Deliverable D4.4:
Skills Gaps Report - Intermediate version

Deliverable D4.4.

Contractual Date:	**30/04/2026**
Actual Date:	**28/04/2026**
Grant Agreement No.:	**101189986**
Work Package:	**WP4**
Lead Partner:	**Riga Technical University**
Authors:	Arnis Lieknins, Marta Narigina, Andrejs Romanovs, Ruta Pirta, Heinrihs Kristians Skrodelis (RTU)
Contributors:	Luisa Focacci, Asja Kamenica (28Digital), Luis Miguel Campos (ULusofona)

The activities leading to these results has received funding from the European Community's DIGITAL Programme under Grant Agreement No. 101189986 (CYCERONE).

Versioning and contribution history

Version	Date	Author/s	Notes
0.1	28/02/2026	Arnis Lieknins, Marta Narigina, Andrejs Romanovs Ruta Pirta, Heinrihs Kristians Skrodelis (RTU)	First version of D4.4.
0.2	20/04/2026	Arnis Lieknins, Marta Narigina, Andrejs Romanovs Ruta Pirta, Heinrihs Kristians Skrodelis (RTU)	Second version of D4.4, incorporated feedback from partners and peer-reviewers.
0.3	28/04/2026	Arnis Lieknins, Marta Narigina, Andrejs Romanovs Ruta Pirta, Heinrihs Kristians Skrodelis (RTU)	Third version of D4.4, incorporated feedback from peer-reviewer and QM

Partner review table

Version	Reviewer (Partner)	Date	Scope of review	Action taken in document
0.1	28Digital	01.04.2026	Peer-review	Feedback incorporated
0.2	TAU	23.04.2026	QM	Feedback incorporated
0.3	ULusofona	23.04.2026	Peer-review	Feedback incorporated

List of Abbreviations

Abbreviation	Full Term
AI	Artificial Intelligence
APT	Advanced Persistent Threat
API	Application Programming Interface
BCG	Boston Consulting Group
CAN	Controller Area Network
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CISM	Certified Information Security Manager
CPS	Cyber-Physical Systems
DevSecOps	Development, Security, and Operations
DNP3	Distributed Network Protocol 3
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management
IaC	Infrastructure as Code
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
IoMT	Internet of Medical Things
IoT	Internet of Things
ISC2	International Information System Security Certification Consortium
ISACA	Information Systems Audit and Control Association
ML	Machine Learning
LLM	Large Language Model
NFV	Network Function Virtualisation
NICE	National Initiative for Cybersecurity Education
NIS2	Network and Information Security Directive 2

NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OSCP	Offensive Security Certified Professional
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PA	Public Administration
PCI DSS	Payment Card Industry Data Security Standard
PHI	Protected Health Information
PLC	Programmable Logic Controller
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprise
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
SOX	Sarbanes-Oxley Act
V2X	Vehicle-to-Everything
WAF	Web Application Firewall

Executive Summary

This deliverable presents a comprehensive analysis of the cybersecurity skills gap within the European Union, with a particular focus on the CYCERONE project's target groups: professionals working in Small and Medium-sized Enterprises (SMEs) and Public Administration (PA) organisations. The report draws upon a multi-pillar methodological framework comprising a systematic literature review, an analysis of EU policy directives, an assessment of industrial demand, a bibliometric analysis of scholarly output, and the collection of primary survey data from 95 respondents across seven European countries.

The primary survey was designed to measure three core dimensions: technical competencies, soft skills, and governance capabilities. To ensure a holistic view of the ecosystem, data were collected from three key stakeholder groups: industry professionals, public administration officials, and academic professionals. The inclusion of academic professionals is critical to the project's objectives as they provide insight into the current educational pipeline and the structural challenges of aligning curricula with the fast-evolving needs of SMEs and public administrations.

The findings reveal a persistent and multifaceted skills deficit that extends well beyond a simple numerical shortage of personnel. The survey results demonstrate that Network Architecture (mean importance: 4.42/5.00), Incident Response & Management (4.35/5.00), and Data security (4.35/5.00) are the most critically valued technical competencies across all professional roles. Among soft skills, Problem-Solving and Critical Thinking (4.60/5.00) and Teamwork and Collaboration (4.39/5.00) were rated as the most essential. A striking finding is the divergence between stakeholder groups: industry professionals' rate practical, operational skills most highly, whilst academic professionals place significantly greater emphasis on legal, regulatory, and governance competencies.

Respondents identified the lack of practical, hands-on experience (cited by 60% of respondents) and a poor understanding of business context and risk management (49%) as the most significant shortcomings among graduates entering the cybersecurity workforce. The perceived effectiveness of academia–industry collaboration was rated below the midpoint across all stakeholder groups (mean: 2.91-3.00/5.00), indicating a clear need for deeper structural partnerships - defined as formalised, long-term frameworks, such as joint curriculum development, integrated apprenticeship programmes, and shared research labs - to ensure educational outputs align more closely with operational industry needs. On-the-job training and apprenticeships (68% of respondents) and short courses or micro-credentials (59%) were identified as the most effective training modalities for closing the skills gap, with blended learning emerging as the most preferred educational format.

These findings, supported by both quantitative survey data and qualitative interview insights, provide an empirical foundation for the subsequent project activities of the CYCERONE project, informing the design of targeted curricula and training programmes that align with the demonstrable needs of EU SMEs and public administration bodies.

Table of Contents

1. Introduction

The global shortage of skilled cybersecurity professionals represents one of the most pressing challenges confronting modern digital economies. Within the European Union, this shortage is acutely felt by Small and Medium-sized Enterprises (SMEs) and Public Administration (PA) bodies-the two principal target groups of the CYCERONE project. [54, 55] As a recent Eurobarometer survey commissioned by the European Commission reveals, the EU faces a growing cybersecurity skills gap that threatens economic resilience, digital sovereignty, and public trust in governmental digital services [17]. This report, deliverable D4.4 of the CYCERONE project, provides a systematic, empirically grounded analysis of this skills gap, with the explicit objective of informing the design of educational and training interventions tailored to these communities.

The cybersecurity skills gap is a multifaceted phenomenon that extends considerably beyond a simple headcount deficit. At its core lies a **quantitative shortage**: the demand for cybersecurity expertise across EU Member States significantly outstrips the available supply [36], [26]. This numerical deficit is a direct consequence of the rapid pace of digitisation across all sectors of the economy-a pace that cybersecurity training and education pipelines have manifestly failed to match. These pipelines face several key constraints. Building realistic cyber range environments is expensive. At the same time, attracting and retaining qualified instructors within European educational institutions remains challenging. Whilst many experts transition to higher-paying roles in the private sector, a more significant structural issue lies in the outflow of skilled professionals to non-EU markets and the limited inflow of talent from third countries, which constrains the overall capacity of the European cybersecurity workforce and education ecosystem. In addition, curriculum approval processes in higher education institutions are often slow and bureaucratic.

However, the challenge is not merely numerical. A more nuanced **qualitative gap** is equally significant. The competencies now required of cybersecurity professionals are increasingly diverse, encompassing not only deep technical knowledge in areas such as cloud security architecture, threat intelligence analysis, and penetration testing, but also a range of essential non-technical capabilities. These include the ability to communicate complex technical risks in clear business terms to executive leadership, to navigate intricate and frequently conflicting international legal and regulatory landscapes (notably the EU's Network and Information Security Directive 2, or NIS2), and to manage large-scale, cross-functional security projects [36]. As the survey findings presented in Section 7 of this report demonstrate, this blend of technical depth and transversal capability is precisely what EU employers find most difficult to source.

Compounding this issue is a persistent disconnect between formal cybersecurity education and the practical requirements of the profession. Academic curricula frequently provide insufficient coverage of critical operational domains such as Web and Mobile Security, Security Operations Centre (SOC) procedures, and high-pressure Incident Management. This results in graduates who, notwithstanding their theoretical grounding, require extensive on-the-job training to become operationally effective-a finding consistently supported by the literature [12],[11] and confirmed by the primary survey data collected for this report.

1.1 Scope and Objectives

This report focuses specifically on the cybersecurity skills needs of EU-based SMEs and Public Administration bodies, in alignment with the CYCERONE project's mandate. Whilst the analysis draws upon global literature and international best practice, its findings and recommendations are oriented towards the European context. Importantly, the report approaches the cybersecurity skills gap as a mismatch between labour market demand and the available supply of competencies, recognising that both dimensions must be considered to fully understand the gap. The report pursues four principal objectives:

- To identify and rank the cybersecurity skills that are in the highest demand across the EU SME'sand public sector organisations.
- To analyse the specific competencies that are most problematic to source and the systemic reasons underlying these deficiencies.
- To present and analyse primary survey data collected from cybersecurity professionals, academics, and public administration officials across the EU.
- To provide an empirical evidence base that will inform the development of curricula and training programmes within subsequent CYCERONE work packages, with future iterations incorporating a more detailed mapping of the existing training and education supply landscape.

1.2 Structure of the Report

The remainder of this report is organised as follows:

- Section 2 describes the multi-pillar research methodology.
- Section 3 presents an analysis of the cybersecurity skills in highest demand.
- Section 4 examines the most challenging skill areas and the reasons for their scarcity.
- Section 5 analyses sector-specific skill requirements.
- Section 6 reports the findings of the bibliometric analysis.
- Section 7 presents the primary survey findings, including detailed visualisations of the data.
- Section 8 presents the interview's findings.
- Section 9 concludes the report with a synthesis of findings and implications for the CYCERONE project.

2. Methodology

This section details the comprehensive research methodology employed to systematically identify, quantify, and analyse the multifaceted cybersecurity skills gap. For a topic as dynamic and rapidly evolving as the cybersecurity workforce, a multifaceted approach is not merely beneficial but essential. No single research method can adequately capture the complexity of threats, technologies, and labour market dynamics; accordingly, this study employs a five-pillar methodological framework designed to overcome the limitations of any single method through systematic data triangulation.

The methodological framework comprises four primary analytical pillars, together with an assessment of methodological limitations, these are described in detail in Sections 2.1 through 2.5 below. An exploratory fifth pillar - the Analysis of Industrial Demand (Section 2.6) - is introduced separately, as its formal integration into the CYCERONE framework remains under evaluation. The four primary pillars are, first, a Systematic Literature Review (Section 2.1), which establishes the theoretical and empirical knowledge base; second, an Analysis of EU Directives and Policy (Section 2.2), which maps the top-down regulatory drivers of skill demand; third, a Bibliometric Analysis (Section 2.3), which quantitatively traces the intellectual structure and evolution of the cybersecurity academic discourse; and fourth, a Primary Survey (Section 2.4), which collects ground-truth data on the perceptions and experiences of practitioners, academics, and public sector professionals across the EU. By examining the issue from these complementary perspectives - academic research, policy frameworks, bibliometric evidence, and direct practitioner experience - the methodology is designed to overcome the limitations of any single method through systematic data triangulation [41].

By examining the issue from these complementary perspectives-academic research, policy frameworks, real-time market needs, and the direct experiences of practitioners-this methodology enables robust cross-validation of findings. A skill identified as critical in EU policy directives can, for instance, be cross-referenced against its prevalence in real-time job postings and its perceived importance in the practitioner survey. This approach captures both broad statistical trends and the deeper contextual nuances of the skills shortage as it manifests across different industries, organisational types, and EU Member States.

2.1 Pillar 1: Systematic Literature Review

A systematic literature review, modelled on PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. PRISMA was adopted to ensure a rigorous, transparent, and replicable methodology, which is essential for minimising researcher bias and ensuring that the synthesis of findings is based on a representative and objective sample of the current literature. The review involved an exhaustive search of leading academic databases, including IEEE Xplore [44], the ACM Digital Library [45], and Scopus [46], as well as peer-reviewed conference proceedings and publications from authoritative professional bodies such as ISACA [47]and ISC2 [25].

The search strategy employed a carefully selected set of keywords and their variants-including ‘cybersecurity skills gap’, ‘cyber talent shortage’, ‘information security education’, ‘cybersecurity competency models’, and ‘Operational Technology (OT) security training’- to ensure a thorough and

replicable collection of relevant materials published, characterize the historical evolution of the skills gap discourse, and synthesise findings on the causes and consequences of the gap [12],[31], [23].

2.2 Pillar 2: Analysis of EU Directives and Policy

To understand the top-down forces shaping the European cybersecurity landscape, a thorough analysis of directives, policies, and strategic documents from EU institutions and Member State governments was conducted. It included an examination of the EU's General Data Protection Regulation (GDPR), the NIS2 Directive, and the EU Cybersecurity Act, as well as targeted talent development initiatives such as the EU Cybersecurity Skills Academy [36]. At the Member State level, relevant national cybersecurity strategies were reviewed. This analysis is critical because regulatory action is a powerful and often prescriptive driver of demand in the cybersecurity labour market: the implementation of GDPR, for instance, created an immediate demand for Data Protection Officers and professionals skilled in conducting Data Protection Impact Assessments (DPIAs) and implementing privacy-by-design principles.

2.3 Pillar 3: Bibliometric Analysis

A quantitative bibliometric analysis was employed to statistically map the intellectual structure and evolution of the academic research landscape. This analysis was performed using the R programming language, primarily leveraging the bibliometrix package [7]. The methodology involved extracting a corpus of scholarly literature from Scopus, including metadata for authors, keywords, citations, and affiliations. Specific techniques included co-authorship analysis to map collaborative networks, co-citation analysis to identify foundational works, and keyword co-occurrence analysis to map the thematic landscape. The detailed results of this pillar are presented in Section 6.

2.4 Pillar 4: Primary Survey

To gather primary data on the lived experiences and perceptions of those directly affected by the skills gap, targeted online surveys were designed and distributed to three key populations: cybersecurity industry professionals, academic professionals, and public administration professionals. The survey instrument, combining Likert-scale items for quantitative measurement and open-ended questions for qualitative insights, was developed based on themes identified in the literature review. The structure, distribution, and detailed findings of the survey are presented in full in Section 7.

2.5 Exploratory Pillar: Analysis of Industrial Demand (Under Evaluation)

Note: This pillar is currently under evaluation as a potential additional methodological component. The findings presented here are preliminary and subject to further review pending formal inclusion in the CYCERONE framework.

To capture a real-time, bottom-up perspective, a systematic analysis of industrial demand was performed. The primary method involved the automated collection of online job advertisements from major platforms, including LinkedIn (https://www.linkedin.com) and Indeed

(https://www.indeed.com), as well as specialised technology job boards, over a defined period. This dataset was subjected to semantic analysis using Natural Language Processing (NLP) techniques, including topic modelling and n-gram analysis, to identify and quantify the most frequently requested technical skills, soft skills, and professional certifications [20], [30], [38]. The quantitative data was supplemented by a qualitative review of industry reports and white papers from leading cybersecurity organisations, including ISC2, Fortinet, the Boston Consulting Group (BCG), ENISA, and the CyberHubs project.

Note: This pillar is currently under evaluation as a potential additional methodological component. The findings presented here are preliminary and subject to further review pending formal inclusion in the CYCERONE framework.

2.6 Methodological Limitations and Bias Mitigation

Each methodological pillar carries inherent limitations. The literature review and bibliometric analysis are retrospective and subject to publication bias. Job market data can reflect aspirational requirements rather than practical needs [28]. Policy documents may be influenced by political agendas. Survey data is susceptible to self-selection bias and social desirability bias [43],[33]. To address these limitations, the study relies heavily on triangulation: findings from one pillar are systematically cross validated against those from the others. Anonymity was guaranteed to survey participants, and the survey instrument was pilot tested to ensure clarity and reduce leading questions.

3. High-Demand Cybersecurity Skills

The cybersecurity landscape is evolving at an unprecedented pace, driven by a surge in sophisticated threats, increasing regulatory pressure, and the rapid digital transformation of critical infrastructure and services across the EU. As organisations adapt, the demand for cybersecurity professionals has not only intensified but shifted in nature, placing a premium on specific technical competencies and cross-disciplinary capabilities. According to recent workforce studies, over 64% of organisations report difficulty in filling cybersecurity roles owing to a lack of suitably skilled candidates-a trend that directly affects resilience, risk posture, and regulatory compliance [10].

3.1 Technical Skills

Drawing on industry surveys, workforce studies, and the primary data collected for this report, the following technical cybersecurity skills are in consistently high demand across EU organisations:

Cyber Threat Intelligence and Analysis is a critical capability for assessing potential threats, analysing vulnerabilities, and preparing organisations to withstand cyberattacks. Several EU Member States, including Hungary, Spain, and Lithuania, specifically highlight this as a national priority area [24], [13].The CYCERONE survey data confirm its importance, with a mean rating of 4.08/5.00, indicating strong and consistent demand across all professional groups.

Incident Response and Management capabilities are consistently in high demand. This skill is crucial for managing, prioritising, and resolving cybersecurity incidents effectively. The CYCERONE survey data confirm this, with Incident Response receiving a mean importance rating of 4.35/5.00 across all respondent groups.

Cloud Security is consistently identified as one of the most important and in-demand technical competencies. It remains one of the most challenging roles to fill, with 44% of organisations reporting difficulty in sourcing this expertise-a challenge projected to intensify as IT budgets increasingly prioritise cloud solutions [18], [25]. The CYCERONE survey data corroborate this finding, with Cloud Security receiving the mean importance rating (4.14 out of 5) among all technical skills.

Systems, Network and Security Architecture encompasses the design and implementation of secure network infrastructures. Our survey found this to be rated at 4.45/5.00 by industry professionals and 4.58/5.00 by public administration professionals, making it the highest-rated technical skill across all categories.

Data Security, Privacy and Cryptography is an area where demand is expected to increase further owing to expanding EU data privacy regulations, notably the GDPR and the forthcoming ePrivacy Regulation. Cryptographic expertise is essential for ensuring secure communications and data storage [13], [10]. The CYCERONE survey results reinforce this trend, with this skill area receiving a mean importance rating of 4.31/5.00, placing it among the top three most critical technical competencies identified. This highlights the growing importance of regulatory-driven security requirements and the need for organisations - particularly SMEs and public administration bodies - to ensure robust data protection capabilities in order to maintain compliance and trust.

3.2 Non-Technical (Soft) Skills

The demand for transversal skills is growing across EU Member States and is considered critical in the cybersecurity field, complementing technical expertise and increasingly emphasised by employers. The role of soft skills, including communication, teamwork, and knowledge management, has emerged as critical for professional success, reflecting a theoretical shift towards a more holistic understanding of cybersecurity expertise beyond technical proficiency [20], [8], [22].

Problem-Solving and Critical Thinking is consistently identified as the single most valued soft skill. The CYCERONE survey data confirm this emphatically, with a mean importance rating of 4.60/5.00 -the highest of any skill, technical or non-technical, assessed in the survey. This skill is expected to become even more vital with the advancement of AI-assisted tools, as non-technical competencies are considered more transferable [25].

Communication is the most in-demand transversal skill cited in industry reports, crucial for conveying technical information effectively, particularly when explaining risks to non-technical stakeholders. Clear communication and information sharing are paramount for developing situational awareness during cyber crises [13], [16].

Teamwork and Collaboration is essential in environments where cybersecurity professionals work alongside cross-functional teams encompassing IT, legal, and management functions. The CYCERONE survey rated this at 4.39/5.00, with public administration professionals valuing it particularly highly (4.58/5.00).

Leadership and Strategic Thinking is crucial for senior cybersecurity roles such as the Chief Information Security Officer (CISO) position. Cybersecurity leadership is considered the most pressing concern by 50% of organisations surveyed by [10].

3.3 The Role of Certifications

Industry reports strongly emphasise the value of cybersecurity certifications in the hiring process. Fortinet reports globally that 91% of hiring managers prefer candidates who hold certifications, viewing them as validation of cybersecurity awareness and knowledge. [14] The CYCERONE survey data, however, present a more nuanced picture: professional certifications received a mean valuation of only 3.15 out of 5, whilst academic certifications were valued slightly more highly at 3.44/5.00. This may reflect the cost barrier of professional certifications such as the Certified Information Systems Security Professional (CISSP) or the Offensive Security Certified Professional (OSCP), which are typically employer-funded and therefore less accessible to graduates and professionals in SMEs with limited training budgets.

4. Challenging Skills and Reasons for Deficiency

Whilst the demand for cybersecurity professionals is universally high, certain skills are not only in high demand but are also the most challenging for organisations to source. This section examines these problematic skill sets and the underlying reasons for their scarcity, which is driven by a combination of educational shortcomings, the rapid evolution of technology, and systemic challenges in workforce development.

4.1 Analysis of Problematic Skill Areas

Cloud Security represents the most acute technical skills gap. As organisations migrate workloads to cloud environments (Amazon Web Services, Microsoft Azure, Google Cloud Platform), the demand for professionals who can securely configure and manage these complex ecosystems has risen dramatically. This is not a single skill but a cluster of competencies, including Identity and Access Management (IAM), container security (Docker, Kubernetes), and Infrastructure as Code (IaC) security. Misconfigurations remain a leading cause of major data breaches [42]. The shortage is particularly severe because cloud technologies evolve faster than traditional training programmes can adapt.

Web and Application Security remain a critical deficiency area. With the proliferation of web applications and mobile-first strategies, securing these platforms is paramount; yet many academic programmes lack deep, practical coursework in secure coding practices, Application Programming Interface (API) security, and mobile platform vulnerabilities. Graduates may understand the theory of the OWASP Top 10 but lack the hands-on ability to perform a security code review or configure a Web Application Firewall (WAF) effectively [12].

Operational Technology (OT) and Industrial Control Systems (ICS) Security represents an area of extreme scarcity. The convergence of Information Technology (IT) and OT through the integration of Internet of Things (IoT) devices into critical infrastructure has created complex challenges. Securing these systems requires a rare, interdisciplinary knowledge of both IT security principles and industrial engineering processes, including understanding protocols such as Modbus, DNP3, and PROFINET [32]. It should be noted that many legacy OT systems were originally designed for isolated, internal networks without internet connectivity; their subsequent connection to wider enterprise networks was frequently undertaken without a thorough revision of their architecture, access controls, and security posture. This historical oversight is a significant contributing factor to the current vulnerability landscape [9].

Soft Skills Deficits are equally problematic. The CYCERONE survey results demonstrate that the lack of practical, hands-on experience (cited by 60% of respondents) and poor understanding of business context and risk management (49%) are the most frequently observed shortcomings in graduates. Employers are increasingly seeking professionals who can articulate risk to the board in financial terms, collaborate under pressure during incidents, and embed security into development workflows through DevSecOps practices [20], [21].

4.2 Underlying Reasons for Skill Scarcity

Educational Gaps: A persistent disconnect exists between the skills taught in many educational institutions and those required by industry. Curricula are frequently years behind current practice, a failure attributed to lengthy curriculum approval processes, the prohibitive cost of modern laboratory equipment, a lack of access to real-world threat intelligence, and a critical shortage of faculty with recent industry experience [12], [15], [27].

Chronic Underinvestment: This educational gap is exacerbated by insufficient investment in cybersecurity education infrastructure, manifesting as fewer scholarships, outdated laboratory equipment, and an inability for public institutions to offer competitive salaries to attract expert instructors-creating a 'brain drain' from academia to industry [27].

Evolving Threat Landscape: The velocity of change in the cybersecurity threat landscape-encompassing AI-generated malware, sophisticated social engineering, and software supply chain attacks-requires continuous learning and adaptation. The 'half-life' of technical skills in cybersecurity is notoriously short, necessitating a shift from front-loaded education to lifelong learning [9], [5], [4].

Coordination and Synergy Failures: Across the EU, existing initiatives to address the skills gap frequently lack coordination. Different Member States develop separate, incompatible certification standards and training programmes, leading to a fragmented talent market. The EU Cybersecurity Skills Academy aims to address this through a centralised platform for training and collaboration [36].

5. Sector-Specific Skill Requirements

The most critical cybersecurity skill requirements vary significantly across key sectors, each with its unique threat landscape, regulatory environment, and operational needs. This section examines the skill requirements most relevant to CYCERONE's target groups and related sectors.

5.1 Finance

Protecting financial data, meeting stringent compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act (SOX), and combating sophisticated financial fraud require a unique blend of cybersecurity skills. Key competencies include deep expertise in data encryption and multi-factor authentication, advanced intrusion detection and continuous monitoring, AI and machine learning for real-time anomaly detection in transactions, and thorough understanding of complex, overlapping regulatory frameworks [34], [39], [35].

5.2 Healthcare

In the healthcare sector, cybersecurity skills are crucial for protecting patient health information (PHI), securing a vast ecosystem of medical devices, and ensuring compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU's GDPR. A breach in this sector can have life-threatening consequences. Vital skills include comprehensive risk assessment, data encryption and access control, incident response planning that ensures continuity of patient care, and the specialised skill of securing the Internet of Medical Things (IoMT), which combines device security knowledge with an understanding of clinical workflows [1], [6], [3], [19].

5.3 Critical Infrastructure and Operational Technology

Defending Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems demands a highly specialised set of skills owing to the unique vulnerabilities of these systems and the potentially catastrophic physical consequences of a breach. Professionals must possess thorough understanding of ICS/SCADA architectures and their specific communication protocols, true expertise in cyber-physical systems, and deep knowledge of standards such as those from the National Institute of Standards and Technology (NIST) and ISA/IEC 62443 [32], [2] [29].

5.4 Telecommunications

The telecommunications sector, encompassing 3G, 4G, 5G LTE, and emerging 6G mobile network infrastructures, presents a distinct set of cybersecurity challenges [51]. Professionals in this domain require knowledge of radio access network security, signalling protocol vulnerabilities (such as those in SS7 and Diameter), core network security for virtualised and cloud-native architectures (Network Function Virtualisation, or NFV, and Software-Defined Networking, or SDN), and the security implications of network slicing in 5G environments [50]. This sector's properties and employee skill profiles differ meaningfully from those of other critical infrastructure domains such as energy or transportation.

5.5 Automotive and Transportation

The automotive sector and the broader transportation industry (including rail and aviation) face rapidly growing cybersecurity requirements driven by the increasing connectivity and autonomy of vehicles and transport systems. Key skill areas include in-vehicle network security (Controller Area Network, or CAN, bus protocols), Vehicle-to-Everything (V2X) communication security, compliance with emerging standards such as UNECE WP.29 and ISO/SAE 21434 [53,54], and the security of autonomous driving systems and their associated AI components.

5.6 Government and Public Administration

The cybersecurity skill needs of the public sector differ from those of the private sector owing to the unique focus on national security, public safety, and the immense scale of critical infrastructure. It should be noted that the boundaries between this sector and critical infrastructure are not discrete but overlapping public administration bodies are frequently responsible for overseeing and regulating critical infrastructure sectors, whilst themselves operating digital services that constitute critical societal functions. Key skills include critical infrastructure protection at a national level, specialised capabilities in countering state-sponsored cyber threats including Advanced Persistent Threats (APTs), and skills in developing and implementing national regulatory and policy frameworks [14], [40], [37].

6. Bibliometric Analysis

This section presents the findings of the quantitative bibliometric analysis, which complements the qualitative synthesis of the literature review by statistically mapping the intellectual structure and evolution of cybersecurity skills gap research within Europe. The analysis was performed using a dataset collected from Scopus, processed using the R programming language with the bibliometrix package. The package provides a comprehensive set of tools for quantitative scientometrics, facilitating a complete science mapping workflow. By integrating data extraction, pre-processing, and advanced network visualization, it ensures methodological rigor and statistical objectivity in identifying key thematic clusters and research trends.

6.1 Dataset Construction

The dataset was constructed through keyword-based retrieval using predefined seed terms directly connected to the cybersecurity workforce and skills gap (see Table 1). Geographical filtering was applied to limit the dataset to publications originating in Europe, and a controlled thesaurus was applied to harmonise synonyms and ensure consistency across keywords.

Seed Search Term	Scopus Results
Information security education	3,398
NICE framework	994
Cybersecurity skills gap	520
Cybersecurity professional development	271
Cybersecurity skills shortage	56
Cybersecurity workforce gap	49
Cyber talent shortage	9
Healthcare cybersecurity skills gap	4
EU cybersecurity workforce gap	2
Financial sector cybersecurity skills gap	2

Table 1: Predefined seed search terms and corresponding Scopus results (Europe).

6.2 Key Findings

The analysis of annual scientific production reveals clear growth in the field. Between 2010 and 2016, fewer than 200 documents per year were published. After 2017, output accelerated sharply, peaking above 600 documents in 2023. Most works were published in conference proceedings, with the most frequent outlets being Lecture Notes in Computer Science, CEUR Workshop Proceedings, and Lecture Notes in Networks and Systems. Among journals, Computers and Security and IEEE Access appear prominently. This distribution indicates that the field remains practice-driven and still consolidating, with rapid outputs disseminated at conferences rather than in journal articles.

The keyword co-occurrence network reveals three primary thematic clusters: (i) an Education and Training cluster, comprising terms such as education, curriculum, students, and e-learning; (ii) a

Technology and Security cluster, including cybersecurity, network security, artificial intelligence, and machine learning; and (iii) a Healthcare and Social Sciences cluster, with keywords such as health care, patient safety, and public health. Whilst education and technology are closely linked, healthcare-related research remains more isolated, suggesting sectoral fragmentation in the academic discourse.

Temporal analysis indicates that cybersecurity and education have been consistent research themes throughout the last decade, whilst artificial intelligence and machine learning rose sharply after 2018. Sector-specific terms relating to finance and critical infrastructure are largely absent from the academic literature, representing a significant research gap given the acute skills needs in these domains.

7. Survey Analysis

This section presents the findings of the primary survey conducted as part of the CYCERONE project to capture ground-truth data on the cybersecurity skills gap as perceived by professionals working in industry, academia, and public administration across the European Union. The survey was designed to validate and contextualise the findings derived from the literature review, policy analysis, and industrial demand assessment presented in the preceding sections.

7.1 Survey Design and Distribution

The survey instrument was developed based on themes identified in the systematic literature review and was structured around six thematic blocks:

- professional profile and demographics.
- perceived importance of technical cybersecurity skills.
- perceived importance of non-technical and governance skills.
- assessment of graduate shortcomings.
- valuation of credentials and collaboration effectiveness.
- preferences for training modalities and educational formats.

The majority of items employed a 5-point Likert scale (1 = Not at all important/effective; 5 = Extremely important/effective), supplemented by multiple-choice and open-ended items. The questionnaire was distributed through professional networks, CYCERONE project partners, and relevant industry associations during October-December 2025. Anonymity was guaranteed to all participants to encourage honest responses.

7.2 Respondent Demographics

A total of 95 valid responses were collected from professionals across seven European countries. The respondent population comprised 75 Industry Professionals (79%), 12 Public Administration Professionals (13%), and 8 Academic Professionals (8%). The geographical distribution was led by Italy (45.3%), Sweden (24.2%), and Hungary (13.7%), with additional responses from Finland, Romania, Switzerland, and Belgium. In terms of organisational size, most respondents (65.5%) were employed by Small or Medium-sized Enterprises (SMEs), with 19.5% working in Large Enterprises and the remainder not specifying. This demographic composition is well aligned with the CYCERONE project's focus on EU-based SMEs and Public Administration bodies. In Figure 1,2,3 distribution of survey respondents by professional role, country, and organisation size is shown.

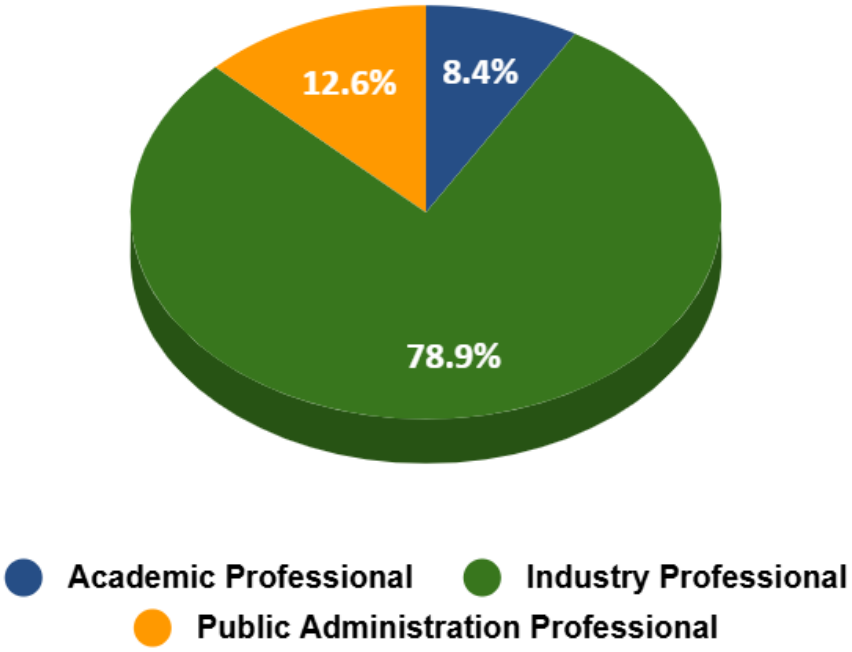

Figure 1: Distribution of survey respondents by professional role (n = 95).

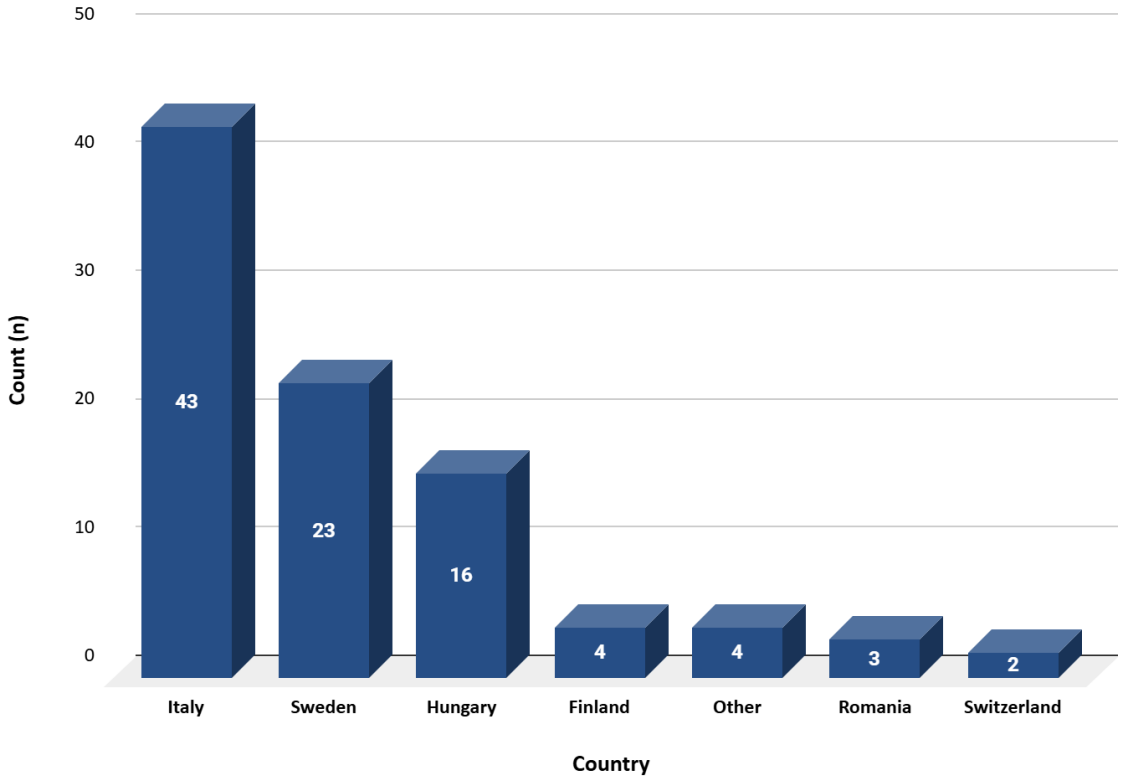

Figure 2: Distribution of survey respondents by country (n = 95).

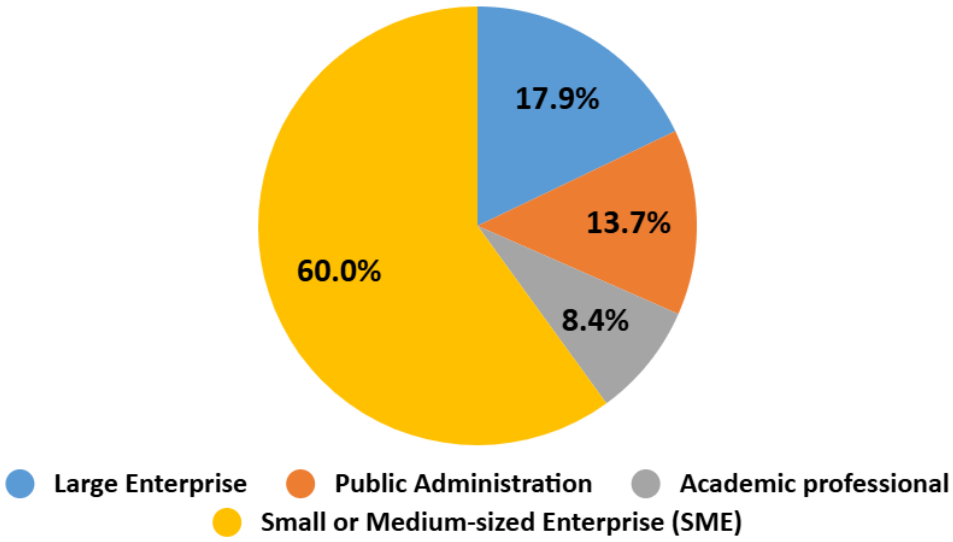

Figure 3: Distribution of survey respondents by organisation size (n = 95).

7.3 Perceived Importance of Technical Skills

Respondents were asked to rate the importance of eleven technical cybersecurity skill areas on a 5-point Likert scale. The results, presented in Figure 4, reveal a clear hierarchy of valued competencies with notable divergences across professional roles.

Across the full sample, the five highest-rated technical skills were Architecture/Design (Overall mean: 4.42/5.00), Incident Response and Management (4.35/5.00), Data Security/Privacy (4.31/5.00), Cloud Security (4.14/5.00) , and Cyber Threat Intelligence and Analysis (4.08/5.00). These findings strongly corroborate the demand patterns identified in the industrial analysis (Section 8) and align with the priorities articulated in EU policy documents.

A striking finding is the divergence between professional roles. Industry professionals consistently assigned higher importance ratings to operational, hands-on skills such as Architecture/Design (4.45/5.00), Incident Response (4.41/5.00), and OT/ICS Security (3.91/5.00) compared to their academic counterparts (3.88, 3.88, and 2.88, out of 5.00). Conversely, academic professionals tended to rate foundational and governance-adjacent skills more comparably (e.g., Data Security/Privacy at 4.00/5.00, Threat Intelligence at 4.00/5.00) but assigned markedly lower ratings to specialised domains such as Digital Forensics (2.38 vs. 3.24 out of 5.00for industry) and Penetration Testing (2.88 vs. 3.66 out of 5.00). Public Administration professionals rated Architecture/Design highest of all groups (4.58/5.00) and also valued OT/ICS Security highly (3.91/5.00), reflecting the sector's responsibility for overseeing critical national infrastructure.

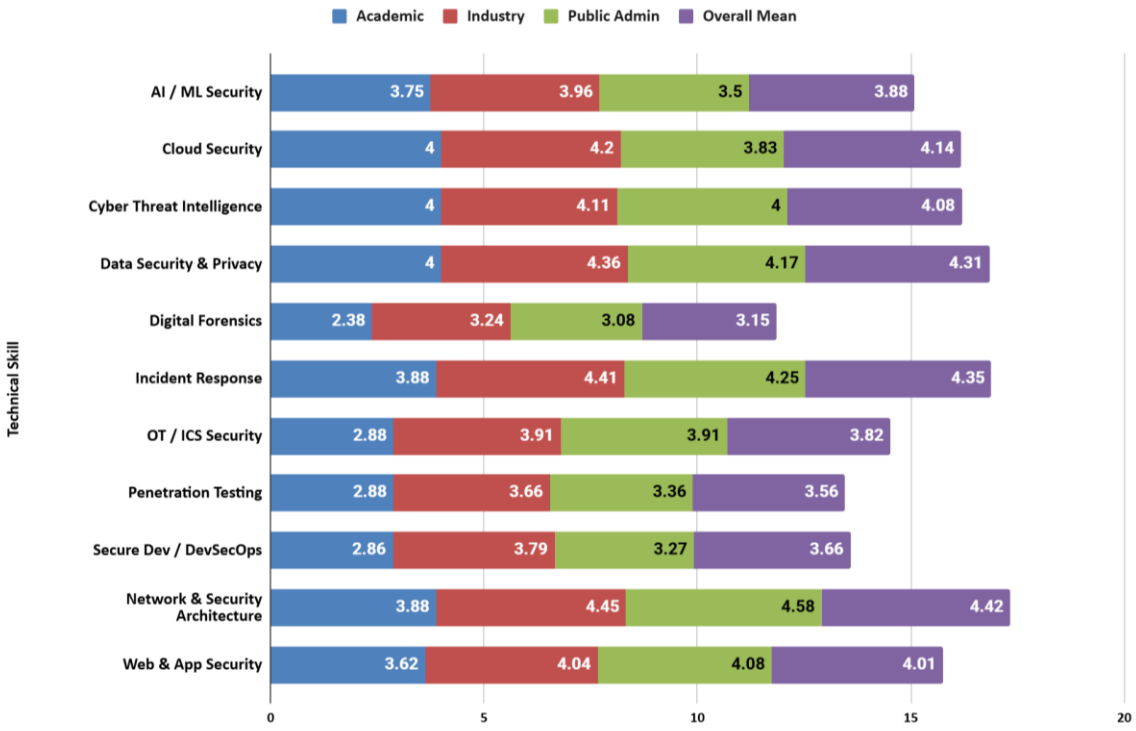

Figure 4: Mean importance of technical cybersecurity skills by professional role (5-point Likert scale).

7.4 Perceived Importance of Non-Technical and Governance Skills

The results, depicted in Figure 5, reveal that Problem-Solving and Critical Thinking (mean: 4.60/5.00) was rated as the single most important non-technical competency across all categories assessed in the survey. Teamwork and Collaboration (4.39/5.00), Leadership and Strategic Thinking (4.33/5.00), and Communication to Non-Technical Audiences (4.22/5.00) followed closely.

A particularly noteworthy divergence was observed in the valuation of governance-oriented skills between professional roles. Academic professionals rated Legal, Regulatory and Policy Compliance significantly higher (4.63/5.00) than industry professionals (3.08/5.00), representing the largest single discrepancy observed in the entire survey. A similar pattern was observed for Risk Management and Governance (academic: 4.50 vs. industry: 3.21 out of 5.00) and for Training, Awareness and Education (academic: 4.13 vs. industry: 2.95 out of 5.00). This divergence may reflect differences in professional priorities: industry practitioners are focused on immediate operational effectiveness, whilst academics take a broader, longer-term view of the competencies required for a mature cybersecurity practice.

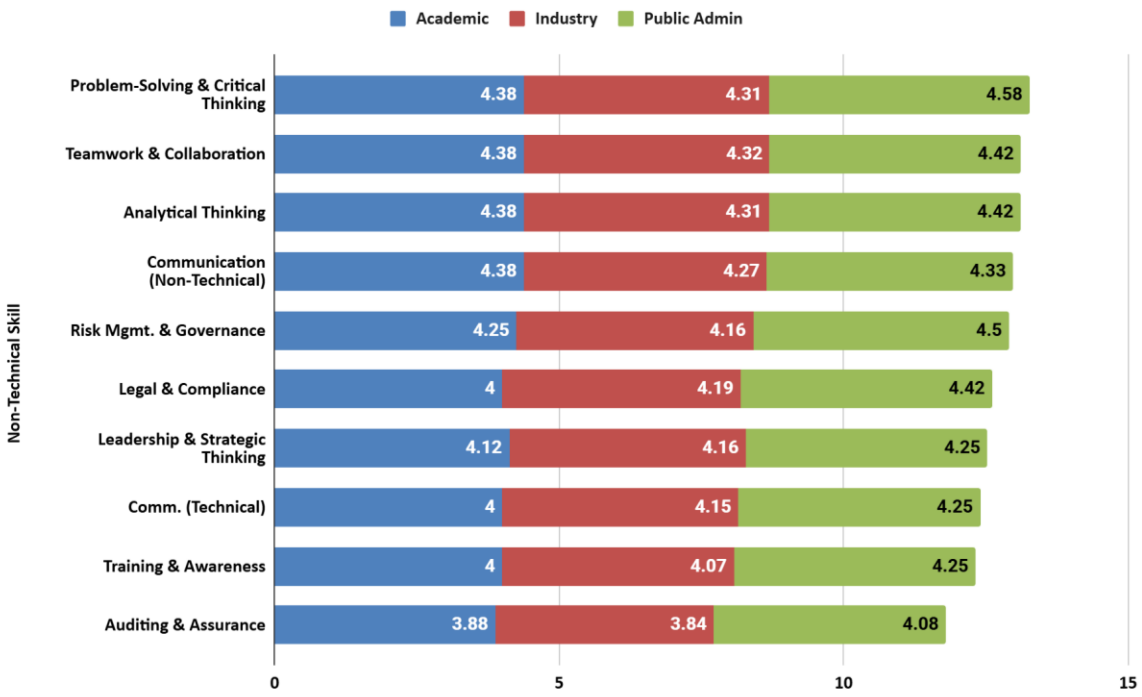

Figure 5: Mean importance of non-technical and governance skills by professional role (5-point Likert scale).

7.5 Observed Shortcomings in Graduates

Respondents were asked to identify the most significant shortcomings they observe in graduates entering the cybersecurity workforce. This item permitted multiple selections, and the results (Figure 6) provide compelling evidence of the theory-practice divide.

The Practical Experience Gap:

- **Lack of practical, hands-on experience (75.0%):** Cited by 57 respondents, this remains the most critical barrier to entry, confirming that theoretical knowledge is not translating into operational readiness.
- **Unfamiliarity with modern tools and technologies (19.7%):** While less prevalent, a subset of graduates struggles with the specific technical stacks used in e.g. contemporary SOC and network environments.

The Contextual and Regulatory Gap:

- **Poor understanding of business context and risk management (61.8%):** 47 respondents highlighted that graduates often fail to align security measures with organizational objectives.
- **Insufficient knowledge of EU regulations (51.3%):** Over half of the respondents noted a lack of readiness for compliance frameworks such as **NIS2 and GDPR**, which are vital for SMEs and Public Administrations.

The Cognitive and Soft Skills Gap:

- **Deficiencies in problem-solving and investigation (44.7%):** Highlighting a need for improved analytical and self-led learning capabilities.
- **Underdeveloped communication and teamwork skills (38.2%):** Underscoring the importance of transversal skills in cross-departmental security roles.

These findings directly corroborate the persistent educational gaps identified in the literature review (Section 2.1) and provide quantitative validation of the widely discussed academia–industry disconnect. The fact that hands-on experience and business context comprehension together account for the two most cited shortcomings underscores the need for curricula that integrate practical, scenario-based learning with real-world business and regulatory contexts-precisely the type of training that the CYCERONE project is designed to develop.

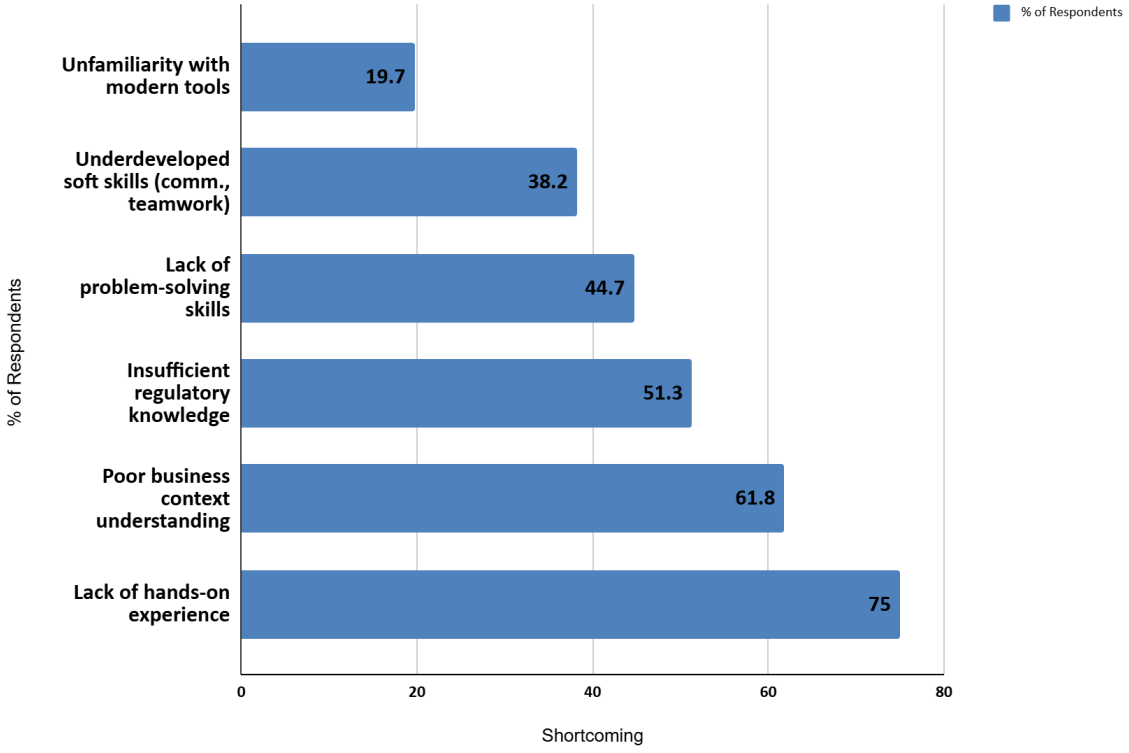

Figure 6: Most significant shortcomings observed in graduates entering the cybersecurity workforce (multiple selections permitted; n = 87).

7.6 Valuation of Credentials and Collaboration Effectiveness

Respondents were asked to rate the value they place on different types of credentials when evaluating cybersecurity candidates, and to assess the effectiveness of current academia–industry collaboration. The results are presented in Figure 7 and 8.

The mean valuations across credential types were remarkably similar: academic certifications were rated at 3.44/5.00, formal credentials at 3.42/5.00, and professional certifications at 3.15/5.00 . The finding that professional certifications (e.g., CISSP, OSCP) were valued marginally lower than academic qualifications may reflect the cost barrier associated with these certifications, particularly for professionals in SMEs where employer-funded certification programmes are less common.

The perceived effectiveness of academia–industry collaboration was rated below or at the midpoint across all stakeholder groups: industry professionals rated it at 2.91/5.00, academic professionals at 3.00/5.00, and public administration professionals at 3.00/5.00. These figures indicate a shared perception that current collaborative mechanisms are, at best, moderately effective - a finding that has direct implications for the CYCERONE project's approach to building operational public–private partnerships for cybersecurity education.

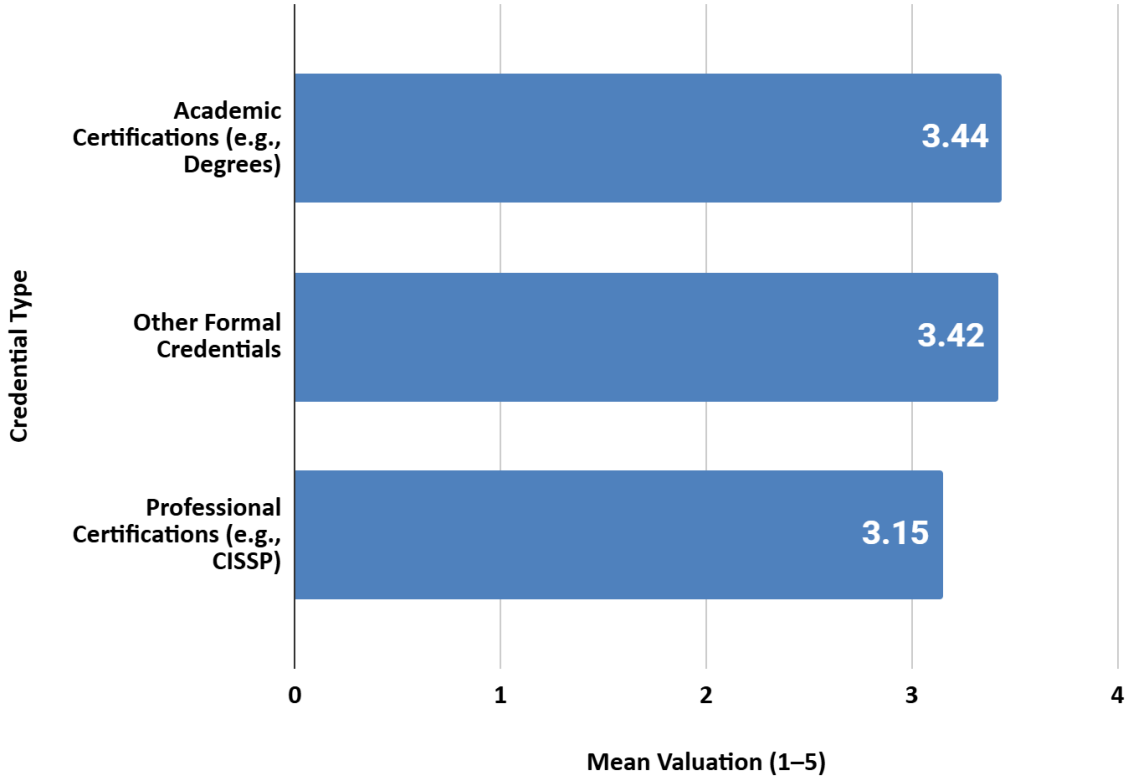

Figure 7: Mean Valuation of credential by Types.

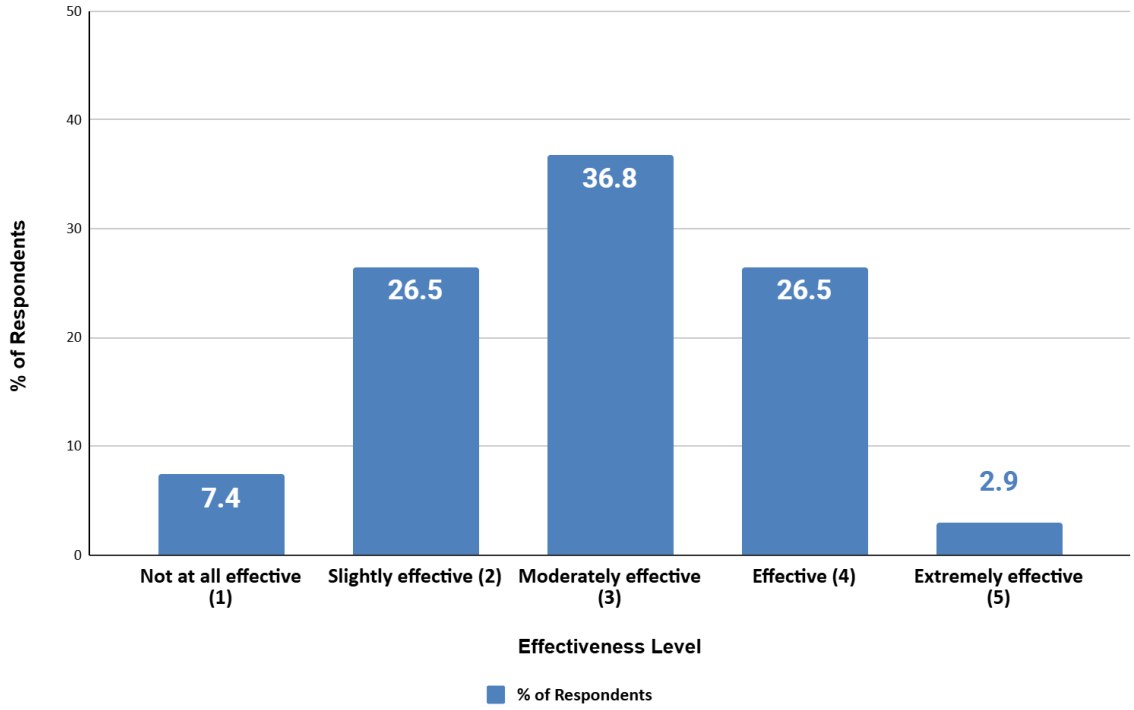

Figure 8: Valuation of perceived effectiveness of academia–industry collaboration.

7.7 Organisational Investment in Upskilling

Respondents were asked whether their organisation invests in upskilling or reskilling for employees in cybersecurity. The survey results indicate a significant level of active investment in employee development, with over three-quarters of surveyed organisations (76.8%) reporting that they are actively investing in upskilling or reskilling their workforce. This investment is split between formal programs (36.8%) and occasional or informal methods (40.0%). The most prevalent form of investment is "Yes, occasionally or informally" (40.0%), suggesting that while training is widespread, it often lacks the structured planning or consistent funding associated with formal programs. Only a small minority of organisations (16.8%) reported no investment in this area. Organisational Investment in Cybersecurity Upskilling and Reskilling is visible on Figure 8.

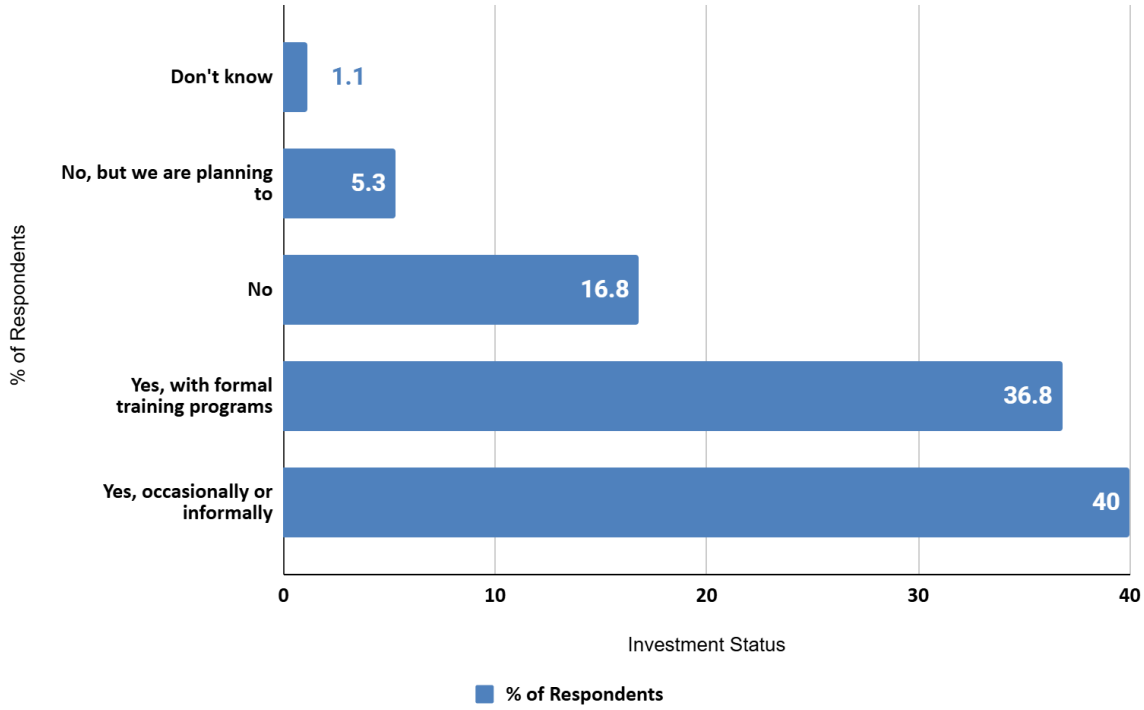

Figure 8: Organisational Investment in Cybersecurity Upskilling and Reskilling

7.8 Preferred Training Modalities and Educational Formats

Respondents were asked to identify the types of education or training they consider most effective for closing the cybersecurity skills gap, and their preferred formats for cybersecurity education. These items permitted multiple selections, and the results are presented in Figures 9 and 10. On-the-job training and apprenticeships were identified as the most effective modality by 65 respondents (68.4%), followed by short courses and micro-credentials (56 respondents, 58.9%), professional certifications (47 respondents, 49.5%), and university degree programmes and bootcamps (each at 37 respondents, 38.9%). These findings indicate a strong preference for practice-oriented, work-integrated learning over purely academic approaches. In terms of delivery format, blended learning combining online and in-person elements was the most preferred option (34 respondents, 35.8%), followed by hands-on laboratories and simulations (18 respondents, 18.9%) and in-person classroom learning (14 respondents, 14.7%). The strong preference for blended learning is particularly relevant for the CYCERONE project's design of distance-accessible training programmes that can serve professionals across multiple EU Member States.

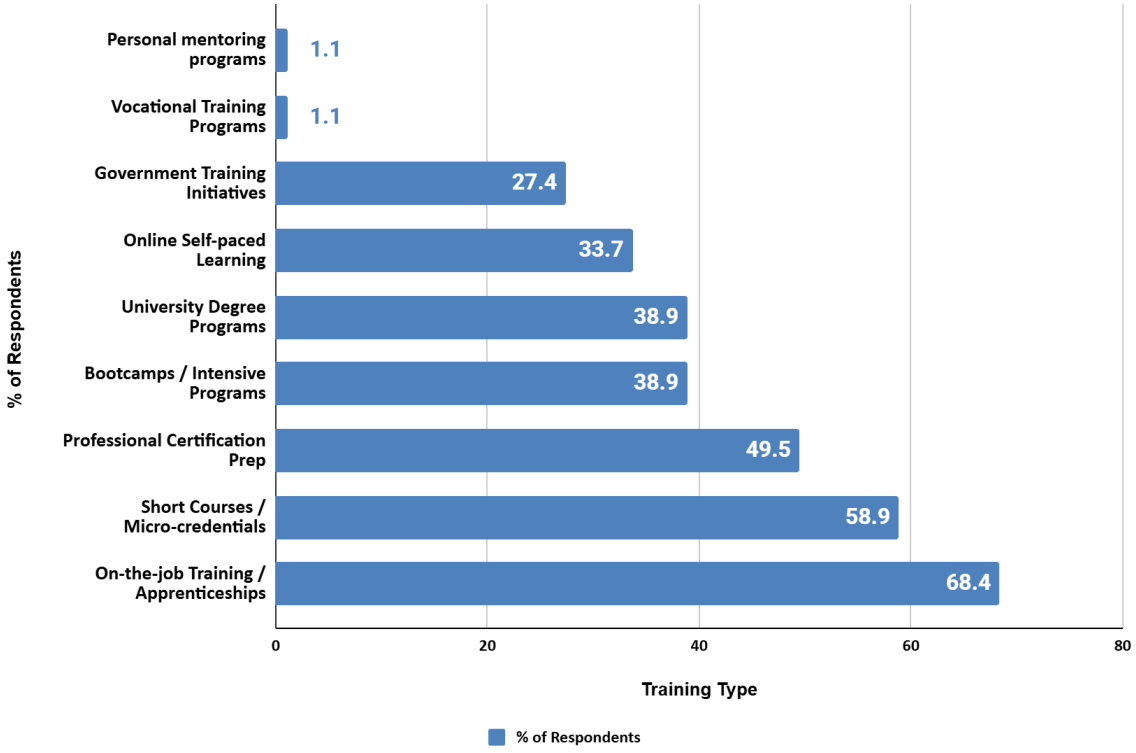

Figure 9: Preferred training types for closing the cybersecurity skills gap.

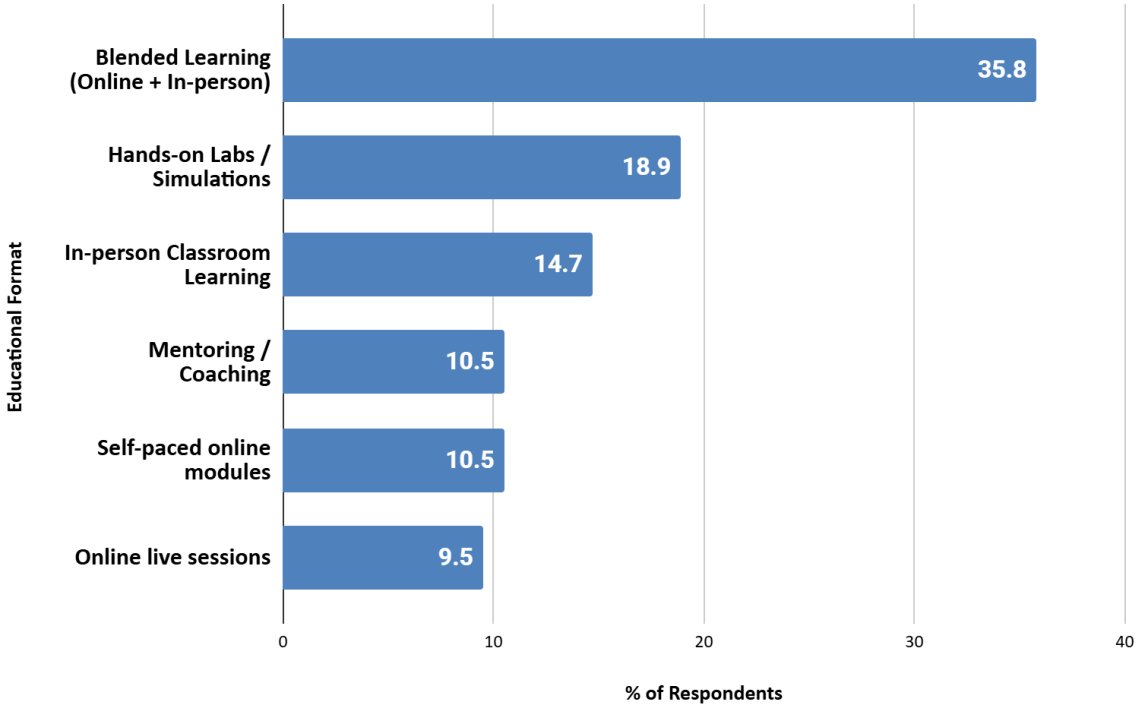

Figure 10: Preferred educational formats for closing the cybersecurity skills gap.

7.9 Summary of Survey Findings

The qualitative interviews conducted across Finland and Romania in early 2026 successfully corroborated the primary survey data, providing deeper insights into the persistent cybersecurity skills gap within the European labour market. The findings reveal that while technical proficiencies in systems architecture, incident response, and data security are highly prioritized across all professional roles, cognitive abilities such as problem-solving and critical thinking remain the single most valued competencies overall. Despite this clear industrial demand, a significant perception gap exists between academic institutions and the private sector regarding the importance of governance, risk, and compliance (GRC) skills, which often results in their under-representation within higher education curricula. This misalignment is further evidenced by the primary shortcomings identified in recent graduates, who frequently lack both practical experience and a fundamental understanding of broader business contexts. Furthermore, current collaboration between academia and industry is perceived as only moderately effective, indicating a critical need for more strategic partnerships. To bridge these divides, stakeholders consistently identify on-the-job training and blended learning models as the most effective and preferred modalities for future professional skills development.

8.Interview-Based Qualitative Analysis

This chapter outlines the in-depth qualitative findings of the CYCERONE project's Skills Gap Analysis (Deliverable D4.4). While the preceding quantitative survey provided a macro-level statistical overview of the European cybersecurity landscape, the qualitative data gathered through semi-structured interviews offers critical explanatory depth, illuminating the causal mechanisms driving the identified workforce deficits. To systematically capture and categorize this complex qualitative data, the research utilized the TBCR (Trunk-Branches-Canopy-Roots) theoretical framework. This methodology structures the phenomenological inquiry across four distinct, yet interdependent, thematic dimensions. These dimensions encompass core competency demands that are universally required across the profession (Trunk), role-specific and sector-specific skill differentiation (Branches), emerging, aspirational, and advanced technical capabilities driven by technological innovation (Canopy), and the foundational educational, pedagogical, and cognitive requirements necessary to support advanced learning (Roots).

8.1 Methodology, Sample Characteristics, and Analytical Approach

The study employed a rigorous purposive sampling strategy designed to capture multidimensional, cross-sectoral perspectives from key stakeholder groups, including academic educators, industry practitioners, and public sector officials. Data collection occurred intensively between January and February 2026, comprising ten highly specialized participants across three strategic European partner institutions [41]. The interview protocol involved extended, audio-recorded sessions lasting between sixty and ninety minutes, which were subsequently subjected to verbatim transcription and rigorous anonymization in strict compliance with the respective institutional ethics and data governance guidelines.

To ensure analytical rigor, the transcribed data underwent a multi-stage thematic analysis. This involved an initial phase of open coding to identify emergent concepts, followed by axial coding to map relationships between the TBCR dimensions, and concluding with selective coding to distil the core cross-site themes. Inter-coder reliability was established through cross-validation of the coding matrix by two independent researchers. The participant cohort included five individuals from Aalto University Executive Education (Aalto EE) in Finland, interviewed between January 19 and 21, 2026.

An additional three participants representing Tampere University and the Finnish Government were interviewed across January and February 2026. Finally, two participants from Babeș-Bolyai University (UBB) in Romania were interviewed in February 2026. The sample purposefully comprises cybersecurity programme directors, corporate training managers, government digital transformation officers, and senior security architects. All participants and their specific organizational affiliations are referenced pseudonymously to protect confidentiality and encourage candid discourse regarding institutional vulnerabilities.

8.2 Partner Specific Findings

8.2.1 Aalto University Executive Education, Finland

Participants representing the Aalto EE ecosystem highlighted a critical and widening misalignment between current academic curricula and the rapidly evolving, applied competencies required by the Finnish technology and manufacturing industries. Within the core Trunk dimension, severe, chronic shortages were identified in cloud security architecture, dynamic incident response, and advanced network security. Furthermore, respondents stressed a paradigm shift in how technical roles are perceived: technical acumen must now be inextricably paired with advanced business communication skills. Specifically, participants noted a profound inability among recent graduates to articulate cyber risk in terms of financial impact and business continuity to non-technical executive boards, treating security purely as an engineering problem rather than a dimension of enterprise risk management.
Sectoral divergence emerged with striking clarity within the Branches dimension. Participants noted that the financial sector heavily prioritizes regulatory compliance, data governance, and adherence to frameworks such as the Digital Operational Resilience Act (DORA). Conversely, critical infrastructure operators and the manufacturing sector demand deep expertise in Operational Technology (OT) security, Supervisory Control and Data Acquisition (SCADA) system protection, and physical resilience engineering. Analysis of the Canopy dimension revealed significant, aggressive investment shifts towards AI-augmented threat detection mechanisms and the implementation of Zero-Trust Architectures (ZTA). Despite this industry momentum, interviewees lamented a systemic lack of formal, academic training pathways for these paradigms, forcing companies to rely on proprietary vendor training. Finally, the Roots dimension highlighted persistent, concerning pedagogical gaps in applied cryptography and the integration of secure software development lifecycle (SDLC) principles. Interviewees emphasized that the continued prevalence of supply-chain vulnerabilities stems directly from engineering programs failing to teach secure-by-design principles from the first year of study.

8.2.2 Tampere University and Government Representatives, Finland

Interviews associated with Tampere University and government representatives focused heavily on public sector workforce constraints, specifically highlighting the structural, macroeconomic difficulty of competing with aggressive private sector compensation models.
The Branches dimension demonstrated that public administration faces unique operational and bureaucratic hurdles. Notably, the secure procurement of IT services, vendor risk management, and the auditing of third-party digital supply chains were identified as critical competencies that are entirely absent from standard academic degree programs. Regarding emerging capabilities within the Canopy dimension, public sector upskilling is heavily influenced by the contemporary geopolitical climate. Initiatives are strongly driven by digital sovereignty mandates and complex EU regulatory compliance, with the NIS2 Directive and the Cyber Resilience Act cited as primary catalysts forcing government agencies to modernize their security postures. Discussions on the Roots dimension indicated a growing institutional consensus demanding a radical pedagogical shift. Participants argued for the mandatory integration of scenario-based, hands-on security training, such as immersive cyber

range exercises and interactive tabletop simulations, directly into core computer engineering and information systems degrees, rather than treating cybersecurity as an optional elective.

8.2.3 Babeș-Bolyai University, Romania

The qualitative data from the Romanian ecosystem exposed distinct macroeconomic and regional challenges, primarily the accelerated "brain drain" of highly specialized cybersecurity talent to Western European and North American employers, juxtaposed against a maturing, yet still nascent, localized education infrastructure. In terms of core Trunk competencies, the local market exhibits an overwhelmingly high industry demand for foundational operational skills, specifically applied network security, ethical hacking, and advanced penetration testing. Participants noted that the rapid digitalization of local industries currently outpaces the academic supply of practitioners capable of executing these hands-on defensive and offensive operations.

The Branches dimension highlighted the precarious situation of Romanian Small and Medium-sized Enterprises (SMEs). Operating under severe financial and resource constraints, these organizations cannot afford dedicated security teams. Consequently, they require highly versatile "hybrid" professionals - such as DevSecOps engineers or hybrid IT-Security administrators-who are capable of simultaneously managing general IT infrastructure while implementing robust security protocols. This creates an unsustainable cognitive burden on individual employees. Furthermore, advanced cybersecurity education is currently heavily bottlenecked at the Roots level. Interviewees stressed that critical deficits in rigorous mathematics, algorithmic logic, and low-level programming curricula (such as C and C++) within undergraduate programs prevent students from fundamentally understanding system vulnerabilities, memory corruption, and the mechanics of sophisticated exploitation techniques.

8.3 Cross-Site Themes and Comparative Analysis

A comprehensive synthesis of the qualitative data successfully triangulates, validates, and significantly expands upon the quantitative metrics established in the CYCERONE survey detailed in Chapter 7. This synthesis reveals four primary, structural macro-themes that define the current European cybersecurity landscape. First, there is a systemic competency misalignment that goes far beyond a simple deficit of technical knowledge. It represents a structural, temporal lag between the bureaucratic cycle of academic curriculum development and the hyper-dynamic, iterative innovation of global threat actors. Second, a severe and crippling 'soft-skill' deficit exists within highly technical roles. Cross-functional collaboration, crisis management under psychological pressure, and executive risk articulation remain systematically underdeveloped in computer science graduates, directly corroborating and explaining the quantitative findings detailed in Section 7.4 [12, 31].

Third, the industry demonstrates a pronounced and urgent demand for agile micro-credentialing. The velocity of technological change dictates that professionals require modular, stackable training architectures. Industry leaders are advocating for short, targeted upskilling pathways and specialized, highly focused certifications rather than returning to universities for monolithic, multi-year degree programs. There is a strong desire to see these micro-credentials integrated into the European Credit Transfer and Accumulation System (ECTS) to ensure standardization. Finally, regulatory compliance now serves as the primary, undisputed driver for corporate and governmental training investments. Frameworks such as NIS2, which introduces personal liability for C-suite executives in the event of negligence, and the broader EU Cybersecurity Skills Academy initiative [36], are forcing institutional momentum. These regulatory instruments are transforming structured cybersecurity training from a discretionary operational expense into an absolute legal necessity, particularly within the interconnected frameworks of the public sector and critical infrastructure.

8.4 Summary of Interview Findings

The qualitative inquiry detailed in this chapter provides the necessary depth to interpret the baseline quantitative metrics of the CYCERONE project. Phenomenological findings confirm that technical inadequacies and communication barriers are interrelated factors; they create synergistic vulnerabilities that undermine overall organizational resilience.

A critical finding is the significant divergence in competency requirements across different sectors. While regulatory compliance is the primary focus within the corporate finance domain, the small and medium enterprise (SME) segment is primarily characterized by the constraints of limited resources. These distinctions validate the necessity of moving away from universal, "one-size-fits-all" training models.

Educational institutions should instead implement modular and adaptive learning architectures capable of dynamic content updates. The synthesis of these qualitative insights with the previously presented statistics establishes a robust empirical foundation for the strategic recommendations detailed in Chapter 9.

9. Conclusions

The analysis presented in this report confirms that the cybersecurity skills gap within the European Union is not merely a question of workforce shortage, but a systemic mismatch between the competencies demanded by organisations and those supplied by current education and training systems. Across all methodological pillars, a consistent pattern emerges: organisations require a combination of advanced technical capabilities, practical operational experience, and transversal skills, yet these are not sufficiently developed through existing educational pathways.

A central finding is the persistence of the theory-practice divide, with the majority of respondents identifying lack of hands-on experience and limited understanding of business context as the most critical shortcomings among graduates. This gap is further reinforced by divergent stakeholder perspectives, where academic institutions prioritise governance and regulatory knowledge, while industry and public administration emphasise operational effectiveness and real-world applicability.

Report also highlights structural constraints affecting SMEs and public administration, including limited training budgets, reduced access to certifications, and lower capacity to invest in workforce development. In this context, the finding that professional certifications are not perceived as highly valuable (mean: 3.15/5.00) is particularly significant, suggesting that current certification-driven approaches may not adequately address the needs of these target groups.

Furthermore, the analysis identifies emerging and interdisciplinary skill domains, such as OT/ICS security, AI/ML security, and sector-specific competencies, as critically underserved both in academic research and in training provision. This reflects a broader challenge in adapting educational systems to the rapidly evolving cybersecurity landscape.

Taken together, these findings demonstrate that addressing the cybersecurity skills gap in the EU requires a coordinated, multi-stakeholder response, focused on aligning education, training, and labour market needs. The CYCERONE project contributes to this objective by providing an empirical foundation for the development of practice-oriented, accessible, and targeted training solutions, particularly for SMEs and public administration bodies.

References

[1] Abbasi, N. and Smith, D. A. (2024) 'Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPAA compliance framework and the responsibilities of healthcare providers', Journal of Knowledge Learning and Science Technology, 3(3), pp. 278–287. doi: 10.60087/jklst.vol3.n3. p.278-287.

[2] Aftabi, N., Li, D. and Sharkey, T. C. (2024) 'An Integrated Cyber-Physical Framework for Worst-Case Attacks in Industrial Control Systems', IISE Transactions. doi: 10.1080/24725854.2024.2439856.

[3] Aitty, P. S. T. et al. (2024) 'Cybersecurity in Healthcare: IOT Security for Medical Devices', in Proceedings of ICCCNT 2024. IEEE. doi: 10.1109/icccnt61001.2024.10724329.

[4] Almoughem, K. (2023) 'The Future of Cybersecurity Workforce Development', Academic Journal for Research and Scientific Publishing, 45(3). doi: 10.52132/ajrsp.en.2023.45.3.

[5] Anthony, R. G. (2024) 'Adoption of Advanced Cybersecurity Tools by Organisations: Motivations, Barriers, and Leader Responses', Journal of Behavioural and Applied Management. doi: 10.21818/001c.126835.

[6] Argaw, S. T. et al. (2020) 'Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks', BMC Medical Informatics and Decision Making, 20(146). doi: 10.1186/s12911-020-01161-7.

[7] Aria, M. and Cuccurullo, C. (2017) 'bibliometrix: An R-tool for comprehensive science mapping analysis', Journal of Informetrics, 11(4), pp. 959–975.

[8] Armstrong, M. E. et al. (2020) 'Knowledge, Skills, and Abilities for Specialised Curricula in Cyber Defense: Results from Interviews with Cyber Professionals', ACM Transactions on Computing Education, 20(4). doi: 10.1145/3421254.

[9] Avdibasic, E., Toksanovna, A. S. and Durakovic, B. (2022) 'Cybersecurity challenges in Industry 4.0: A state of the art review', Defense and Security Studies, 3. doi: 10.37868/dss.v3.id188.

[10] BCG (2024) 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap. Boston Consulting Group.

[11] Bulai, R., Turcanu, D. S. and Ciorba, D. (2022) 'Education in Cybersecurity', Central and Eastern European eDem and eGov Days. doi: 10.24989/ocg.v335.2.

[12] Catal, C. et al. (2022) 'Analysis of cyber security knowledge gaps based on cyber security body of knowledge', Education and Information Technologies. doi: 10.1007/s10639-022-11261-8.

[13] CyberHubs (2024) Cybersecurity Skills Needs Analysis Summary Report. Available at: https://cyberhubs.eu.

[14] Dawson, M. et al. (2021) 'Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors', Romanian Armed Forces Technical Bulletin. doi: 10.2478/RAFT-2021-0011.

[15] Dillon, R. and Tan, K.-L. (2023) 'Cybersecurity Workforce Landscape, Education, and Industry Growth Prospects in Southeast Asia', Journal of International Affairs. doi: 10.1177/27538931231176903.

[16] ENISA (2024) 2024 Report on the State of Cybersecurity in the Union. European Union Agency for Cybersecurity.

[17] European Commission (2024) EU Faces Growing Cybersecurity Skills Gap, New Eurobarometer Reveals. Digital Skills and Jobs Platform.

[18] Fortinet (2024) 2024 Cybersecurity Skills Gap Global Research Report. Fortinet.

[19] Gandhi, N. (2024) 'CSPM for Healthcare: Securing Electronic Health Records (EHR) and Ensuring HIPAA Compliance', IJSRCSEIT. doi: 10.32628/cseit241061174.

[20] Graham, C. M. and Lu, Y. (2022) 'Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements', Journal of Computer Information Systems. doi: 10.1080/08874417.2022.2115954.

[21] Gupta, M., Ryan, J. and Boyer, T. (2024) 'Mitigating the Humans Risks to Cybersecurity Posture', in Advances in Information Security, Privacy, and Ethics. IGI Global. doi: 10.4018/979-8-3693-4211-4.ch002.

[22] Hall, J. L. and Rao, A. (2024) 'Gender of Recruiter Makes a Difference: A study into Cybersecurity Graduate Recruitment'. arXiv:2408.05895.

[23] Hulatt, D. and Stavrou, E. (2021) 'The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation', in Proceedings of IFIP SEC 2021. Springer. doi: 10.1007/978-3-030-81111-2_12.

[24] IBM (2024) Skills Shortage Directly Tied to Financial Loss in Data Breaches. IBM.

[25] ISC2 (2024) Cybersecurity Workforce Study 2024. International Information System Security Certification Consortium.

[26] Jager, M. de, Futcher, L. and Thomson, K.-L. (n.d.) 'An Investigation into the Cybersecurity Skills Gap in South Africa', in Springer. doi: 10.1007/978-3-031-38530-8_19.

[27] John, S. et al. (2020) 'Cybersecurity Education: The Skills Gap, Hurdle!', in Springer. doi: 10.1007/978-3-030-50244-7_18.

[28] Kannelonning, K. and Katsikas, S. K. (2023) 'A systematic literature review of how cybersecurity-related behavior has been assessed', Information and Computer Security. doi: 10.1108/ics-08-2022-0139.

[29] Komarov, M. et al. (2022) 'Recommendations for Ensuring Cyber Protection of Industrial Control Systems of Energy Sector', Electronic Modelling. doi: 10.15407/emodel.44.05.061.

[30] Lukauskas, M. et al. (2023) 'Enhancing Skills Demand Understanding through Job Ad Segmentation Using NLP', Applied Sciences. doi: 10.3390/app13106119.

[31] Martin, A. P. and Collier, J. (2020) 'Beyond awareness: Reflections on meeting the inter-disciplinary cyber skills demand', in Routledge. doi: 10.4324/9780367822576-3.

[32] Mohapatra, A. and Ramanathan, K. G. (2022) 'Cybersecurity anatomisation and assurance of industrial control systems', AIP Conference Proceedings. doi: 10.1063/5.0122823.

[33] Palczynska, M. and Rynko, M. (2021) 'ICT skills measurement in social surveys: Can we trust self-reports?', Quality and Quantity, 55, pp. 965–984. doi: 10.1007/s11135-020-01031-4.

[34] Paul, E. O. et al. (2023) 'Cybersecurity Strategies for Safeguarding Customer Data and Preventing Financial Fraud', International Journal on Soft Computing. doi: 10.5121/ijsc.2023.14301.

[35] Prabhakar, S., Nalinaksha, I. and Anjaneyulu, V. (2023) 'Role of AI in enhancing cybersecurity measures to protect sensitive financial data', IJSRA. doi: 10.30574/ijsra.2023.10.1.0700.

[36] Spanou, D. (2024) 'The EU Cybersecurity Skills Academy: A silver bullet to address the cyber security skills gap in the European Union?'. doi: 10.69554/kono7296.

[37] Streich, G. (2023) '(Re-)Configuring Federal Cybersecurity Regulation: From Critical Infrastructures to the Whole-of-the-Nation', Indiana Law Review. doi: 10.18060/27133.

[38] Ternikov, A. A. (2022) 'Soft and hard skills identification: insights from IT job advertisements in the CIS region', PeerJ Computer Science. doi: 10.7717/peerj-cs.946.

[39] Uzougbo, N. S., Ikegwu, C. G. and Adewusi, A. O. (2024) 'Cybersecurity compliance in financial institutions: A comparative analysis', IJSRA. doi: 10.30574/ijsra.2024.12.1.0802.

[40] Vakulyk, O. et al. (2020) 'Cybersecurity as a component of the national security of the state', Journal of Security and Sustainability Issues. doi: 10.9770/JSSI.2020.9.3(4).

[41] Vivek, R., Nanthagopan, Y. and Piriyatharshan, S. (2023) 'Beyond methods: Theoretical underpinnings of triangulation in qualitative and multi-method studies', Scientific Studies on Social and Political Psychology. doi: 10.61727/sssppj/2.2023

[42] Yadav, S., Kalaskar, K. D. and Dhumane, P. D. P. (2022) 'A Comprehensive Survey of IoT-Based Cloud Computing Cyber Security', Oriental Journal of Computer Science and Technology. doi: 10.13005/ojcst15.010203.04.

[43] Yao, M. and Xu, Y. C. (2021) 'Method Bias Mechanisms and Procedural Remedies', Sociological Methods and Research. doi: 10.1177/00491241211043141.

[44] IEEE Xplore Digital Library (n.d.) Institute of Electrical and Electronics Engineers. Available at: https://ieeexplore.ieee.org

[45] ACM Digital Library (n.d.) Association for Computing Machinery. Available at: https://dl.acm.org

[46] Scopus (n.d.) Abstract and Citation Database. Elsevier. Available at: https://www.scopus.com

[47] ISACA (n.d.) Information Systems Audit and Control Association. Available at: https://www.isaca.org

[48] LinkedIn (n.d.) Professional Network. Microsoft Corporation. Available at: https://www.linkedin.com

[49] Indeed (n.d.) Employment Search Platform. Indeed Inc. Available at: https://www.indeed.com

[50] Nethisinghe, M. et al. (2023) 'A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions', IEEE Communications Surveys & Tutorials, 26(1), pp. 1–35. doi: 10.1109/COMST.2023.3312349.

[51] Singh, A. and Chatterjee, K. (2024) 'Security in 5G Network Slices: Concerns and Opportunities', IEEE Access, 12, pp. 58634–58656. doi: 10.1109/ACCESS.2024.3386632.

[52] Siddiqui, F. et al. (2023) 'Cybersecurity engineering: bridging the security gaps in advanced automotive systems and ISO/SAE 21434', in Proceedings of the 97th IEEE Vehicular Technology Conference (VTC2023-Spring). IEEE. doi: 10.1109/VTC2023-Spring57618.2023.10200490.

[53] Ward, D. and Wooderson, P. (2022) 'Automotive Cybersecurity: An Introduction to ISO/SAE 21434', SAE International, pp. 1–120. doi: 10.4271/9781468603417.

[54] European Forum for Urban Security (2026) 'Where have all the security professionals gone?', Efus. Available at: https://efus.eu/topics/mediation-security-professions/where-have-all-the-security-professionals-gone/ (Accessed: 28 April 2026).

[55] The Cyber Express (2025) 'ENISA: Cyber Talent Shortage Pushes EU Firms Toward Tech and Outsourced Security', The Cyber Express. Available at: https://thecyberexpress.com/cybersecurity-investments-nis-report/ (Accessed: 28 April 2026).

Appendix A – Cybersecurity Skills Gap Survey Instrument

This appendix presents the complete set of questions used in the "Cybersecurity Skills Gap Survey for Industry & Academia" (CYCERONE project). The survey utilizes branching logic based on the respondent's primary professional role.

Part 1: Initial Routing (All Respondents)

1. Please identify your primary professional role. (Determines branching for subsequent sections)
   - Industry Professional
   - Academic Professional
   - Public Administration Professional

Part 2: Professional Profile (Branching)

Branch A: Industry Profile

2A.1. In which country do you primarily work? [Open text]
2A.2. Please specify your organization's primary sector:
   - Information Communication Technology
   - Finance
   - Healthcare
   - Critical Infrastructure (e.g., Transportation/Energy/etc.)
   - Legal, Law Enforcement, Military
   - Public sector
   - Manufacturing
   - Other

2A.3. Please specify your primary role:
   - Cybersecurity practitioner/specialist
   - Cybersecurity (hiring) manager
   - Early career professional
   - Decision makers (e.g., board member)
   - Other

2A.4. Please specify your organization's size:
   - Small or Medium-sized Enterprise (SME) - up to 249 employees
   - Large Enterprise
   - Public Administration

Branch B: Academic Profile

2B.1. In which country is your institution located? [Open text / Dropdown] 2B.2. Please specify your institution's type:
   - University

- University of Applied Sciences
- Vocational School/College
- Private Training Provider
- Other

2B.3. Please specify the primary focus of your program/department:

- Cybersecurity (dedicated program)
- Computer Science
- Information Technology
- Engineering
- Mathematics
- Legal/Compliance
- Administration
- Other

Branch C: Public Administration Profile

2C.1. In which country do you primarily work? [Open text / Dropdown] 2C.2. Please specify your organization's primary domain:

- National/Federal Government
- Regional/State Government
- Local Government
- Law Enforcement
- Military
- Critical Infrastructure Authority (e.g., Energy, Transportation)
- Regulatory Agency
- Other

2C.3. Please specify your primary role:

- Cybersecurity Practitioner / Specialist
- Cybersecurity Policy / Governance
- Cybersecurity (hiring) manager
- Decision Maker (e.g., department head)
- Early Career Professional
- Other 2C.4. Please specify your organization's size:
- Small or Medium-sized Entity (up to 249 employees)
- Large Entity (250 or more employees)

Part 3: The Skills Landscape (All Respondents)

Note: All questions in this section use a Likert scale from 1 (Not Important now) to 5 (Critically Important), plus a "Don't know" option.

3.1. How important are the following Core Technical Skills for a cybersecurity professional in your organization?

- Cloud Security (e.g., secure configuration, IAM)
- Systems, Network & Security Architecture/Design
- Incident Response & Management
- Cyber Threat Intelligence & Analysis
- Web & Application Security
- Data Security, Privacy & Cryptography
- Digital Forensics
- Penetration Testing

3.2. How important are the following Advanced / Specialized Skills for a cybersecurity professional in your organization?

- Operational Technology (OT) / ICS Security
- Artificial Intelligence (AI) / Machine Learning Security
- Secure Software Development / DevSecOps

3.3. How important are the following Non-Technical ("Soft") Skills for a cybersecurity professional in your organization?

- Problem-Solving & Critical Thinking
- Communication to non-technical audiences
- Communication to technical audiences
- Analytical Thinking
- Leadership & Strategic Thinking (Risk Management)
- Teamwork & Collaboration

3.4. On a scale of 1 (No Gap) to 5 (Critical Gap), to what extent do you consider your organization is lacking the following Governance & Supporting skills among cybersecurity professionals?

- Legal, Regulatory & Policy Compliance
- Auditing & Assurance
- Risk Management & Governance
- Training, Awareness & Education

Part 4: Identifying Gaps & Preparedness (Branching)

4.1. General Question (Asked prior to branch-specific matrices) What do you perceive as the biggest barriers to filling cybersecurity roles in your organization? (Select all that apply)

- Lack of qualified candidates
- Competition from other employers
- High salary expectations
- Lack of practical experience among applicants
- Insufficient education or certification options
- Lack of awareness of cybersecurity careers
- Other

Branch A: Industry Perspective

4A.1. Based on recent graduates you have hired or interviewed, how would you rate the extent to which they lack competence in the following key areas? (Scale: 1 - Fully Competent to 5 - Severely Lacking, plus "Don't know")

- Cloud Security (Practical, hands-on skills)
- Web and Mobile Security (Practical, hands-on skills)
- Operational Technology (OT) Security (Interdisciplinary skills)
- AI/Machine Learning Security (Interdisciplinary skills)
- Incident Management (High-pressure, practical skills)
- Communication (Translating technical risk to business impact)
- Information Security Fundamentals (Policies, controls, defense basics)
- Threat Intelligence (Collection, analysis, reporting)
- Security Architecture & Systems Design (Designing secure systems/networks)

Branch B: Academic Perspective

4B.1. How would you rate your institution's ability to provide effective, hands-on training in the following key areas? (Scale: 1 - Highly Ineffective to 5 - Highly Effective, plus "Don't know")

- Cloud Security (Practical, hands-on skills)
- Web and Mobile Security (Practical, hands-on skills)
- Operational Technology (OT) Security (e.g., using realistic labs)
- AI/Machine Learning Security (e.g., access to GPU clusters/data)
- Incident Management (e.g., high-pressure simulations)
- Communication (Integrating business context into technical courses)
- Implementation & Systems Testing (practical deployment & testing skills)
- Digital Forensics (investigation & evidence handling)
- Penetration Testing (offensive security skills)
- Risk Management (basic assessment & mitigation approaches)

Branch C: Public Administration Perspective

4C.1. Based on recent graduates you have hired or interviewed for public sector roles, how would you rate the extent to which they lack competence in the following key areas? (Scale: 1 - Fully Competent to 5 - Severely Lacking, plus "Don't know")

- (Note: Uses the exact same 10 skills listed in 4B.1)

Part 5: Education, Training, and Collaboration (Branching)

Branch A & B (Combined flow for Industry/Academia in the survey)

5A/B.1. What are the most significant shortcomings you observe in graduates entering the cybersecurity workforce?

- Lack of practical, hands-on experience
- Poor understanding of business context and risk management
- Underdeveloped soft skills (communication, teamwork)
- Insufficient knowledge of current regulations (e.g., NIS2, GDPR)
- Lack of familiarity with modern tools and technologies
- Lack of problem solving, investigation and learning skills
- Other

5A/B.2. Value placed on credentials/certifications: (Scale: 1 to 5, plus "Don't know")

- How much value do you place on professional certifications (e.g., CISSP, OSCP) when upscaling employees?
- How much value do you place on professional certifications when evaluating candidates?
- How much value do you place on academic certifications?
- How much value do you place on formal credentials?

5A/B.3. How effective is the current level of collaboration between academia and industry in your country for addressing the skills gap? (Scale: 1 to 5, plus "Don't know")

Specific Additional Question for Branch B (Academia)

5B.4. What are the biggest barriers your institution faces in providing practical, hands-on cybersecurity trainings?

- High cost of equipment and virtual lab environments
- Lack of faculty with up-to-date industry experience
- Rigid curriculum structures that are slow to adapt
- Insufficient collaboration with industry partners
- Difficulty in simulating realistic, large-scale cyber-attacks
- Lack of engagement and time

- Other

Branch C: Public Administration

5C.1. What are the most significant shortcomings you observe in graduates entering the public cybersecurity workforce?

- Lack of practical, hands-on experience
- Poor understanding of public policy, legal frameworks, and risk management in a government context
- Underdeveloped soft skills (communication, inter-agency collaboration)
- Insufficient knowledge of specific government/public sector regulations (e.g. NIS2, DORA)
- Lack of familiarity with public sector procurement and technology adoption cycles
- Lack of problem solving investigation and learning skills
- Other

5C.2. How much value does your organization place on the following when hiring or upskilling employees? (Scale: 1 - No Value to 5 - High Value, plus "Don't know")

- Professional certifications (e.g., CISSP, OSCP)
- Academic certifications (e.g., degrees)
- Security clearance
- Formal government-led training programs

5C.3. How effective is the current level of collaboration between academia, industry, and the public sector in your country for addressing the skills gap? (Scale: 1 - Highly Ineffective to 5 - Highly Effective, plus "Don't know")

Part 6: Future Outlook and Recommendations (All Respondents)

6.1. From the list below, please rank most crucial skills for a cybersecurity professional, from most important to least important.

- AI and Machine Learning Security
- Cloud Security Architecture (Networking, TCP/IP stack)
- Operational Technology (OT) Security
- Quantum Computing Security
- Supply Chain Risk Management
- Data Privacy and Protection
- Board-level Governance and Communication
- Threat Intelligence Analysis

6.2. Does your organization invest in upskilling or reskilling employees in cybersecurity?

- Yes, with formal training programs
- Yes, occasionally or informally
- No, but we are planning to
- No
- Don't know

6.3. Which types of education or training do you think would be most effective in closing the cybersecurity skills gap? (Select all that apply)

- University degree programs
- Professional certifications (e.g., CISSP, CEH, CompTIA)
- Short courses / micro-credentials
- On-the-job training or apprenticeships
- Online self-paced learning
- Bootcamps or intensive programs
- Government-supported training initiatives
- Other

6.4. What formats do you prefer for cybersecurity education?

- In-person classroom learning
- Online live sessions
- Self-paced online modules
- Blended learning (online + in-person)
- Hands-on labs or simulations
- Mentoring / coaching
- Other

6.5. From your professional perspective, what topics or skills should cybersecurity education and training emphasize?

- [Open-ended text response]

6.6. What would you recommend for improving the cybersecurity workforce?

- [Open-ended text response]