Competency Requirements for the Juniors in the Finnish Cybersecurity Service and Consultancy Business

Pasi Kämppi[1], Jani Ekqvist[2] and Jyri Rajamäki[1]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]Turku University of Applied Sciences, Turku, Finland

pasi.kamppi@laurea.fi
jani.ekqvist@turkuamk.fi
jyri.rajamaki@laurea.fi

Abstract: Fresh graduates or career changers face challenges entering the competitive cybersecurity job market. Cybersecurity is evolving rapidly, and even professionals must put in extra effort to keep themselves updated and competent. Most existing studies on the competency requirements in the Finnish job market are based on surveys, literature reviews, and trends, and in-depth work-life skills analysis is limited. This phenomenon makes Finnish higher education institutes' work challenging because they need to train graduates for the local, European and global job markets with relevant work-life skills, and in-depth input from the workforce is essential. This study aims to find more in-depth input from the work-life. It identifies the work-life skills required in the cybersecurity service and consultancy business, particularly for junior-level positions available to fresh graduates in the Finnish job market. The case study is based on in-depth interviews with eight representatives from five companies that offer cybersecurity services in Finland. The interviewees had 5 to 24 years of working experience and represented positions ranging from technical experts to directors. The data was analyzed using an AI-aided analysis methodology, the enhanced European Joint Research Center Cybersecurity Taxonomy and the European Catalogue of Soft Skills References to ensure a comprehensive and job market-compliant outcome covering hard and soft skills. The results show that traditional cybersecurity competencies, including software, hardware, and network security, are still the most valued in the hard skills category. Still, incident handling and information security management skills are essential as well. Employers highly value soft skills such as problem-solving, critical thinking, communication, and teamwork. In summary, Finnish higher education institutes should ensure that both skill categories are covered in their training programs.

Keywords: Cybersecurity competency, Hard skills, Soft skills

1. Introduction

The cybersecurity domain is constantly suffering from the need for a competent workforce. One of the most prominent cybersecurity associations, the International Information Systems Security Certification Consortium (ISC2), publishes its studies yearly, and the study published in 2024 reveals that the problem has remained the same during the last three years (ISC2, 2024). According to their report, the cybersecurity workforce gap has grown from 3.4 million employees to 4.8 million employees from the year 2022 to the year 2024 (ISC2, 2024). Another well-known association, the Information Systems Audit and Control Association (ISACA), publishes its surveys annually, and their results considerably amplify ISC2's observations. ISACA's annual report on 2023 states that over 60% of respondents indicated that they are at least somewhat understaffed (ISACA, 2023). In Finland, over 70% of organizations (businesses, authorities, and the third sector) suffer from a cybersecurity skill gap (Lehto *et al.*, 2022). In the long term, this phenomenon can lead to a snowball effect where the business life, authorities, and the third sector suffer from the lack of qualified workforce while the personnel is aging, and junior-level applicants have difficulties entering the work market.

The phenomena mentioned above raise an interesting question: How should Finnish higher education institutions (HEIs) educate and train graduates to be equipped with skills that match current work-life requirements in cybersecurity? The question has been partly covered by Lehto et al. (2022) and Saharinen (2023), but their studies are based on surveys, trends, and literature reviews, and an in-depth analysis of hard and soft skills requirements is limited. Niemelä (2019) enriched his job ad-based analysis with interviews. Still, the results focused more on educational capacity and quality than hard and soft skills needed in the cybersecurity job market.

This study examines the hard and soft skills required in the Finnish cybersecurity service and consultancy business. More specifically, it seeks to provide insights into the hard and soft skills most valued by employers when hiring fresh graduates or entry-level professionals. The research examines hard and soft skills by conducting in-depth interviews with experienced professionals from leading cybersecurity companies in the Finnish cybersecurity services and consulting business, offering a comprehensive understanding of what is needed to succeed in entry-level roles.

The article is structured as follows: Section two elaborates on related research, surveys, and applied theoretical frameworks for thematic data analysis. Section three focuses on the research methodology and questions. Section four presents research results, and section five discusses research findings.

2. Related Studies

The skills required in cybersecurity are discussed in many research papers, surveys and reports. A prevalent finding is that cybersecurity is a diverse working domain and hard and soft skills are needed (Potter and Vickers, 2015; Dawson and Thomson, 2018; Jones, Namin and Armstrong, 2018; ISACA, 2023; ISC2, 2023). It is also argued that cybersecurity is seen as a technical domain (Haney and Lutters, 2021), and educational institutes focus on technical topics in their curricula (Cinque, 2016).

Technical expertise and related hard skills vary across different cybersecurity roles (Potter and Vickers, 2015; Armstrong *et al.*, 2020). For example, common hard skills for security analysts, consultants, and engineers include network security, incident response, vulnerability assessment, penetration testing, security frameworks and standards, and threat and risk assessment (Potter and Vickers, 2015). The report published by ISC2 in 2023 mentioned that artificial intelligence (AI) and machine learning (ML) have climbed the list of skills in demand (ISC2, 2023). At the same time, entry-level candidates should manage fundamental skills, including networking and programming (Jones, Namin and Armstrong, 2018).

Maria Cinque (2016) highlighted in her paper the growing importance of soft skills for employability, particularly for recent graduates entering the labor market. The paper discusses how graduates often need more non-technical skills, such as communication, teamwork, and problem-solving, despite needing to be more technically prepared. The ISACA amplifies the phenomenon in its annual report, stating how soft skills are becoming the most significant skill gap among graduates (ISACA, 2023). Interestingly, among 57 interviews at two cybersecurity conferences, soft skills were often mentioned as a skill set they wish they had learned in school (Jones, Namin and Armstrong, 2018).

Few studies in the Finnish context focus on competency requirements in the Finnish job market (Niemelä, 2019; Lehto *et al.*, 2022; Saharinen, 2023). Surveys and literature reviews conducted by Lehto et Al. (2022) and Saharinen (2023) focus more on how Finnish higher education matches work-life needs than on what hard and soft skills should be achieved. Niemelä (2019) enriched his survey with five interviews, but in-depth analysis of required hard and soft skills in the Finnish job market is limited.

Employers emphasize hard and soft skills as critical for job success. According to the ISACA report (2023), only 26 percent of respondents believed that approximately half of the applicants were well-qualified. There is a mismatch between what universities teach and what employers need, with only 35% of employers believing that graduates are adequately prepared (Cinque, 2016). Ultimately, it advocates for curriculum reform to close the gap between education and labor market demands. These insights suggest that success in cybersecurity demands a holistic skill set combining hard and soft skills. Haney and Lutters (2021) indicate that cybersecurity work should be repositioned more as a people-oriented service profession than a purely technically oriented working environment. In the Finnish context, there is room for further analysis of hard and soft skills requirements in the Finnish job market.

2.1 Definitions for Hard Skills

The categories of hard skills in cybersecurity in this study follow the European Cybersecurity Taxonomy (ECT) by the European Commission Joint Research Centre (JRC), (Nai, Hernandez and Neisse, 2022) which has been refined by the work of Hakkala et al. (2023). The taxonomy is divided into 16 categories (Figure 1). This provides us with a precise categorization of topics and allows the mapping of industry skills requirements to curriculum content on a sufficiently high level while avoiding the direct coupling to work roles in contrast to frameworks like the European Cyber Security Framework (ECSF) by ENISA and Workforce Framework for Cybersecurity (NICE Framework) by National Institute of Standards and Technology (NIST).

1. Assurance, audit and certification
2. Cryptology (Cryptography and cryptanalysis)
3. Data Security and Privacy
4. Education and Training
5. Human Aspects
6. Identity Management
7. Incident Handling and Digital Forensics
8. Legal Aspects
9. Network and Distributed Systems
10. Security Management and Governance
11. Security Measurements
12. Software and Hardware Security Engineering
13. Steganography, Steganalysis and Watermarking
14. Theoretical Foundations
15. Trust Management and Accountability
16. Artificial Intelligence and Machine Learning

Figure 1: Skills taxonomy for cybersecurity (Hakkala et al., 2023).

2.2 Definitions for Soft Skills

In this study, the European Catalogue of Soft Skills References by the European Soft Skills project (2021) was selected for categorizing soft skills. It is aimed at evaluating the primary soft skills required for employment and is thus aligned with the objectives of this study. It was assessed to be comprehensive while averting unnecessary detail that would have caused undue burden on the respondents. The European Catalogue of Soft Skills defines five categories: growth mindset, reliability, self-awareness, interactions and commitment. Furthermore, four primary skills are defined for each category (Figure 2). The defined skills were used as the basis of the analysis. During the study of the interviews, it became evident that the skill category of problem-solving and decision-making needs to be sufficiently represented in the selected framework. Thus, it was introduced into the model.

Growth mindset	**Self-awareness**	**Commitment**	**Reliability**	**Interactions**
Learning to learn	Self-reflection	Sense of organization	Respect of rules	Communication
Autonomy	Self-confidence	Sense of responsibility	Efficiency	Leadership
Adaptability	Emotional intelligence	Taking initiative	Conscientious-ness at work	Teamwork
Accepting professional remarks	Presentation	Ability to anticipate	Sense of ethics	Assertiveness

Figure 2: Taxonomy for soft skills (Soft Skills Project, 2021)

3. Research Methodology

This study was made as a single case study. According to Yin (2013), the case study is applicable when researchers investigate a contemporary real-world phenomenon and the research questions aim to answer questions such as what, how, and why. Yin (2013) also recommends collecting evidence from multiple sources of case study and defining a precise data analysis methodology. For a single case study, Gerring (2006) states that a researcher gains better within-case evidence with fewer carefully selected homogenous cases than an extreme case heterogeneity with a higher sample rate. According to Marshall et al. (2015), there are no strict guidelines for the sample size in Information Systems (IS) case study research, and it is case-dependent when the data starts to saturate.

This study aims to gain a deeper understanding of the skills needed for junior-level positions in the Finnish cybersecurity service and consulting business, so it investigates a real-world phenomenon with a solid single-case focus. The deeper understanding refers to two research questions:

- What skills are required in the Finnish cybersecurity service and consultancy business for junior-level positions?
- Why are found skills valued in the Finnish cybersecurity service and consultancy business for junior-level positions?

The primary sources of the case study evidence are interviews, surveys, and other researchers' research contributions. The interview data was analyzed thematically into hard and soft skills by an artificial intelligence (AI)-based large language model (LLM) and then matched manually with the enhanced European Joint Research Center's Cybersecurity Taxonomy (Hakkala *et al.*, 2023) and the European Soft Skills Framework (Soft Skills Project, 2021).

In practice, the study applied AI to transcribing online interviews and LLM-based (ChatGPT 4o) thematic data analysis. According to Hou et al. (2024), LLM-based qualitative data analysis is a reliable methodology, but Nejjar et al. (2024) remind us that researchers should select the applied LLM model carefully. The ChatGPT has been used successfully in the medical sector (Ayers *et al.*, 2023; Mirzaei, Amini and Esmaeilzadeh, 2024) and was considered a rigorous reference for this study.

The LLM model (ChatGPT 4o) was fed with a transcript one by one, and then it was prompted to find ten hard skills and ten soft skills. The results were copied into a spreadsheet and researchers made the pattern matching manually with selected frameworks. Notably, the LLM model (ChatGPT 4o) was not prompted to focus on cybersecurity-related competencies or was not trained specifically for this task. The results were checked by the researchers who conducted the interviews. The AI-assisted case study research process is described in Figure 3.

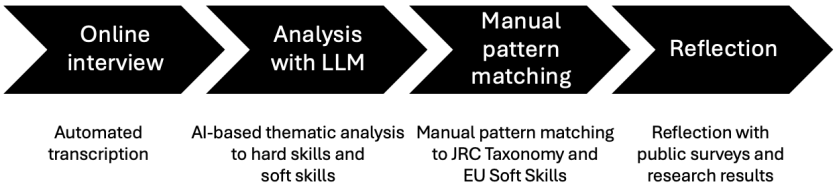

Figure 3: AI-assisted case study research process

4. Results

The research was conducted among five cybersecurity services and consultancy companies represented by eight Finnish professionals. Selected companies represent 13% of the members in the consulting and service business of the Finnish Information Security Cluster (FISC) (Finnish Information Security Cluster, 2024). The interviewees' working experience varied from 5 to 24 years, and they belonged to different work roles, including two Human Resource (HR) specialists, an incident responder, a team leader, a senior manager, and three executive-level directors. Each interview took 60-120 minutes, and the interviewer had a brief agenda, and he gave freedom to interviewees expressing their thoughts freely. However, the interviewer asked more focused questions whenever needed regarding the topic being discussed. The demography of the interviewees is presented in Table 1.

Table 1: Demography of interviewees

Industry	Interviewees business unit	Interviewee's role	Interviewee's working experience
Consulting	Cybersecurity Consulting	Director	20 years
Consulting	Human Resources	Talent Acquisition Specialist	9 years
Consulting	Human Resources	Talent Acquisition Consultant	14 years
IT-service provider	Security Operation Center	Director	24 years
IT-service provider and consulting	Cybersecurity	Head of Business	24 years
IT-service provider and consulting	Security Delivery	Senior Manager	17 years
Telecommunications	Digital Forensics, Incident Response, Threat Hunting	Incident Responder	5 years
Telecommunications	Cybersecurity Service Delivery Management	Team Leader	19 years

4.1 Hard Skills

The LLM model (ChatGPT 4o) was asked to find ten hard skills from each transcription individually, resulting in 80 data points to be analyzed with eight interviewees. After the LLM thematic analysis, the data points were matched manually according to the enhanced European Joint Research Center's Cybersecurity Taxonomy (Hakkala *et al.*, 2023).

According to the analysis, the most valued enhanced JRC categories are Software and Hardware Security Engineering (31%) and Network and Distributed Systems (29%). The third most valued category is Incident Handling and Digital Forensics (14%), the fourth most valued is Security Management and Governance (11%), and the fifth most valued is Assurance, Audit and Governance (8%). The results are presented in Figure 4.

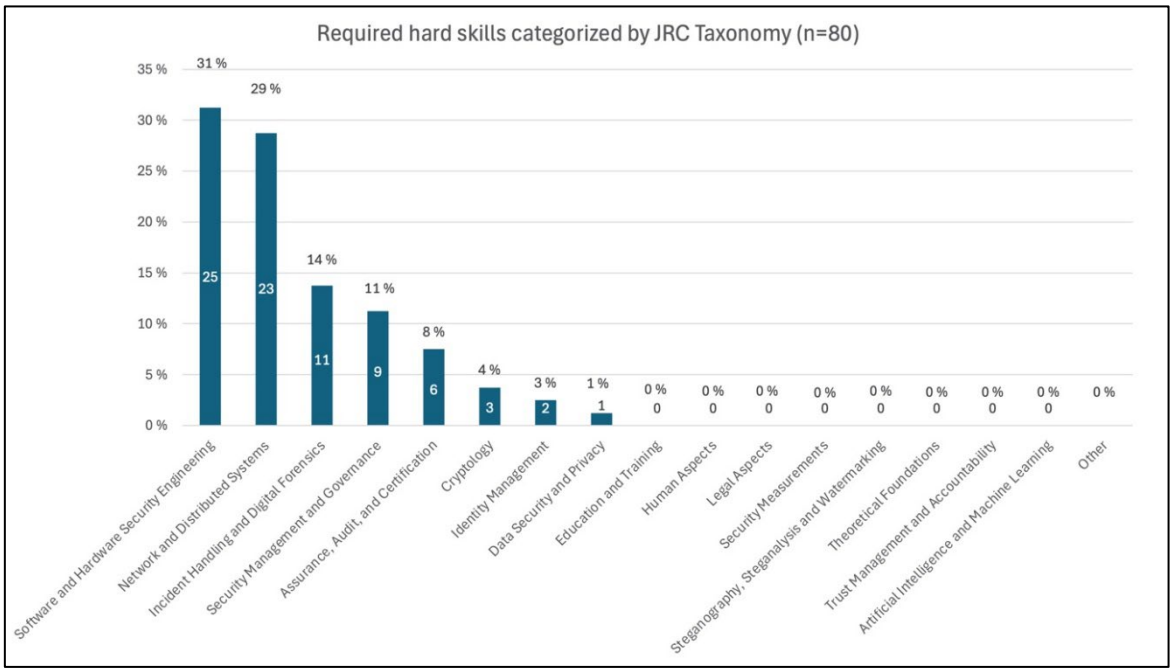

Figure 4: Required hard skills categorized by enhanced JRC Taxonomy

According to the interviewees, having good foundational knowledge and understanding of networks and IT services is necessary because it enables building deeper cybersecurity competency on top of a good foundation, which explains why the category Network and Distributed Systems was valued in the top two categories. More specifically, IP networking, cloud services (AWS, Azure, Google), operating systems (Linux, Windows), and databases (SQL, NoSQL) were mentioned. Notably, the respondents did not necessarily expect graduates to have deep cybersecurity competency in networking and distributed systems, but the foundation should be strong enough.

The other equally valued category, Software and Hardware Security, also has a reasonable justification. The respondents indicated that when graduates can manage one programming language well, it is easy to learn other programming languages if necessary. However, excellent programming skills are not essential, but basic programming skills help tremendously when building your toolkits, scripts, and applets. For example, the interviewees identified Python, Java, C++, Bash, and PowerShell. Additionally, fundamental vulnerability- and penetration testing skills associated with good reporting skills are valuable.

The third most valued category, Incident Handling and Digital Forensics, typically requires more advanced competencies. Still, one tool, Security Information and Event Management (SIEM), was identified and should be in every junior's toolbox. When junior cybersecurity specialists can manage SIEM, starting work as a junior cybersecurity specialist in a Security Operation Center (SOC) is much easier.

The fourth most valued Security Management and Governance refers to information security-related standards and regulations. The interviewees mentioned a few examples, such as ISO27001, General Data Protection Regulation (GDPR), Network and Information Security Directive 2 (NIS2), Information Technology Infrastructure Library (ITIL), and risk management practices. They highlighted that every cybersecurity professional should understand how information security is managed in a company and how cybersecurity is regulated at the European level.

The fifth most valued Assurance, Audit, and Governance was associated with individual professional certificates. The respondents said that professional certificates are essential in the consultancy business when a customer requires consultants' competency to be validated by accredited means.

4.2 Soft Skills

The LLM model (ChatGPT 4o) was asked to find ten soft skills from each transcription individually, making 80 data points to be analyzed when we had eight interviewees. After LLM thematic analysis, the data points were matched manually to the European Soft Skills Catalogue References (Soft Skills Project, 2021). The results of the analysis are presented in Figure 5. The most important skills were problem-solving and decision-making (16%), followed by communication (14%) and teamwork (11%). Other significant skills were adaptability (10%), emotional intelligence (8%) and learning to learn (8%).

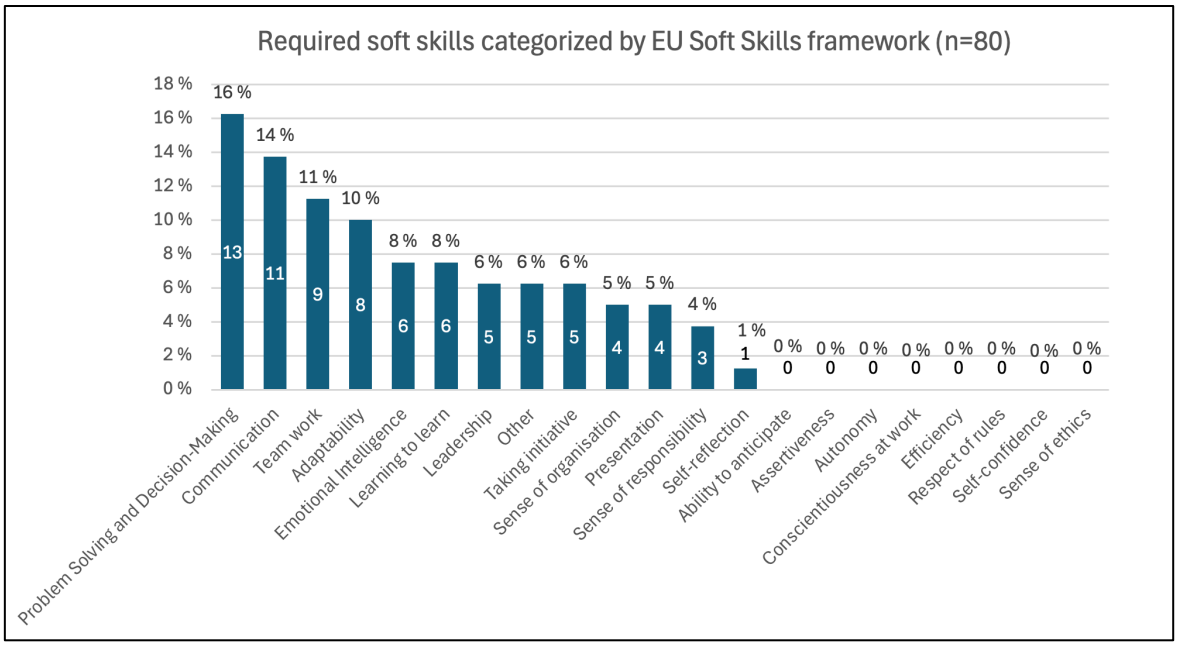

Figure 5: Required soft skills categorized by EU Soft Skills

The importance of problem-solving is understandable in cybersecurity as most work tasks aim to prevent problems from occurring or solve them once they have happened. The interviews mentioned structured thinking processes like analytical, logical, and causal thinking as contributing to good problem-solving skills. The interviewees represent consulting and service providers, where the relationship with customers is of utmost importance to the continuity and growth of business. Good communication skills enable employees to work effectively with customers and colleagues, and emotional intelligence helps solve conflicting situations. Both internal and external, as well as written and oral communication, were deemed necessary. The ability to simplify complex issues and explain them understandably was also mentioned, which is also often attributed to domain expertise in relevant hard skills. Improvement of technical cybersecurity typically requires changes in several systems, and similarly, cybersecurity governance touches several business functions to be effective. This is markedly easier with good communication and teamwork skills. Cybersecurity is also an ever-changing field where adaptability and the ability for learning to learn are essential.

4.3 Comparison to the Global Context

This section compares the interview findings to the latest surveys published by ISC2 and ISACA. Tables 2 and 3 compare the top five hard and soft skills from interviews, the ISC2 2023 report, and the ISACA 2023 report, complemented by lower ranking skills if they were not matched among the top five skills. The skills are ordered based on their rankings and occurrences in the individual studies.

4.3.1 Hard skills comparison

Table 2 shows clearly that hard skills in the enhanced categories of Network and Distributed Systems, Incident Handling and Digital Forensics, and Software and Hardware Security Engineering are in high demand on a global scale, and there are reasons behind that. According to surveys by ISACA (2023) and ISC (2023), companies are migrating their data centers to the cloud and creating a skill gap in the cybersecurity domain due to high workforce demand. Secondly, modern businesses rely heavily on IT systems, and it is necessary to recover from incidents as soon as possible to minimize downtime and the impact of data breaches and learn how to avoid such incidents in the future (ISACA, 2023; ISC2, 2023). In the context of ISC2 2023- and ISACA 2023 reports,

software and hardware security engineering refers to the whole software, application, and hardware development lifecycle. Still, in the cybersecurity service business, e.g., in SOC, it is associated with the capability for developing small tools, applets, scripts, SIEM security rules and automation, which makes specialists' work more efficient and robust. According to the enhanced JRC taxonomy, vulnerability scanning and penetration testing are also included in this category. It can be assumed that if a job applicant manages the aforementioned hard skills, the possibility of getting a job is higher.

Table 2: Hard skills comparison between interviews in this study, ISC 2023 survey and ISACA 2023 survey

	Interviews in this study	ISC2 (2023)	ISACA (2023)	
1.	2. Network and Distributed Systems	1. Cloud computing security	2. Cloud computing	
2.	3. Incident Handling and Digital Forensics	3. Security analysis	4. Incident response	
3.	1. Software and Hardware Security Engineering	4. Security engineering	5. Development, Security and Operations	
4.	4. Security Management and Governance	2. Risk assessment, analysis, and management 5. Governance, Risk Management and Compliance (GRC)	Not mentioned as a skill in demand	Assurance, Audit and Certification
5.	8. Identity Management	9. Identity and access management	1. Identity and access management	
6.	9. Data Security and Privacy	Zero Trust *	3. Data protection	
7.	N/A	Artificial Intelligence/Machine Learning (AI/ML) *	Mentioned as possibility of mitigating skill gaps	
	*) Mentioned as important skills by non-hiring employers			

Both reports, ISC2 2023 and ISACA 2023, state that effective risk management enables companies to proactively manage cybersecurity threats by identifying, assessing, and mitigating risks. The interviewees highlighted that it is necessary to adopt risk-based thinking from the beginning when a person enters to cybersecurity domain.

The assurance, audit, and certifications skills, marked as the fifth most important skill in the interview analysis, turned to discussing personal qualifications and certifications. In this study, personal certifications are set as a cross-cutting theme that makes it possible to verify competency in any cybersecurity subdomain.

The last three skill groups have a significant deviation among the studies. Identity and access management is essential as a preventive cybersecurity control, but it is not necessarily among the vital skills a fresh graduate should manage. The same concerns data security and privacy; a fresh graduate should be able to work according to security and privacy regulations, e.g., GDPR, but they are not expected to able to implement all security controls ordered by a regulation. The last ones, artificial intelligence (AI) and machine learning (ML) are seen as great possibilities, but the interviewees said that it would take time until AI-based solutions are financially profitable in the cybersecurity and consultancy business.

4.3.2 Soft skills comparison

Table 3 compares soft skills identified in this study to those deemed most important in ISC2 2023 and ISACA 2023 studies. Problem-solving, communication and teamwork are the three most essential skills in all three surveys. Strategic thinking, in fourth place by ISC2 (2023), and critical thinking, second in ISACA (2023), have been included in the first category, problem-solving and decision-making, in our study. These results in cybersecurity are in line with the engineering field in general. A literature review by de Campos et al. (2020) found that the six most important soft skills for the employability of engineers are problem-solving and critical thinking, communication, teamwork, ethical perspective, emotional intelligence, and creative thinking.

Notably, according to the ISACA 2023 report, soft skills remain the most significant skill gap among university graduates and the second largest for junior cybersecurity professionals. Similarly, in the ISC2 2023 report, problem-solving, eagerness to learn, and communication are valued above cybersecurity skills, qualifications, and certifications as the essential qualifications for cybersecurity professionals seeking employment. When comparing our results to the global cybersecurity workforce studies and studies on the engineering profession, it can be seen that there is demand for more soft skills-oriented teaching and what the focus areas should be.

For problem-solving, decision-making, and critical thinking, problem-based learning (PBL) is a well-studied methodology in engineering education (Mills and Treagust, 2020; Chen, Kolmos and Du, 2021). It is often practiced with project-based learning, which works well on teaching the second and third most critical soft skills in the study, communication, and teamwork.

Table 3: Soft skills comparison between interviews in this study, ISC 2023 survey and ISACA 2023 survey

	Interviews in this study	ISC2 (2023)	ISACA (2023)
1.	1. Problem Solving and Decision Making	1. Problem-solving abilities 4. Strategic thinking	2. Critical thinking 3. Problem-solving
2.	2. Communication	3. Communication skills	1. Communication
3.	3. Teamwork	5. Coaching/Team development skills	4. Teamwork
4.	4. Adaptability	N/A	Included in Communication
5.	5. Emotional Intelligence	N/A	13. Conflict resolution
6.	6. Learning to Learn	2. Curiosity/Eagerness to learn	N/A
7.	N/A	N/A	5. Attention to detail

5. Discussion

The cybersecurity service and consultancy business requires a well-balanced skill set, which includes hard and soft skills. Due to the service-oriented approach, the consultants should be able to solve technical problems and be team players under high workload and pressure. However, cybersecurity is seen as a technical working environment, leading to situations where students may neglect soft skills in their skill portfolio and higher education institutes are missing adequate training for soft skills in their curricula. The report published by ISACA in 2023 states that soft skills are becoming the most significant skill gap among graduates.

However, based on the results of this study, a few recommendations can be shared for building a more balanced skill set for fresh graduates. The most important hard skills in the service and consultancy business are good knowledge and understanding of IT networks and systems. IT network and system skills are necessary when consultants analyze and solve complex customer IT system problems, and they create a good platform for further professional development. The second most valuable hard skills are fundamentals in programming, scripting, operating systems and penetration testing. Consultants rarely develop new services and applications in the service and consultancy business. Still, they use their capability to create small tools, applets, and scripts that make their work more efficient and robust. Other considerable hard skills are the basics of incident management and an understanding of cybersecurity-related laws, regulations and frameworks.

In the soft skills category, problem-solving is the most valued skill in the service and consultancy business. This is understandable because solving customers' problems is the heart of the business model in the service and consultancy business. Other relevant soft skills are communication, teamwork, adaptability, and emotional intelligence, which are necessary when the consultants act as an interface between the service provider and the customer.

The main limitation of this study is the relatively small sample size of interviewees (n=8), and the results could be double-checked with additional interviews. However, the findings of this study are well aligned with the global trends, and international surveys amplify the results of the national studies in Finland.

In conclusion, training for hard skills is still crucial, but soft skills need special attention due to increased work-life demands. By including the most essential hard- and soft-skills training in their curricula, higher education institutions can prepare graduates for the national and global cybersecurity job markets in the best possible way.

Acknowledgements

The research is conducted in a collaboration project where Finnish higher education institutions aim to develop cybersecurity education in Finland. The project is funded by the Ministry of Education and Culture.

References

Armstrong, M.E., Jones, K.S., Namin, A.S. and Newton, D.C. (2020) 'Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals', *ACM Transactions on Computing Education*, 20(4), pp. 1–25. Available at: https://doi.org/10.1145/3421254.

Ayers, J.W., Poliak, A., Dredze, M., Leas, E.C., Zhu, Z., Kelley, J.B., Faix, D.J., Goodman, A.M., Longhurst, C.A., Hogarth, M. and Smith, D.M. (2023) 'Comparing Physician and Artificial Intelligence Chatbot Responses to Patient Questions Posted to a Public Social Media Forum', *JAMA Internal Medicine*, 183(6), pp. 589–596. Available at: https://doi.org/10.1001/jamainternmed.2023.1838.

Campos, D.B. de, Resende, L.M.M. de and Fagundes, A.B. (2020) 'The Importance of Soft Skills for the Engineering', *Creative Education*, 11(8), pp. 1504–1520. Available at: https://doi.org/10.4236/ce.2020.118109.

Chen, J., Kolmos, A. and Du, X. (2021) 'Forms of implementation and challenges of PBL in engineering education: a review of literature', *European Journal of Engineering Education*, 46(1), pp. 90–115. Available at: https://doi.org/10.1080/03043797.2020.1718615.

Cinque, M. (2016) '"Lost in translation". Soft skills development in European countries', *Tuning Journal for Higher Education*, 3(2), pp. 389–427.

Dawson, J. and Thomson, R. (2018) 'The future cybersecurity workforce: Going beyond technical skills for successful cyber performance', *Frontiers in psychology*, 9, p. 744.

Finnish Information Security Cluster (2024) *Jäsenet*, *Kyberala*. Available at: https://teknologiateollisuus.fi/fisc/tietoa-meista/jasenet/ (Accessed: 28 November 2024).

Gerring, J. (2006) *Case Study Research: Principles and Practices*. 1 edition. New York: Cambridge University Press.

Hakkala, A., Majanoja, A.-M., Leppänen, V. and Virtanen, S. (2023) 'Framework for the Evaluation of Cybersecurity Curriculum Educational Content', in *Proceedings of the 19th International CDIO Conference, hosted by NTNU, Trondheim, Norway*. Available at: https://www.cdio.org/sites/default/files/documents/CDIO%202023%20Proceedings%20%28138%29.pdf (Accessed: 5 October 2024).

Haney, J. and Lutters, W. (2021) 'Cybersecurity Advocates: Discovering the Characteristics and Skills for an Emergent Role', *NIST*, 29(3). Available at: https://www.nist.gov/publications/cybersecurity-advocates-discovering-characteristics-and-skills-emergent-role (Accessed: 16 October 2024).

Hou, C., Zhu, G., Zheng, J., Zhang, L., Huang, X., Zhong, T., Li, S., Du, H. and Ker, C.L. (2024) 'Prompt-based and Fine-tuned GPT Models for Context-Dependent and -Independent Deductive Coding in Social Annotation', in *Proceedings of the 14th Learning Analytics and Knowledge Conference*. New York, NY, USA: Association for Computing Machinery (LAK '24), pp. 518–528. Available at: https://doi.org/10.1145/3636555.3636910.

ISACA (2023) 'State of Cybersecurity 2023 Global Update on Workforce Efforts, Resources and Cyberoperations'. ISACA. Available at: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023 (Accessed: 20 September 2024).

ISC2 (2023) 'I S C 2 C Y B E R S E C U R I T Y W O R K F O R C E S T U D Y How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023'. ISC2. Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e (Accessed: 19 September 2024).

ISC2 (2024) *Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen*. Available at: https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen (Accessed: 12 September 2024).

Jones, K.S., Namin, A.S. and Armstrong, M.E. (2018) 'The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals', *ACM Transactions on Computing Education*, 18(3), pp. 1–12. Available at: https://doi.org/10.1145/3152893.

Lehto, M., tiedekunta, I., Technology, F. of I., Technology, F. of I., Informaatioteknologia, Technology, I. and Technology, I. (2022) 'Development Needs in Cybersecurity Education : Final report of the project', *Informaatioteknologian tiedekunnan julkaisuja* [Preprint], (96). Available at: https://jyx.jyu.fi/handle/123456789/84719 (Accessed: 13 September 2024).

Marshall, B., Cardon, P., Poddar, A. and Fontenot, R. (2013) 'Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research', *Journal of Computer Information Systems*, 54(1), pp. 11–22. Available at: https://doi.org/10.1080/08874417.2013.11645667.

Mills, J.E. and Treagust, D.F. (2020) 'Engineering education : is problem-based or project-based learning the answer?', *Australasian Journal of Engineering Education* [Preprint], (2003). Available at: https://doi.org/10.3316/aeipt.132462.

Mirzaei, T., Amini, L. and Esmaeilzadeh, P. (2024) 'Clinician voices on ethics of LLM integration in healthcare: a thematic analysis of ethical concerns and implications', *BMC Medical Informatics and Decision Making*, 24(1), p. 250. Available at: https://doi.org/10.1186/s12911-024-02656-3.

Nai, F.I., Hernandez, R.J.L. and Neisse, R. (2022) *JRC Cybersecurity Taxonomy*, *JRC Publications Repository*. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC125533 (Accessed: 20 September 2024).

Nejjar, M., Zacharias, L., Stiehle, F. and Weber, I. (2023) 'LLMs for science: Usage for code generation and data analysis', *Journal of Software: Evolution and Process*, n/a(n/a), p. e2723. Available at: https://doi.org/10.1002/smr.2723.

Niemelä, J. (2019) 'Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastaamaan työvoiman tarvetta Suomessa'. Available at: https://jyx.jyu.fi/handle/123456789/64289 (Accessed: 15 September 2024).

Potter, L.E. and Vickers, G. (2015) 'What Skills do you Need to Work in Cyber Security?: A Look at the Australian Market', in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. *SIGMIS-CPR '15: 2015 Computers and People Research Conference*, Newport Beach California USA: ACM, pp. 67–72. Available at: https://doi.org/10.1145/2751957.2751967.

Saharinen, K. (2023) 'Research into the Aspects of Cybersecurity Education in Higher Education', *JYU dissertations* [Preprint]. Available at: https://jyx.jyu.fi/handle/123456789/86248 (Accessed: 14 September 2024).

Soft Skills Project (2021) 'European Catalogue of Soft Skills References'. Available at: http://www.softskills-project.eu/assets/materials/en/catalogue.pdf (Accessed: 5 October 2024).

Yin, R.K. (2013) *Case Study Research: Design and Methods*. Fifth edition. Los Angeles: SAGE Publications, Inc.