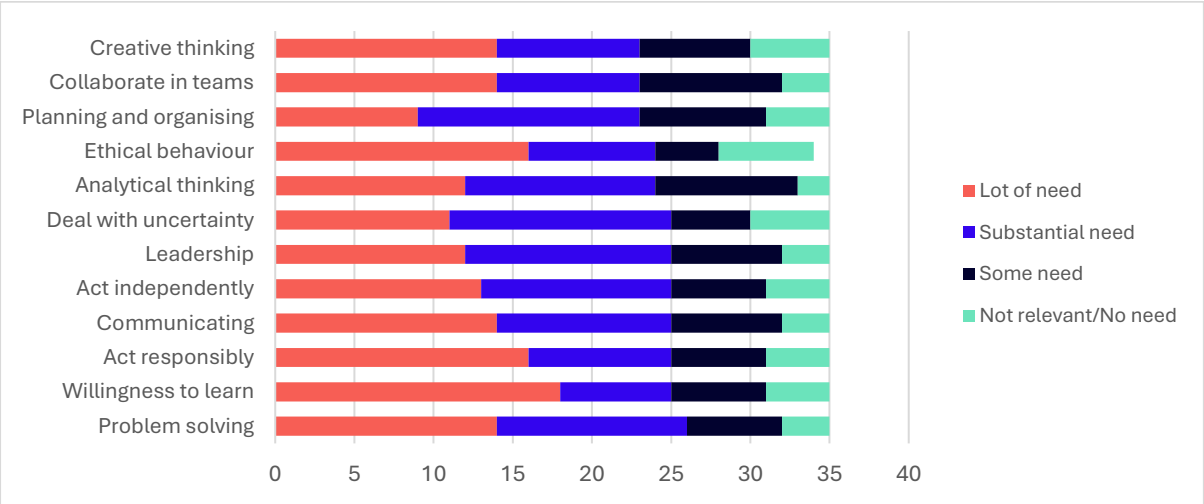

Chart 10: Survey question "Soft/transversal skills needs".

3.2.3 Training of cybersecurity professionals

All companies agree on the necessity of continuous training and development. The biggest emphasis is on "Upskill own ICT personnel", "In-company training by own staff", "Hire people with already the right skills" and "External training", as presented in chart 11.

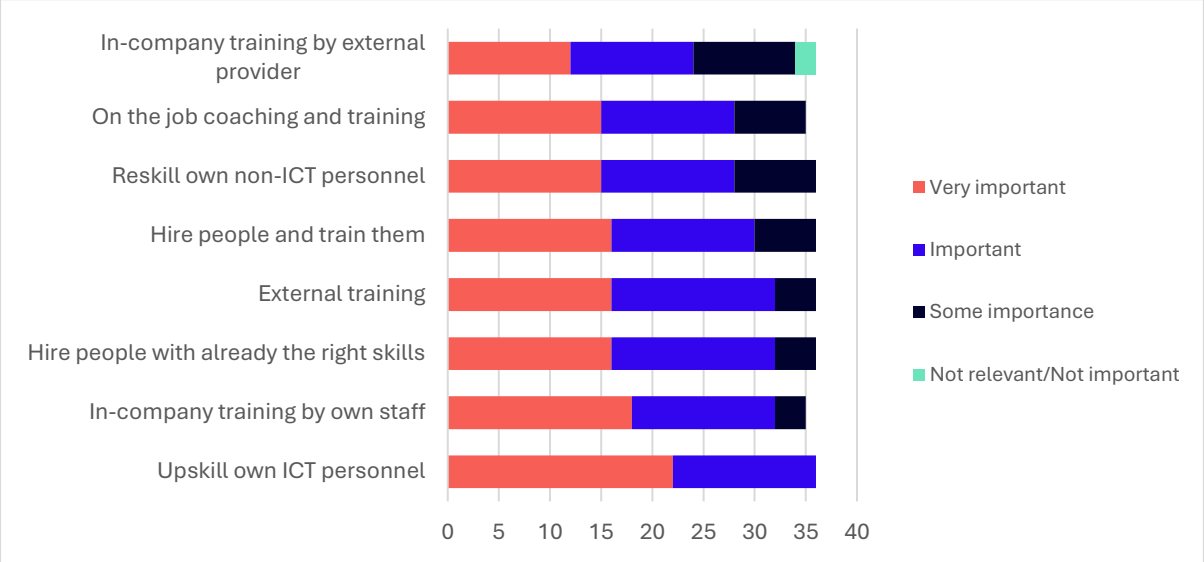

Chart 11: Survey question "Importance of training strategies".

Overall, the data in chart 12 suggests that while all forms of qualifications have some level of importance, there is a clear preference for certifications and education that are directly relevant to the role. Formal certifications and specific professional education are particularly valued, with a strong emphasis on their relevance to the position being hired for. Bachelor/master degree relevant for the role is not as highly prioritized. This indicates a trend towards valuing specialized knowledge and skills over broader educational backgrounds in hiring decisions.

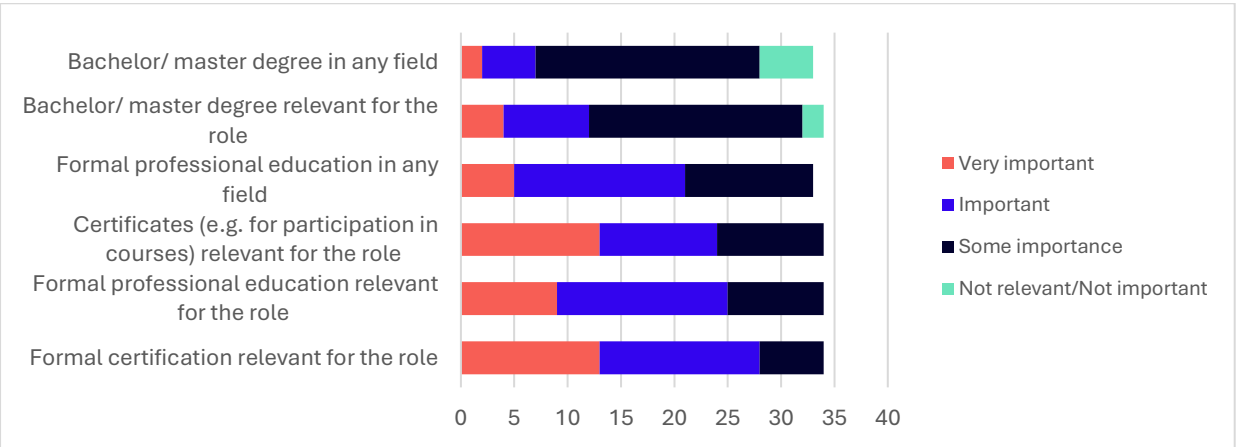

Chart 12: Survey question "Importance of qualification when hiring".

3.3 Conclusions

Although the survey was executed for a smaller number of non-ICT and ICT organisations, the survey is highly relevant due to its balanced distribution, capturing insights from key decision-makers in large companies, specialized cybersecurity and ICT organizations, as well as a diverse range of private and public sector organizations across different industries and company sizes.

This analysis shows a clear trend of high demand for specific skills and qualifications, with organisations recognizing the importance of both technical and soft skills. The data indicates a strong emphasis on training and qualifications, demonstrating a commitment to building and validating workforce expertise.

Cybersecurity Implementer/Expert and Incident responder are among the most sought-after roles. The main reasons are:

- **Smaller IT departments in many organizations** while such companies often hire external IT providers to implement security systems, they still need an internal person to respond to incidents, making the Incident Responder role essential.
- **Demand for versatile roles:** organizations, especially smaller IT companies, often need a "universal" security role to cover a wide range of security needs. The Cybersecurity Implementer/Expert is crucial because it combines various tasks, from setting up to maintaining security systems.
- **Lack of awareness about specialized roles in non-IT companies**: Many non-IT companies still do not recognize the advantages of more specialized roles in cybersecurity. This leads to higher demand for broader, more versatile roles like Implementer/Expert and Incident Responder, who can handle a range of challenges.

The findings suggest a significant focus on roles such as:

- Cybersecurity implementer/expert and Incident responder
- Cybersecurity Auditor and Cyber Threat Intelligence Specialist
- Digital Forensics Investigator

In terms of skills, the data reveals key priorities in:

- **Cybersecurity** skills: Communications Security, Cloud Security, Information Systems & Network Security/ Cyber Resiliency, Incident Management and Access Controls/ Identity Management
- **IT related** skills: System Administration & Integration, Network Management, Software Development & Computer Languages, Enterprise Architecture & Infrastructure Design and Operating Systems
- **Organization-related** skills: Risk Management, Business Continuity, and Process
- **Soft/transversal** skills: Problem-solving, Willingness to Learn, Acting Responsibly, Communication, and Ethical Behaviour

Training strategies are considered essential, with a strong preference for upskilling current staff, hiring skilled individuals, and utilizing internal training resources. The emphasis on relevant qualifications—particularly formal certifications and role-specific education—demonstrates that these are prioritized over general degrees.

This suggests that organizations are not only focused on acquiring immediate skill sets in new hires but are also committed to the continuous development of their workforce. The prioritization of specific qualifications and targeted training strategies reflects a strategic approach to creating a capable and adaptable team, well-equipped to meet the evolving challenges of their industries.

4 Job vacancy analysis

4.1 Data collection

In the initial attempt to analyse job vacancies in Slovenia, it is important to note the difficulty in automatically scraping job listings from Slovenian job boards and websites. Platforms such **as SloTech, Mojedelo, and Deloglasnik** do not easily support scraping methods due to technical restrictions and variations in their website structures. As a result, it becomes necessary to collect job data manually, searching through job postings and extracting relevant cybersecurity positions, roles.

However, this issue will be addressed in future versions of the report by automating the data collection process. By collaborating with specialized providers like Abodoo, there will be an opportunity to implement more efficient and accurate scraping techniques, ensuring a more comprehensive and timely capture of job vacancies.

It is also worth noting that, while scraping Slovenian sites posed challenges, LinkedIn yielded a significant number of remote job listings. Many of these roles are offered by companies outside Slovenia, which opens opportunities for Slovenians to apply for remote jobs in international companies or even jobs with reallocation to another country. However, these positions are typically not based in Slovenia itself.

This manual process allows for insights into the current cybersecurity job market, although the data is gathered at a slower pace. The following sections will explore the results and trends based on the data collected through both automated and manual methods.

A total of 149 job postings were reviewed. However, some positions could not be mapped to the ENISA European Cybersecurity Skills Framework (ECSF) and were therefore excluded from the analysis. These excluded roles primarily included positions in product management, sales, senior management, or development roles requiring cybersecurity knowledge. As a result, 128 posts were deemed relevant for this study.

4.2 Results

The figure below shows the distribution of job postings by location. Only 27% of the postings are based in Slovenia. An additional 34% are for remote positions, which have recently gained significant interest. Furthermore, 42 job listings, representing 33% of the total, are located in other European countries. However, if we focus on EU countries with a higher standard of living that are more attractive for migration, the number of listings drops to 13.

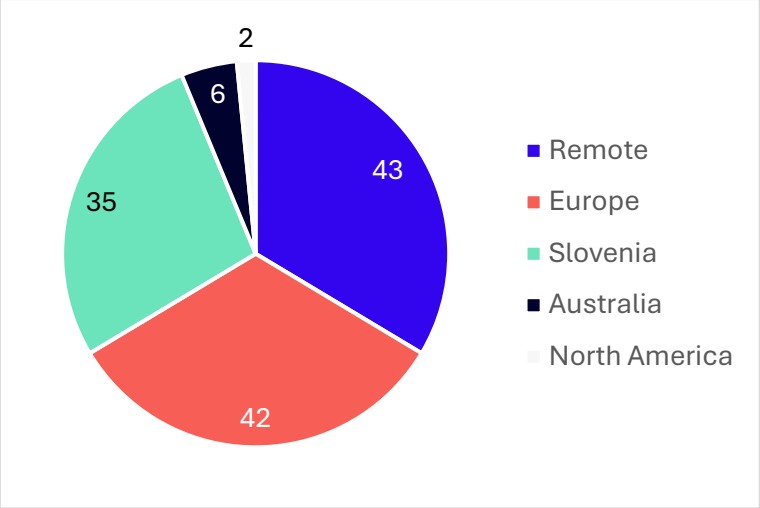

Chart 13: Postings per job location

4.2.1 Cybersecurity roles

The analysis highlights the role of Cybersecurity Implementer/Expert as the most in-demand position. Following this, (Chief) Information Security Officer/Manager role is also highly sought after. Other roles such as Penetration Tester, Cyber Incident Responder, and Cybersecurity Architect see slightly less, but still notable, demand. These roles reflect a broad spectrum of expertise needed in the cybersecurity field, ranging from leadership and strategic management to specialized technical skills.

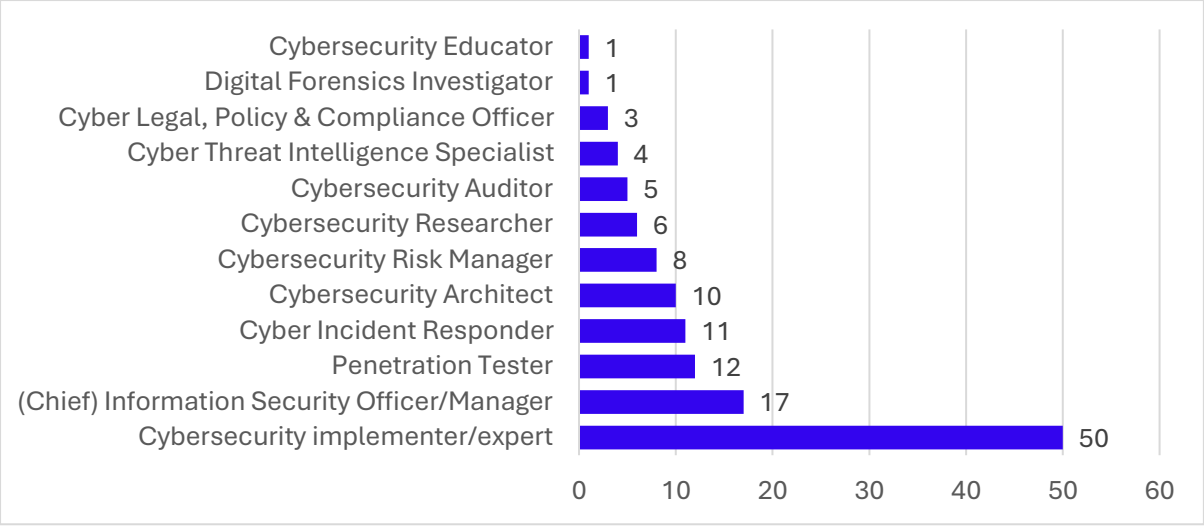

Chart 14: Demand for Cybersecurity roles

When the data is filtered for jobs in Slovenia only, the result remains very similar, with Cybersecurity Implementer/Expert leading and followed by the (Chief) Information Security Officer/Manager. Interestingly, the current data shows no demand for roles such as Cyber Incident Responder, Cybersecurity Auditor, Cyber Threat Intelligence Specialist, Cyber Legal, Policy & Compliance Officer, Digital Forensics Investigator, and Cybersecurity Educator. While one possible reason could be the absence of job postings during this period, the general experience suggests that cybersecurity roles in Slovenia are not yet fully developed.

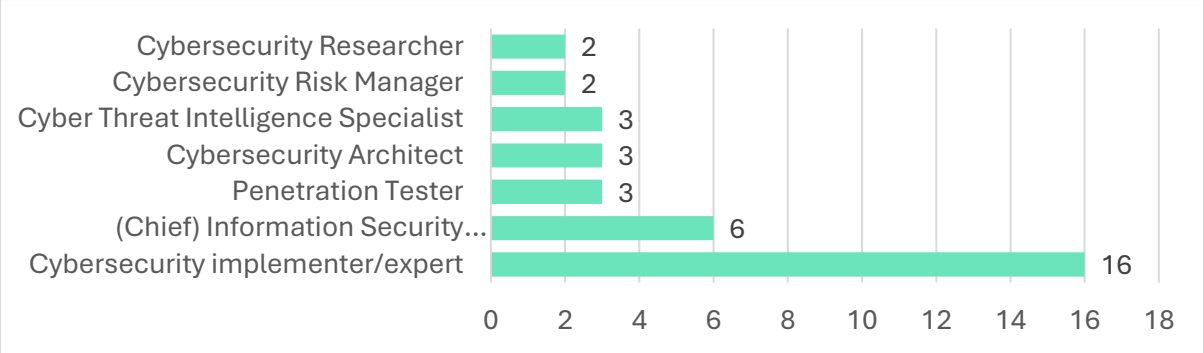

Chart 15: Demand for Cybersecurity roles with Slovenia as job location.

4.2.2 Skills for cybersecurity professionals

Companies most frequently specify soft skills in job postings, with communication, problem solving, and leadership being the most sought after. These are followed by cybersecurity-specific skills, such as incident management and threat analysis, and IT-related skills, like Data Analysis and Software Development & Computer Languages. While organization-related skills are not yet in high demand, risk management and strategic planning are the most requested in this category. There is a noticeable emphasis on technical skills overall, reflecting the need for candidates to have strong foundational knowledge in cybersecurity and IT infrastructure. However, the high demand for soft skills shows that employers are also looking for well-rounded professionals who can collaborate effectively, solve complex problems, and lead teams in a dynamic security environment.

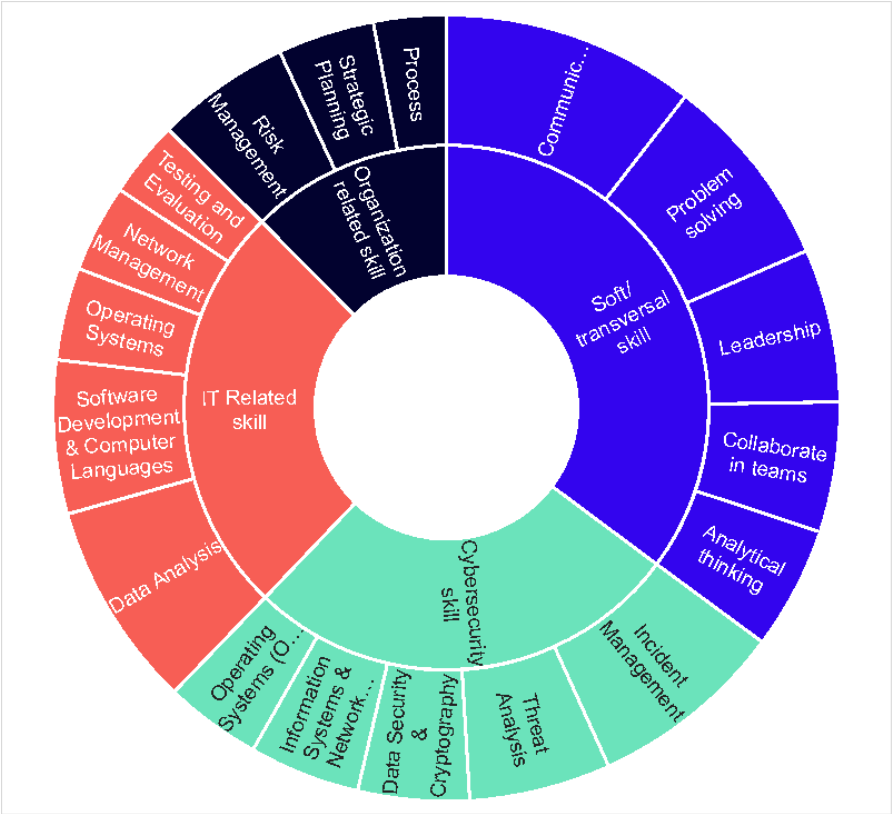

Chart 16: Most in-demand skills from job postings.

4.3 Conclusions

From the analysis of cybersecurity-related job postings, several key trends seem to emerge:

- **Low Volume of Job Postings:**
    - There appears to be a limited number of cybersecurity job vacancies specifically in Slovenia. Few postings seem to directly target cybersecurity professionals, which might suggest that the market for external cybersecurity hires remains underdeveloped.
    - Roles like Penetration Tester, Ethical Hacker, and Cybersecurity Analyst tend to be posted sporadically, with most listings coming from larger institutions, such as the Ministry of Defence Cyber Centre, and a few private companies.
- **Focus on High-Level Expertise:**
    - Many of the available roles, such as Chief Security Officer (CSO) or Information Security Manager, seem to focus on senior professionals who have extensive experience in handling advanced security measures, such as cloud-based security, compliance standards, and penetration testing.
    - Specific certifications like CISSP, ISO 27001, GDPR compliance, and ethical hacking certifications are frequently prerequisites, making these jobs less accessible to newcomers or mid-level professionals.
- **Remote Opportunities and Hybrid Models:**
    - Some roles appear to offer remote or hybrid work options. This seems to open up opportunities for Slovenians to work for international or out-of-region companies without leaving Slovenia. However, these positions are limited and seem to focus primarily on highly technical, security-oriented roles.
- **Upskilling of Internal Employees:**
    - A key trend in Slovenia's job market is the preference for upskilling internal employees rather than hiring new staff for cybersecurity roles. This practice results in fewer public job postings for cybersecurity professionals. Companies seem to prefer training their existing IT staff to meet cybersecurity needs, thereby avoiding the need for external hires.

The cybersecurity job market in Slovenia seems relatively small and tends to focus on highly specialized roles. There appears to be a significant lack of entry- to mid-level opportunities, with most job listings requiring significant experience, certifications, and specific skill sets. Many companies appear to prioritize upskilling their current employees rather than recruiting externally, further limiting the number of available cybersecurity roles.

Although some companies seem to offer remote or hybrid opportunities, most job openings in cybersecurity remain scarce and specialized. This indicates that while Slovenia's cybersecurity job market is growing, it has not yet achieved the maturity level seen in other countries. Companies should consider expanding the availability of entry-level roles and opening the market to younger professionals. This would help foster a more dynamic and competitive cybersecurity workforce.

The results from the job vacancy analysis closely align with the findings of questionnaire, showing a high level of consistency between the two, with only minor deviations observed in specific skill demands or priorities.

This analysis highlights the need for more accessible opportunities in cybersecurity, as well as a greater emphasis on developing external hiring strategies among Slovenian companies. This will be essential to ensuring the growth and resilience of the country's cybersecurity infrastructure.

5 Desk research (supply)

5.1 Data collection

The search for relevant educational programs in Slovenia was conducted using a combination of online searches, institutional websites, and publicly available information. Additional details were obtained through direct communication, such as emails or phone calls, when necessary. The dataset includes a variety of institutions, categorized as either public or private, offering programs across different EQF levels.

Specifically, the dataset comprises:

- Public Institutions: 8 programs
- Private Institutions: 5 programs
- EQF Levels: Ranging from EQF4/5 to EQF8
- Types of Qualifications: Diplomas and Degrees

5.2 Results

This paragraph provides information on the found programs. Table 10 contains an overview of the specializations and the number of learners and potential learners (Kompara, Nemec Zlatolas, Hölbl, Welzer Družovec, Bošnjak, et al., 2022).

Title learning programme	Type of programme	Name provider	Type of institution	Kind of recognition
Informatics and Data Technologies	EQF6 (bachelor)	UM FERI	Public	Diploma
	EQF7 (master)	UM FERI	Public	Diploma
Information security	EQF6 (bachelor)	UM FVV	Public	Diploma
Security and Policing	EQF6 (bachelor)	UM FVV	Public	Diploma
Criminal Justice and Security Studies	EQF6 (bachelor)	UM FVV	Public	Diploma
	EQF7 (master)	UM FVV	Public	Diploma
	EQF8 (post-master, doctorate)	UM FVV	Public	Diploma
Cyber security	EQF6 (master)	FIŠ	Private	Degree
Programming	EQF4/5 (post-secondary/ tertiary VET)	Gea College	Private	Diploma
Information and cyber security program	EQF6 (bachelor)	Gea College	Private	Degree
Computer science and informatics	EQF7 (master)	UL FRI	Public	Diploma
Computing	European Qualification Level 5	Academia	Private	Degree
Web science and technologies	EQF7 (master)	Alma Mater	Private	Degree

Table 10: The study programs available for education in cybersecurity.

In addition to public and private educational institutions, various companies also offer shorter training programs. These training programs are typically tailored to the specific industry of the company that commissions the training, as shown in Table 11. The most common roles available in the training programs, such as Chief Information Security Officer (CISO), Architect, and Penetration Tester. However, while there are plenty of introductory courses in cybersecurity, with general introductions offered by several providers, the availability of specialized training programs is limited. This highlights a significant gap in opportunities for those seeking in-depth expertise in specific areas of cybersecurity, leaving much to be desired for professionals aiming to advance their knowledge beyond the basics.

Role	No. of providers	Required knowledge for application	Training summary
Chief Information Security Officer (CISO)	5	At least 5 years of experience in IT security.	Information security strategies, risk management, regulatory compliance, incident management.
Architect	3	Basic knowledge of IT architecture recommended.	Architectural planning, interior design, sustainable architecture.
Penetration Tester	2	Basic knowledge of IT security recommended.	Penetration testing of networks, applications and wireless networks, security assessments.
Risk Manager	2	Basic knowledge of IT security recommended.	Risk management, risk analysis, risk mitigation strategies.
Threat Intelligence Specialist	0	Basic knowledge of IT security recommended	Threat data collection and analysis, threat management strategies, practical exercises.
Auditor	2	None specified	Audit techniques, regulatory compliance, financial analysis.
Educator/Trainer	0	None specified	/
Researcher	2	Basic knowledge of IT security recommended	Research methods, writing scientific articles, obtaining funding.
Digital Forensics Investigator	2	None specified	Digital forensics, analysis of digital evidence, legal aspects of investigations.
General introduction to cybersecurity	7	No knowledge required	Cybersecurity basics, critical data protection, security risks, mobile device protection, encryption, risk management.

Table 11: Overview of providers and trainings available for specific roles in Slovenia.

5.3 Conclusions

The search revealed a diverse array of programs in Slovenia focusing on information security, cybersecurity, criminal justice, and related fields.

However, key findings indicate that there is a noticeable gap in the availability of education opportunities:

- While there is a significant presence of public institutions offering programs across multiple EQF levels, particularly in criminal justice and security studies, the range of available programs remains limited.
- Although private institutions contribute to the diversity of programs, particularly in specialized fields like cybersecurity and programming, the overall number of such offerings is insufficient to meet the growing demand.
- Despite the existence of programs designed to cater to various professional needs, from foundational education to advanced research and leadership roles, the options available may not be broad enough to adequately support all career paths in these rapidly evolving fields.
- Furthermore, many programs lack a focus on essential soft skills, such as communication, teamwork, and problem-solving, which are critical for professionals to succeed in multidisciplinary and dynamic environments.

6 Expert panel

6.1 Data collection

Organisation of the **Slovenian Expert Panel** was actively organised by the ICT Association of Slovenia at the Chamber of Commerce and Industry of Slovenia together with the Faculty of Electrical Engineering and Computer Science at the University of Maribor. Expert panel was 2 hours long and took place on 2nd July 2024, 13:00 - 15:00 hour. Because of the holiday period, expert panel was organised online (Teams platform) and included 18 different experts with diverse backgrounds, including:

- 1 Head of HR departments of cybersecurity providers or ICT companies,
- 1 Manager of recruitment agency specialising in cybersecurity/ ICT,
- 3 CISOs of large companies (responsible for cybersecurity/ ICT strategy),
- 3 CEOs of the ICT companies,
- 4 Professors specializing in cybersecurity at public and private universities,
- 1 Private education institute professional
- 1 Professional from the research institute,
- 2 Policy makers,
- 2 Representatives of the Cyber Security/ICT associations.

As part of the expert panel data collection process, participants discussed topic of cybersecurity roles, identified cybersecurity gaps in different cybersecurity trainings and gathered insights on the skills necessary for the cybersecurity experts. The panel meeting focused on analysing skill discrepancies on the market, developing strategies for enhancing cybersecurity skills, identifying issues on the cybersecurity field and creation of the draft action plan for the **CyberHubs Slovenia** platform. Preliminary results of the cybersecurity questionnaire for the Slovenia were presented as well at the expert panel and a feedback form the participants was collected.

6.2 Results

To gather information from the participants at the expert panel in Slovenia, a qualitative method was used. Discussion focused on three questions: (1) What will the demand for cybersecurity roles be in the next two years and in the long run, (2) What skills will be important in those roles in the next two years and in the long run and (3) What is the need for training/ education in the next two years and in the long run. Discussion on above three topics was open and took place on Mural platform (please see annex 1). Below are results that were brought up by the participants.

6.2.1 Cybersecurity roles

At the discussion on the cybersecurity roles, experts from the Slovenia highlighted several critical points. Firstly, there is a notable increase in cyber-attacks targeting human recourses, underscoring the need to invest in education of the teams on recognizing suspicious cyber behaviours. All experts agree that demand for the roles, who will have expert knowledge in cybersecurity (social engineering, phishing attacks, incident response), will increase in the coming years. There will be also increase in demand for the people who will have expert knowledge about the legal and business compliance with the current laws. Additionally, the integration of the AI into cybersecurity must be expanded beyond diagnostics to include response mechanisms. Looking ahead, the evolving role of AI in cybersecurity will necessitate a broader range of profiles within cybersecurity teams (Cyber security analyst with AI knowledge). Participating experts also agreed that we will need more experts in the future than we expect right now. Lastly, it is essential for the hub to establish a prioritized list of focus areas, distinguishing between essential services and those that are beneficial but not critical. Experts discussed also about the new, deep tech technologies that will have significant effect on the cybersecurity roles (f.i. quantum technologies) in the future.

Experts' quotations:

- *IT company representative*: *"AI in cybersecurity can be categorized into two main pillars: Integration of AI into business processes and incorporation of AI into incident response to counter AI-driven attacks. While one professional could handle a broad field five years ago, the rise of AI now requires three to five specialists to cover the same scope."*
- *Education institution representative: "One of the most pressing issues are currently cyber-attacks on human assets."*

6.2.2 Skills for cybersecurity professionals

The discussion on the second topic, about the necessary skills cybersecurity professionals will need, emphasized the importance of both technical and non-technical skills in the field. While technical expertise is crucial, soft skills such as effective communication with end-users, teamwork, and managing diverse personalities are equally vital. In the realm of cybersecurity, the need extends beyond industry professionals to include educators as well. Additionally, there is a significant need for personnel management skills within teams. Individuals who can manage and understand the unique personalities often found in the IT world are essential to building effective teams.

Experts' quotations:

- *IT company representative: "A cyber security expert is someone who can be equated with a virtuoso on the violin, someone who sees the world in a very different way. It is a special type of personality that requires a special way of leading and managing. Such personalities rarely accept a person above them to lead and manage them, so they have problems with authority that is above them. This is why we urgently need people to manage personnel as part of the cyber security team."*

6.2.3 Training of cybersecurity professionals

The discussion about trainings highlighted several key points regarding IT and cybersecurity education in Slovenia. Firstly, there is a need to enhance basic IT education and understanding among high school students. At the university level, while cybersecurity experts receive extensive general IT knowledge, there is a lack of specialized niche cybersecurity training, and the duration of training programs needs to be reduced. Additionally, the number of students enrolling in technical and IT universities is decreasing, necessitating an increase in enrolment places by the government. Slovenia's slow pace in implementing changes was also noted, with a call for the industry to organize concrete projects to drive progress. Lastly, there is a need for a central institution or connection link to bring together all stakeholders, including educational organizations, faculties, high schools, and companies, to foster collaboration and advancement.

Experts' quotations:

- *Education institution representative: "The students coming from high schools lacks basic computer literacy."*
- *Education institution representative: "In the future, we need to build on the IT basis and then on this basis, build on cybersecurity knowledge. Cybersecurity skills are unique and niche."*

6.3 Conclusions

In the context of the CyberHubs project, the Slovenian expert panel highlighted several critical insights:

- **Lifelong learning** is essential for all cybersecurity professionals to remain adaptable in a rapidly evolving field.
- Team leads must be educated in **soft skills** to effectively manage and lead expert teams.
- Fostering **collaboration between industry and educational organizations**—both private and public—bridges knowledge gaps and prepares graduates for real-world challenges.
- There is a need for **shorter and targeted trainings** on niche topics, which enhances skill of the experts.

The demand for the cybersecurity roles and related skills and trainings will be high in the coming years. The establishment of the Slovenian cybersecurity hub will therefore serve as a central hub to enable cooperation and facilitate knowledge sharing among various cybersecurity players in Slovenia.

7 Conclusions

7.1 Cybersecurity roles

The different desk research approaches do not consistently use ENISA role definitions, though an approximate mapping between them is possible. One significant shortcoming of labour market reports is that they do not include key roles such as Incident Responder, Cybersecurity Implementer/Expert, and Cyber Legal, Policy & Compliance Officer. When discrepancies occur between analyses, it is advisable to prioritize the most recent data, given the highly dynamic nature of the field.

The most relevant desk research indicates that the highest demand is for technical roles. This finding is supported by the questionnaire, expert panel, and job vacancy analysis. Moreover, companies have stated, both in job advertisements and directly, that if they cannot find a candidate with sufficient cybersecurity knowledge, they seek individuals with a strong foundation in IT systems whom they can further train. This clearly reinforces the conclusion that current training programs are unable to fully meet these needs.

Therefore, the following roles should be prioritized for development in this order:

1. Cybersecurity implementer/expert and (Chief) Information Security Officer/ Manager.
2. Incident responder and Penetration Tester.
3. Cybersecurity Auditor, Cyber Threat Intelligence Specialist.
4. Cybersecurity Architect.

7.2 Skills for cybersecurity professionals

All desk research and analysis consistently highlight a strong demand for Cybersecurity and IT-related skills, indicating these areas as critical across various sectors. Even more, certifications are regularly requested in job postings as a proof of knowledge. However, when it comes to soft/transversal and organization-related skills, the perceived need is more varied, with some of these skills being regarded as less essential by certain studies.

Despite these differences, to effectively address the overall needs, the recommendation is to prioritize and focus on the most in-demand skills, ensuring that the most critical areas are adequately covered. The key skills are:

- **Cybersecurity skills**: Incident Management, Threat Analysis, Communications Security, Cloud Security, Information Systems & Network Security/Cyber Resiliency, Incident Management and Access Controls/ Identity Management, Data Privacy.
- **IT related skills:** System Administration & Integration, Data Analysis, Network Management, Software Development & Computer Languages, Enterprise Architecture & Infrastructure Design and Operating Systems, Testing and Evaluation and Database Administration.
- **Organization-related** skills: Risk Management, Business Continuity, Process, Strategic Relationship Management and Strategic Planning.
- **Soft/transversal** skills: Problem-solving, Acting Responsibly, Acting Independently, Communication, Leadership, Collaborate in teams, Analytical thinking and Ethical Behaviour.

However, it is crucial that the hub not only keeps pace with the latest technology trends but also anticipates the skills needed in the future. The hub's role is to align these projections with industry and coordinate with educational organizations to ensure these skills are incorporated into training programs.

7.3 Training of cybersecurity professionals

Educational institutions have only recently started offering programs in cybersecurity. These programs primarily focus on IT and cybersecurity skills, with significantly less emphasis on organization-related skills and even less on soft/transversal skills. Additionally, the number of available spots per year is limited, and there is still a lack of awareness among young people about this career path. Given that student dropout rates are also an issue, current capacities do not meet the existing demand for qualified professionals.

On the other hand, the industry is well accustomed to upskilling its workforce, and this continues to be the primary method of education. Collaboration between industry and educational institutions is strong, with many events organized to help students engage with companies. As a result, many students secure employment before completing their studies, and the industry is gradually adapting to this new talent pipeline.

Providing formal education and certifications that target the most in-demand roles and skills will reshape the approach to both hiring and upskilling. Additionally, there is a pressing need to expand lifelong learning programs, particularly those focused on specialized or niche topics, which would result in shorter, more targeted education and reduce the time required for upskilling and reskilling.

Furthermore, the industry will be better positioned to accommodate employees taking time off for training, with the added advantage of learning not only from their colleagues but from professionals and specialized training content. This is especially important as many companies lack employees with the full range of necessary skills, particularly in soft and organization-related areas.

Following activities are proposed:

1. Align with the industry on content, especially in the areas of organization-related skills, and soft/transversal skills, to be incorporated into the curricula of educational organizations.
2. Engage with educational organizations to explore the inclusion of skills training based on industry needs in their curricula.
3. Explore the possibility of offering more certification-based training through educational organizations.
4. Hub could organize courses covering content that is not currently offered by educational organizations.

7.4 Summary

While working on this study, additional insights were gathered from conferences and discussions with representatives from industry, including:

- Younger cybersecurity professionals are seeking opportunities abroad, either through remote jobs or relocation to countries, offering them better conditions.
- For several years Slovenian ICT companies are being sold to foreign owners mostly to well-known ICT corporations, which aim to expand their work but also get additional resources. The influence on Slovenian market is exacerbating the local talent gap.
- Major ICT companies have established internal training programs focusing on specific cybersecurity and IT skills but continue to report a need for more cybersecurity professionals.

While the exact size of the talent gap is difficult to calculate, it is clear that formal education currently delivers around 50 bachelor's degrees and up to 20 master's degrees per year in various cybersecurity roles. Additional cybersecurity courses are offered as part of broader computer science and informatics programs, but it is unclear how many graduates pursue careers in cybersecurity.

On the demand side, the current need for professionals exceeds the available supply, and this gap is expected to widen. New regulations such as NIS-2, combined with the increasing frequency of cyber-attacks, will drive even higher demand for cybersecurity professionals, further increasing the gap.

Establishing a CyberHub can significantly enhance the national cybersecurity landscape by bringing together all relevant stakeholders, including students. The hub can support education and certification in the most critical roles and skills required by the industry. By promoting the cybersecurity profession, fostering lifelong learning, and strengthening collaboration between industry and educational institutions, the hub will help close the skills gap and ensure a steady pipeline of qualified professionals capable of meeting the demands of the labour market.

8 References

DIGITAL SLOVENIA 2030: An Overarching Strategy for Slovenia's Digital Transformation by 2030. (2023).

Dušek, T. (2022). *OZAVEŠČENOST O INFORMACIJSKI VARNOSTI V POLICIJSKI UPRAVI LJUBLJANA Diplomsko delo*.

Gergorić, I., & Lampe, A. (2021). *Katalog IKT kompetenc*.

Kocbek, N., & Lampe, A. (2021). *Poročilo o preverjanju in aktualizaciji napovedanih profilov in kompetenc IKT Horizontalna mreža, SRIP PMIS*.

Kompara, M., Nemec Zlatolas, L., Hölbl, M., Welzer Družovec, T., Bošnjak, L., Vodopivec, P., Gabor, M., & Turkanović, M. (2022). *Celovit pregled in analiza izobraževanj na področju kibernetske varnosti*.

Kompara, M., Nemec Zlatolas, L., Hölbl, M., Welzer Družovec, T., Taneski, V., & Turkanović, M. (2022). *Analiza pomembnosti kompetenc na področju kibernetske varnosti*.

Maček, S., Mulec, F., & Močilar, F. (2018). *Prizadevanja Slovenije za obvladovanje groženj v kibernetskem prostoru*.

Markun, A. (2023). *VLOGA SKRBNIKA INFORMACIJSKE VARNOSTI V PODJETJU X*.

Napovedovanje potreb po kadrih na področju digitalnih profilov. (2023). http://dihslovenia.si

Prislan, K. (2012). *Slovenska perspektiva informacijskega bojevanja z vidika kibernetske kriminalitete*.

Štrucl, D. (2021). *National Cybersecurity Organization: Slovenia*.

Urajnar, K. (2023). *OBVLADOVANJE KIBERNETSKIH TVEGANJ ZAPOSLENIH V JUGOVZHODNI SLOVENIJI*.

Zupančič, K. (2020). *UNIVERZA V LJUBLJANI FAKULTETA ZA UPRAVO Magistrsko delo ANALIZA PRAVNEGA UREJANJA KIBERNETSKE VARNOSTI V SLOVENIJI IN EU*.

9 Annexes

9.1 Annex 1: Mural questionnaire for Expert Panel

The Mural questionnaire is available here:

https://app.mural.co/t/projektnagzs5793/m/projektnagzs5793/1718364803559/8d9d0c78f79a917cd424cd55319aef60262dcbba?sender=u18986120876b995c91030616

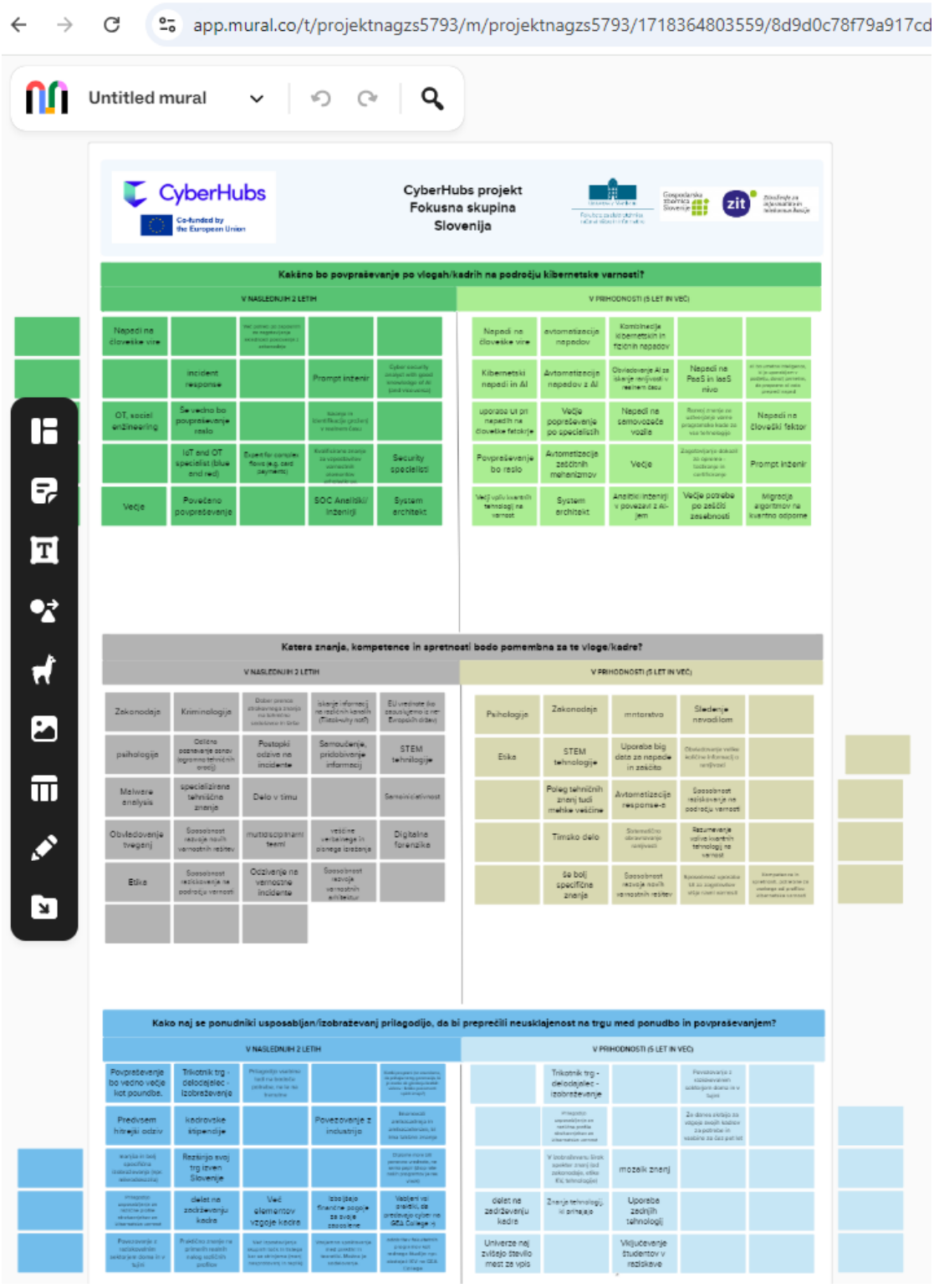

Figure 25: Slovenian CyberHubs Expert Panel - Mural questionnaire

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.