Cybersecurity Micro-credentials and Career Path Design: The Digital4Security Good Practices

Sara Ricci[1](✉), Petr Dzurenda[1], Carmel Somers[2], Horacio González-Vélez[3], and Lisa Janine Moravek[1]

[1] Brno University of Technology, Brno, Czechia
{ricci,dzurenda,moraveklisa}@vut.cz
[2] Digital Technology Skills, Dublin, Ireland
carmel.somers@digitaltechnologyskills.ie
[3] Cloud Competency Centre, National College of Ireland, Dublin, Ireland
horacio@ncirl.ie

Abstract. Cybersecurity is critical to safeguarding digital economies, yet the sector faces a significant expert shortage. Addressing this gap requires scalable and flexible education to upskill both specialists and nonspecialists. This paper introduces a novel, good-practice methodology for the design of micro-credentials and an AI-driven career path planning solution, both aligned with the European Cybersecurity Skills Framework (ECSF). The primary objective is to support the scalable development of standardized, ECSF-aligned cybersecurity micro-credentials that address evolving labour market needs and facilitate personalized career progression. The proposed approach is validated through the Digital4Security case study, where 17 ECSF-aligned micro-credentials were developed and analyzed. Additionally, a dedicated open-source web application, the Cybersecurity Career Path Designer, supports personalized pathway planning for users by matching existing skills to ECSF profiles. This work demonstrates a practical and scalable framework for aligning education with cybersecurity market needs.

Keywords: Micro-credentials · Career Path · ECSF Framework · Cybersecurity Education · Methodology

1 Introduction

Cybersecurity is critical to protecting governments, businesses, and individuals, especially as digital technologies become central to modern economies. The COVID-19 pandemic intensified the reliance on digital platforms, thereby increasing exposure to cyber threats [15]. Despite a record number of 5.5 million professionals in the field, the global cybersecurity workforce faces a 4.7 million shortfall, with Europe alone lacking more than 392,000 experts [10].

F. Skopik et al. (Eds.): ARES 2025 Workshops, LNCS 15999, pp. 77–95, 2025.
https://doi.org/10.1007/978-3-032-00644-8_5

Public sector institutions, such as governments and central banks, face particular difficulty in attracting skilled talent compared to private industries such as finance [13]. The European Network and Information Security Agency (ENISA) has repeatedly highlighted not only the scarcity of professionals, but also the urgent need for continuous and up-to-date training in the legal, technical, and policy domains [7,13]. Addressing this talent gap requires flexible and scalable education to up-skill both specialists and the broader population.

Our pan-European survey [19] conducted between December 2023 and January 2024, as part of the DIGITAL4Security initiative, yielded 190 valid responses from cybersecurity professionals in 14 EU member states. Among the various insights garnered, a notable finding pertains to program delivery preferences: 24% of respondents expressed a preference for modular learning formats that award micro-credentials. This preference underscores the growing demand for flexible, skills-focused, and stackable educational offerings that allow learners to gain recognition for discrete areas of expertise. This inclination aligns with broader trends in higher education, where micro-credentials are increasingly recognised as viable pathways for rapid upskilling and continuous professional development. Recent research highlights that micro-credentials offer learners short, practical, and up-to-date courses tailored to specific career paths, thereby enhancing employability and meeting the dynamic needs of the workforce [21]. Furthermore, the potential of micro-credentials to revolutionize higher education by providing modular, competency-based learning opportunities that are responsive to technological advancements and stakeholder expectations has also been cited [1].

1.1 Contributions and Paper Organisation

This paper contributes to advancing cybersecurity education by proposing a novel, good-practice methodology for the design of micro-credentials and an AI-driven solution for career path planning, both aligned with the European Cybersecurity Skills Framework (ECSF). The primary objective is to support the scalable development of standardised, ECSF-aligned cybersecurity micro-credentials that address evolving labour market needs and facilitate personalised career progression. This investigation is guided by the following research questions (RQs):

(RQ1) *How can effective micro-credentials be designed to align with ECSF roles while ensuring quality, modularity, and relevance?*

(RQ2) *How can AI and optimization techniques be applied to support micro-credential labelling and career path development in cybersecurity?*

(RQ3) *How can a usable, practical tool be developed to assist learners in exploring and planning cybersecurity career paths using micro-credentials?*

The rest of the article is organised as follows. Section 2 reviews the current state of micro-credentials in the EU. Section 3 outlines the foundational components of our approach, including the ECSF and the AI and optimisation techniques employed. Section 4 presents our micro-credential development methodology, addressing RQ1 by detailing the mapping of learning outcomes to ECSF profiles and the quality evaluation process. Section 5 introduces the career path development methodology, addressing RQ2 through AI-driven labelling, ECSF-based profile matching, and ILP-based optimization. Section 6 describes the CCPD tool, supporting RQ3, while Sect. 7 illustrates its application through a case study based on Digital4Security micro-credentials. The final section provides concluding remarks and outlines potential next steps.

2 The European Micro-credentials Landscape

Micro-credentials have emerged as significant policy and educational innovation in Europe, responding to the increasing demand for flexible, accessible, and modular learning pathways. This demand is driven by the convergence of several factors, including digital and green transitions, demographic change, global economic changes, and the aftermath of the COVID-19 pandemic. In this context, the EU has taken strategic steps to formalise a common European approach to micro-credentials, as evidenced by the Council Recommendation of June 2022 [17] and the preceding 2021 proposal [16] of the European Commission. These instruments provide a structured framework for the development, implementation, recognition, and quality assurance of micro-credentials across Member States, sectors, and institutional providers. The core rationale behind micro-credentials lies in their potential to support lifelong learning and enhance employability. They offer a flexible, learner-centred modality for acquiring specific skills and competences without the need to commit to long, full-degree programmes. According to the Council Recommendation 2022 [17]:

> "*Micro-credentials are defined as documented statements of learning outcomes that result from a small volume of learning, assessed against transparent criteria and underpinned by quality assurance. Crucially, they are designed to be portable, shareable and, where appropriate, stackable, that is, capable of being combined into larger credentials or qualifications depending on national and institutional frameworks.*"

The Recommendation proposes a standardised set of descriptors and principles to ensure comparability and mutual recognition across borders. These include the title of the micro-credential, issuing body, learning outcomes, notional workload, preferably expressed in European Credit Transfer System (ECTS), assessment methods, quality assurance processes, and the level and type of learning achieved and linked, where applicable, to the European Qualifications Framework (EQF). Such standards are vital for transparency, facilitating recognition across Member States and between education and labour market systems. The landscape of micro-credentials in Europe is heterogeneous. Some countries, such as Ireland, France, and the Netherlands, have begun integrating micro-credentials into their national qualifications frameworks. Ireland's National Framework of Qualifications has initiated pilots to incorporate micro-credentials within formal and non-formal learning systems [18]. In France, the development of "certificats de compétences" and their integration into the "Répertoire Spécifique" serves a similar purpose [22]. Meanwhile, Dutch higher education institutions have explored micro-credentials through stackable modules within Bachelor's and Master's programmes, often supported by the SURF platform and national funding initiatives [11]. At the institutional level, alliances of European universities under the Erasmus+ programme have launched a key pilot project for transnational micro-credential schemes. These alliances serve as testbeds for cross-border recognition and interoperability [9].

In terms of application, micro-credentials offer several benefits. They support personalised learning by allowing people to acquire competencies at their own pace and according to their specific goals. They enable rapid response to labour market demands by providing focused training in areas of emerging need. For employers, micro-credentials facilitate targeted workforce development and can serve as tools for human resource management, particularly in sectors undergoing transformation. For education providers, they open new avenues for participation with adult learners, professionals, and non-traditional student populations. Despite these advantages, there are considerable challenges. One of the primary issues is the lack of harmonised quality assurance across different types of providers. While higher education institutions typically operate within established accreditation systems, non-formal providers such as private companies or civil society organisations may lack formal mechanisms for quality control. Recognition is another area of concern. Although the European approach proposes a common definition and standards, the degree to which Member States adopt and implement these measures remains variable. In particular, questions remain about the stackability of micro-credentials and the authority of different providers to issue them.

The integration of micro-credentials into employment and active labour market policies also holds promise. Training linked to micro-credentials can be included in recognised programmes supported by individual learning accounts or public employment services. They can be used to address skills bottlenecks in specific sectors or regions and to support transitions between employment statuses, including for self-employed and platform workers. The Council Recommendation explicitly suggests their use in fulfilling mandatory training requirements and supporting re-entry into the labour market for long-term unemployed or low-qualified individuals. To fully realise the potential of micro-credentials, the Commission has committed to several supportive measures. These include developing quality assurance guidelines, adapting existing tools such as the ECTS user guide, enhancing interoperability through the Europass platform, and promoting research and dialogue among stakeholders. Furthermore, EU funding mechanisms, particularly Erasmus+ and the European Social Fund Plus (ESF+), provide financial support for pilot projects, capacity building, and implementation activities.

3 Key Components of Cybersecurity Skill Development

In this section, we describe the key components of our cybersecurity skill development. Specifically, Sect. 3.1 introduces the ECSF framework, Sect. 3.2 looks at the REWIRE project and its relevant outputs on automated curriculum design, and Sect. 3.3 presents the Digital4Security project and its skill needs analysis which is the basement of our micro-credential design methodology.

3.1 European Cybersecurity Skills Framework

The European Cybersecurity Skills Framework (ECSF) [6] is a practical tool developed by ENISA and its ad-hoc working group to support the identification and articulation of tasks, competencies, skills, and knowledge relevant to cybersecurity roles in Europe. It aims to provide a standardised reference for roles, competencies, skills, and knowledge within the cybersecurity domain, supporting skills recognition and the structured development of cybersecurity training programs. The ECSF framework categorises the cybersecurity workforce into 12 distinct profiles, each analysed in terms of key tasks, required skills, and knowledge areas. In total, the framework identifies 84 key skills and 69 key knowledge areas, offering a comprehensive taxonomy to guide academic curricula and training content. The 12 ECSF profiles include: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator, and Penetration Tester.

3.2 REWIRE Skills Grouping and Cybersecurity Profiler

The REWIRE Cybersecurity Profiler (CSProfiler) [4] Web application tool supports the development of curriculum aligned with the ECSF through six steps: collection of data from academic sources, AI-assisted course labelling for the alignment of the ECSF, manual refinement, and presentation of results based on user-defined profiles. A central challenge in using the ECSF framework is the diverse phrasing of its 84 skills and 69 knowledge areas in 12 professional profiles. To improve clarity, REWIRE introduced a grouping method that clusters similar skills and knowledge areas into 31 coherent categories. These clusters were initially derived from the NIST NICE competencies [23], adapted to the European context, and validated by cybersecurity experts. The grouping improves the usability of the ECSF, facilitates clearer links between roles and competencies, and reveals possible gaps in the current ECSF structure that could inform future updates. We refer to [3] for more details.

To automate skill identification in course descriptions, REWIRE employed an AI-based labelling methodology using a Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) architecture [2]. Trained on 937 manually labelled cybersecurity job ads, the model predicts relevant skills with consistency across academic and industry datasets. This enables cross-domain skill mapping and supports curriculum alignment with labour market demands. The approach reduces manual workload, improves scalability, and ensures a feedback loop for continuous curriculum refinement. After training, the model labels each course description with the appropriate cybersecurity skill groups and, consequently, maps the proposed curriculum to the coverage of the ECSF profiles.

To determine the optimal combinations of curriculum courses to achieve the desired ECSF profile, REWIRE used an Integer Linear Programming (ILP) [14] method, specifically 0–1 ILP, since the decision variables (i.e. whether to select a course or not) are binary in nature. This algorithm identifies the best combination of courses based on user-defined input conditions, such as the number of years of the study programme, the maximum number of courses per semester, the total number of ECTS credits, and the desired ECSF profiles to be covered by the curriculum.

3.3 Digital4Security Mission and Skills Needs Analysis

Digital4Security is a ground-breaking pan-European master's programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This four-year initiative has received support from a Consortium comprising 31 partners spanning 14 countries. The consortium aims to design a European Master's Program in Cybersecurity Management & Data Sovereignty. The goal is to equip European businesses, particularly SMEs, with the critical skills needed to prevent and respond to cybersecurity threats, ensuring a secure digital future for all.

As an initial step, the Digital4Security project conducted a survey [19] between December 2023 and January 2024, collecting 190 valid responses from cybersecurity professionals across 14 EU member states. Aligned with the ECSF, the survey aimed to identify priority knowledge areas and competencies to ensure alignment with evolving cybersecurity threats. The results confirmed a strong foundation of established skills, while also highlighting the growing importance of communication, creativity, technical proficiency, and integrity. The survey design focused on seven key ECSF role profiles (i.e., CISO, Cyber Threat Intelligence Specialist, Cybersecurity Educator, Digital Forensics Investigator, Cybersecurity Auditor, Risk Manager, and Cyber Legal, Policy & Compliance Officer) to gather role-specific insights. It also explored expectations for the master's programme and addressed concerns from organisations managing sensitive data or operating smart technologies, where targeted cybersecurity threats are more prevalent.

4 Micro-credentials Development Methodology

We propose a novel methodology for micro-credential development that strengthens the connection between academia and industry. Specifically, micro-credential Learning Outcomes (LOs) and lecture content serve as detailed descriptors, offering a structured framework for articulating the skills and knowledge that students are expected to acquire. The proposed methodology consists of three steps:

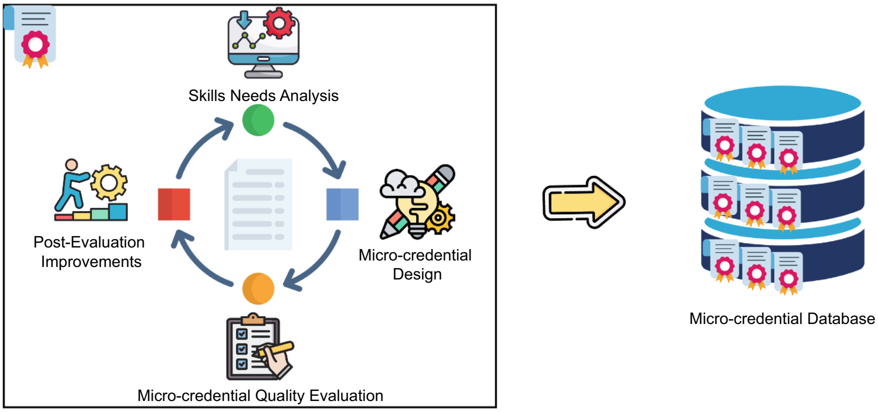

Skills Needs Analysis
Micro-credential Design
Micro-credential Quality Evaluation
Post-Evaluation Improvements
Micro-credential Database

Fig. 1. Micro-credentials Development Methodology.

(1) a skills needs analysis focused on current market demands in the cybersecurity field, with particular emphasis on ECSF role profiles; (2) a micro-credential design strategy informed by the skills analysis and aligned with the existing Digital4Security Master's programme in Cybersecurity Management & Data Sovereignty; and (3) a micro-credential quality evaluation that reflects market needs and ECSF profiles. The proposed methodology is depicted in Fig. 1

From an educational design perspective, integrating micro-credentials into the Digital4Security programme offers several strategic advantages. It aligns with contemporary pedagogical trends that emphasise modularization, personalization, and lifelong learning. In addition, it reflects the increasing importance of competency-based education in fields such as cybersecurity, where professionals must continuously adapt to emerging threats, regulatory requirements, and technological innovations. Additionally, micro-credentials provide an avenue for recognizing prior learning and professional experience, thus enhancing the inclusivity and accessibility of the programme.

Considering these findings and scholarly perspectives, the inclusion of micro-credential pathways in the Digital4Security curriculum represents a pedagogically informed response to the increasing demand for flexibility in higher education. This approach supports the development of modular and adaptable programme structures that can better accommodate the varied learning needs and professional contexts of cybersecurity practitioners across Europe.

4.1 Skills Needs Analysis

Having proven relevant for funded European projects that focus on digital skills [20], needs analyses identify the level of skills and training requirements in a given team or organisation. For the Digital4Security project, in designing the survey each step was carefully planned and executed, starting by setting a clear objective to guide the creation of focused and relevant questions. The survey was structured logically, with questions phrased using plain English principles, encompassing a variety of formats including multiple-choice and open-ended responses. The survey was designed to be concise (the average was 11 min to complete), in anticipation of a higher completion rate, and was optimised for mobile devices to facilitate accessibility. Prior to the survey's launch, a pilot test was conducted to address any potential issues. The utmost importance was placed on maintaining respondents' privacy and anonymity. Clear instructions and an explanatory introduction were provided at the outset. Effective distribution strategies were employed, and a detailed plan for data analysis was defined. The survey questions aimed to:

1. identify the *first and second most in-demand cybersecurity roles* within respondents' organizations to inform the design of relevant micro-credential content;
2. determine the *three most important skills* required for cybersecurity professionals;
3. assess the *key knowledge areas and skills* necessary for cybersecurity management roles.

These questions were carefully selected to ensure the survey captures actionable insights directly linked to curriculum development. By identifying the most in-demand cybersecurity roles, we aim to align micro-credential content with real organisational needs, thereby enhancing employability and relevance. Determining key skills and knowledge areas for general and management-specific roles allows us to design content that supports both up-skilling and role-specific professional development. Given the Master's programme's emphasis on cybersecurity management, this focus ensures that the micro-credentials reflect the competencies required for leadership positions in the field.

4.2 Micro-credential Design

Our micro-credential design strategy is informed by the skills needs analysis and the existing Digital4Security master's programme in Cybersecurity Management & Data Sovereignty. This approach incorporates the following good-practice strategies:

- **Need:** Micro-credentials must address current market demands.
  Response: We selected components from the proposed master's programme that correspond to the most in-demand skills. Notably, the master's programme was itself developed based on the skills needs analysis. By further selecting cybersecurity topics that reflect emerging trends, we strengthen our alignment with labour market demands.
- **Need:** Micro-credentials should follow a standardised methodology to ensure scalability and broad adoption.
  Response: Our micro-credentials are aligned with the ECSF role profiles, and each credential includes a clear mapping to the relevant ECSF profile. This enables learners to target the skills required for specific roles.

- **Need:** Micro-credentials must support modularity, personalization, and upskilling pathways.

  Response: Each master's module is designed to carry 5 or 10 ECTS. To enhance flexibility and personalization, these modules are divided into smaller, topic-oriented micro-credentials tailored to learners' specific needs.
- **Need:** Micro-credentials should respond to company demands and promote understanding between industry and education sectors.

  Response: Industry partners are actively involved in content development, design and evaluation. In particular, their direct participation in teaching ensures the delivery of practice-oriented and industry-relevant education.

4.3 Micro-credential Quality Evaluation

The methodological approach to evaluating micro-credentials offered as part of a master's programme in Digital4Security involves a number of stages. The target learners for this programme are non-technical but digitally aware individuals seeking to enhance their professional competence in the domain of cybersecurity and digital risk. The methodology supports a structured evaluation of the micro-credential curriculum to ensure academic rigour, industry relevance, and alignment with the ECSF. Each section of the methodology corresponds to a specific evaluative action to ensure complete validation of the curriculum.

1. **Alignment of Learning Outcomes with Lesson Content:** A mapping matrix cross-references Learning Outcomes (LOs) with lesson titles and descriptions to verify alignment [12]. Lessons not clearly supporting LOs are flagged, and revisions are proposed where gaps are found.
2. **Application of Bloom's Taxonomy at Master's Level:** LOs are analysed for alignment with EQF Level 7 using Bloom's Taxonomy. Action verbs are categorised by cognitive domain to confirm expectations of specialised knowledge, critical thinking, and independent judgement [8].
3. **Content Accessibility for Non-Technical, Digitally Aware Learners:** Lesson structure and language are reviewed for accessibility. Technical jargon and assumed prior knowledge are identified, and recommendations ensure clarity and inclusivity for digitally literate but non-technical learners.
4. **Relevance to Industry Roles:** Content is mapped to industry roles using frameworks and job taxonomies. This identifies relevant professional profiles (e.g., DPO, Risk Analyst) and demonstrates alignment with practical applications [5].
5. **Mapping to ECSF Role Profiles:** LOs and content are cross-referenced with ECSF competencies to identify aligned roles (e.g., Policy Professional, Risk Manager). Gaps in knowledge or skills are documented for future development.
6. **Evaluation of Content Flow, Quality, and Coverage:** The sequence and coherence of content are evaluated through LOs and module descriptors. The analysis checks for logical progression, topic integration, and redundancy or omission.

7. **Identification of Content Gaps via ECSF Alignment:** Gaps in ECSF-related knowledge or skills are identified through re-analysis. Recommendations focus on enhancing applied content to better prepare learners for ECSF-aligned roles.

Through the application of this multi-dimensional evaluation methodology, curriculum developers and academic coordinators can ensure that micro-credentials in Digital4Security are pedagogically sound, appropriately challenging, accessible to the target learner, and aligned with the strategic goals of cybersecurity workforce development. The results of each evaluation phase contribute to a comprehensive report, supporting iterative improvement and the design of evidence-based curriculum.

4.4 Post-Evaluation Improvements

Following the evaluation, the micro-credential owner conducted an internal review of the assessment findings and implemented targeted improvements. These included refining learning outcomes to ensure full alignment with lesson content, adjusting assessment methods to better reflect Level 7 cognitive demands, and enhancing content accessibility for nontechnical learners. In addition, further examples and applied components were integrated to address the gaps identified in relation to the ECSF role profiles.

5 Career Path Development Methodology

We propose an AI-driven methodology for the development of cybersecurity career pathways, aligning individual learner profiles with the ECSF framework. The approach integrates Curriculum Vitae (CV) analysis, skill extraction, and optimised pathways selection to bridge the gap between personal career goals and industry requirements. Learner CVs serve as structured representations of an individual's professional background, skills, education, and work experience,

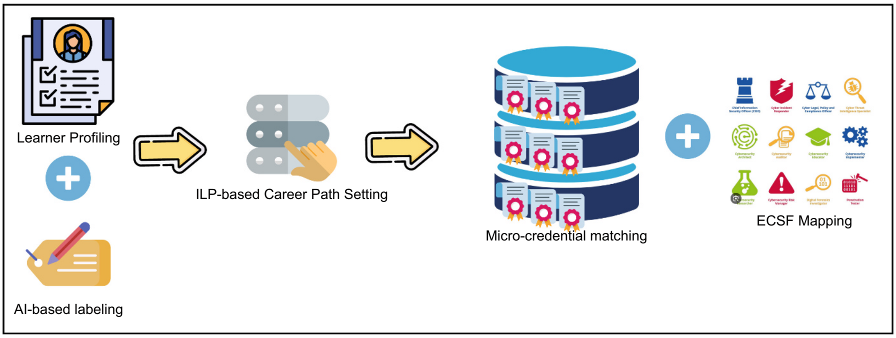
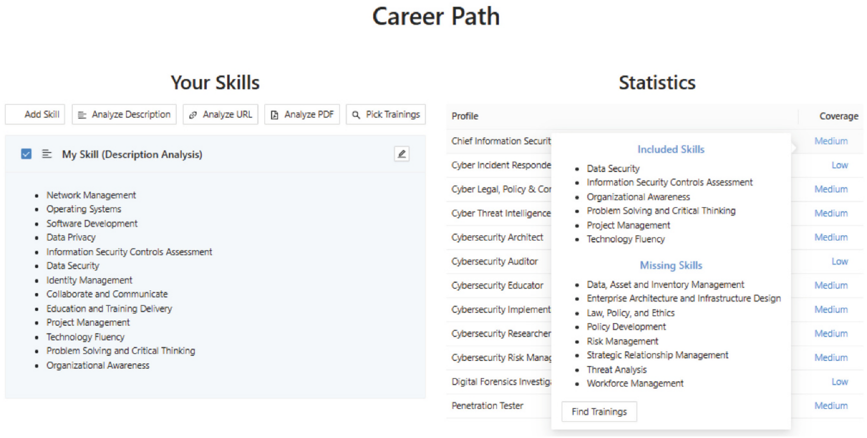

Learner Profiling
AI-based labeling
ILP-based Career Path Setting
Micro-credential matching
Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
Digital Forensics Investigator
Penetration Tester
ECSF Mapping

Fig. 2. Career Path Development Methodology.

offering a personalised snapshot of their current capabilities. In our approach, CVs are processed using an RNN-based algorithm trained on ECSF-aligned job advertisements to extract and classify relevant cybersecurity skill groups. This AI-driven labelling enables the translation of unstructured CV text into standardised ECSF terminology, facilitating accurate skill profile. The labelled data provides a robust foundation for comparing individual competencies with target role requirements, thereby supporting personalised career path optimisation and informed micro-credential recommendations. The proposed methodology is shown in Fig. 2 and consists of the following three steps:

- **Learner Profiling:** The data used for learner profiling and career path analysis were extracted from individual CVs. A CV is typically prepared by the learner and outlines their academic background, work experience, certifications, and acquired skills. These documents serve as key input for career planning and competency assessment. They provide a structured overview of a learner's current qualifications and professional development trajectory, making them suitable for AI-based skill extraction and role matching.
- **AI-based Labelling:** CVs are processed using AI techniques to extract and classify skills and competencies, aligned with the ECSF terminology. This generates structured profiles that reflect each individual's current capabilities and areas for growth. Our application employs an RNN to extract cybersecurity skills from textual input. Sentences are tokenised, converted into integer sequences, and analysed by the RNN to classify relevant skill. The model is trained on a labelled dataset of 937 cybersecurity job advertisements, with ground truths manually annotated. Using the same model for both job ads and micro-credential descriptions offers the following benefits: 1) consistent skill identification across datasets, 2) alignment between job market demands and academic content, 3) dynamic career path updates based on evolving industry trends. Once trained, the model processes each micro-credential description automatically generating associated skill groups.
- **ILP-based Career Path Setting:** An ILP model filters and selects optimal career paths based on ECSF-defined role requirements. The model ensures logical progression and role relevance tailored to the learner's background. The ILP algorithm is configured to match micro-credentials to the selected ECSF profiles, ensuring that all skill groups included in the profile but not yet acquired by the learner are covered by the selected combination of micro-credentials. The user can specify the minimum and maximum number of micro-credentials they are willing to undertake, and the algorithm will return the best possible match based on these constraints.
- **Micro-credential Matching and ECSF Mapping:** Based on the optimised path, the appropriate micro-credentials are matched to the skills gaps of the learner. This step ensures that the recommended learning is coherent, compliant with the ECSF and responsive to the demands of the labour market.

This methodology enables scalable, personalised career planning and better aligns academic training with industry demand in cybersecurity.



☑ My Skill (Description Analysis)

- Network Management
- Operating Systems
- Software Development
- Data Privacy
- Information Security Controls Assessment
- Data Security
- Identity Management
- Collaborate and Communicate
- Education and Training Delivery
- Project Management
- Technology Fluency
- Problem Solving and Critical Thinking
- Organizational Awareness

Profile	Coverage
Chief Information Securit	Medium
Cyber Incident Responde	Low
Cyber Legal, Policy & Cor	Medium
Cyber Threat Intelligence	Medium
Cybersecurity Architect	Medium
Cybersecurity Auditor	Low
Cybersecurity Educator	Medium
Cybersecurity Implement	Medium
Cybersecurity Researcher	Medium
Cybersecurity Risk Manag	Medium
Digital Forensics Investig	Low
Penetration Tester	Medium

Included Skills

- Data Security
- Information Security Controls Assessment
- Organizational Awareness
- Problem Solving and Critical Thinking
- Project Management
- Technology Fluency

Missing Skills

- Data, Asset and Inventory Management
- Enterprise Architecture and Infrastructure Design
- Law, Policy, and Ethics
- Policy Development
- Risk Management
- Strategic Relationship Management
- Threat Analysis
- Workforce Management

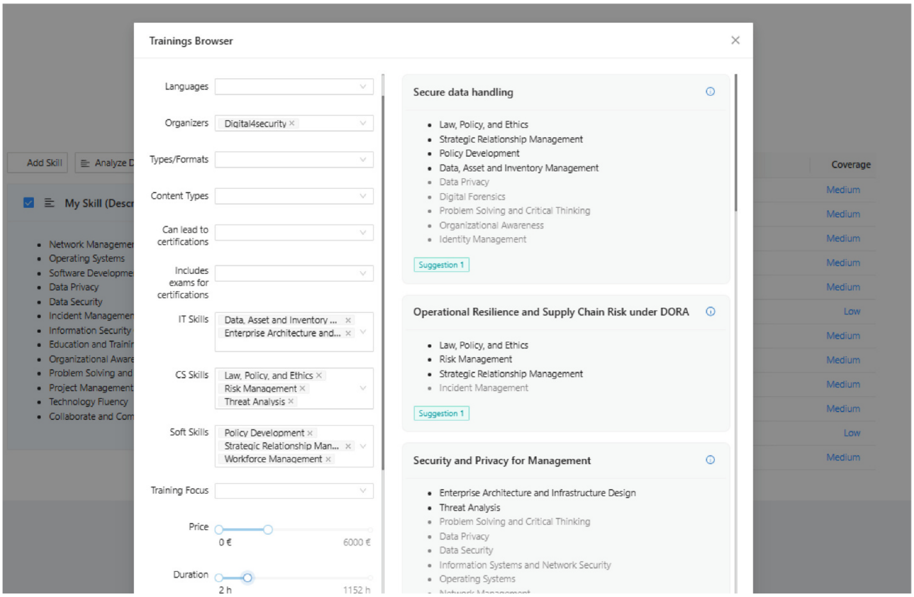
Fig. 3. Cybersecurity Career Path Designer: Learner Profiling and ECSF mapping.

6 Cybersecurity Career Path Designer: Purpose, Targeted Users, and Usability

The Cybersecurity Career Path Designer (CCPD) is an open-source, freely available, dynamic web application that serves as a comprehensive tool for designing and analysing your own professional career path in the cybersecurity domain. The source codes are available on the GitLab repository[1]. Building on the foundation of the REWIRE CyberSecurity Profiler (CSProfiler) [4], it expands its capabilities by allowing dynamic analysis of individuals' skills and knowledge and mapping them into specific ECSF profiles. Users can define their own cybersecurity skills profile in several ways: 1) direct entry, 2) text description analysis (e.g., a short description of their own skills), 3) URL analysis (e.g., a description of the content of a field of study, course, or training), 4) PDF analysis (e.g. a CV), and finally, 5) the option to insert a completed course from a database of available courses. CCPD maps these users' skills to specific cybersecurity roles defined by ECSF profiles, identifies recommended micro-credentials for these roles, and allows users to design their own career path to achieve the desired roles.

The CCPD tool fully integrates the AI-driven cybersecurity career path development concept. The tool is divided into two main sections, see Fig. 3: 1) the left section (Your Skills) allows users to define their own skills and 2) the right section (Statistics) provides the statistical analysis and compliance of the professional profile with ECSF profiles. When users add skills, they can choose from several options, i.e. add a skill, analyse description/URL/ PDF, or simply select an existing course from the available ones. They will have to enter different data depending on the selected option, e.g. name of the skill group or link to

[1] https://gitlab.com/brno-axe/D4Sec/cybersecurity-career-paths.



Trainings Browser

Languages

Organizers: Digital4security ×

Types/Formats

Content Types

Can lead to certifications

Includes exams for certifications

IT Skills: Data, Asset and Inventory ... × Enterprise Architecture and... ×

CS Skills: Law, Policy, and Ethics × Risk Management × Threat Analysis ×

Soft Skills: Policy Development × Strategic Relationship Man... × Workforce Management ×

Training Focus

Price 0 € 6000 €

Duration 2 h 1152 h

Secure data handling

- Law, Policy, and Ethics
- Strategic Relationship Management
- Policy Development
- Data, Asset and Inventory Management
- Data Privacy
- Digital Forensics
- Problem Solving and Critical Thinking
- Organizational Awareness
- Identity Management

Suggestion 1

Operational Resilience and Supply Chain Risk under DORA

- Law, Policy, and Ethics
- Risk Management
- Strategic Relationship Management
- Incident Management

Suggestion 1

Security and Privacy for Management

- Enterprise Architecture and Infrastructure Design
- Threat Analysis
- Problem Solving and Critical Thinking
- Data Privacy
- Data Security
- Information Systems and Network Security
- Operating Systems

Add Skill

Analyze D

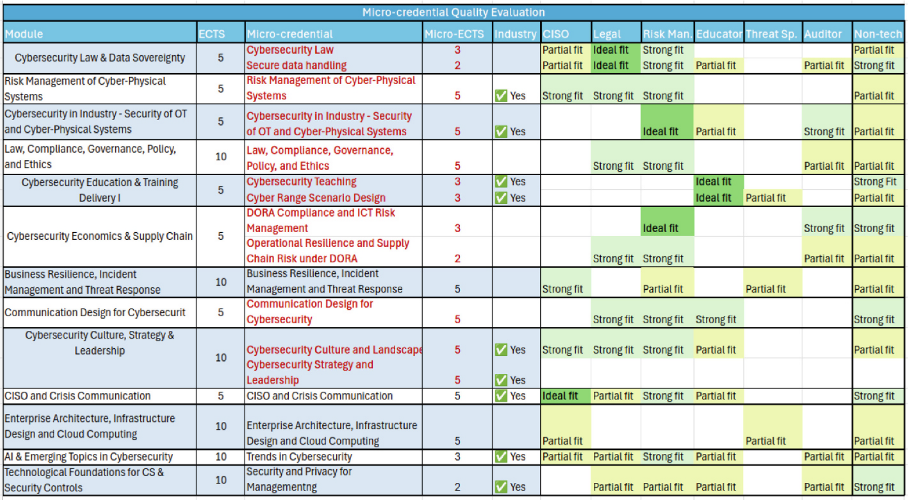
My Skill (Descr

- Network Managemen
- Operating Systems
- Software Developme
- Data Privacy
- Data Security
- Incident Managemen
- Information Security
- Education and Trainin
- Organizational Aware
- Problem Solving and
- Project Management
- Technology Fluency
- Collaborate and Com

Coverage
Medium
Medium
Medium
Medium
Medium
Low
Medium
Medium
Medium
Medium
Low
Medium

Fig. 4. Cybersecurity Career Path Designer: micro-credentials filtering depending on the ECSF selected and learner knowledges.

the data source for analysis. Users can correct the analysis results by adding or removing skills. The corresponding ECSF profiles and their level of compliance with the user's professional profile will then be displayed in the right section. The user then has the option of selecting the ECSF profile that is to be selected. This is where the ILP algorithm plays a key role. The user first clicks on'Find Training' as shown in Fig. 3. Based on the analysis of the skills provided, the algorithm will determine the skill groups to which the micro-credentials relate and, based on the set filter, it will suggest the optimal combination of available micro-credentials; see Fig. 4. Note that filtering allows one to display available courses based on your own preferences such as countries, languages, organisers, types/formats, and content types. If necessary, users can also filter the courses based on the required skills that the courses must contain. Finally, the user can choose the ILP algorithm strategy to ensure that the most suitable combination of micro-credentials is found by setting requirements for 1) total price and 2) duration, 3) displaying the maximum number of proposals, and 4) setting the maximum number of micro-credentials per proposal. After evaluating the user's conditions with the ILP algorithm, the user can then see the recommended combinations of these micro-credentials (i.e., labelled Suggestion 1, Suggestion 2, etc.). Black text fonts of the available skills within the micro-credentials description indicates skills that the user already possesses, while grey text indicates the user's missing skills. It is also worth mentioning that the ILP algorithm can be set to prioritise courses that are close to the user. This is selected using



Micro-credential Quality Evaluation

Module	ECTS	Micro-credential	Micro-ECTS	Industry	CISO	Legal	Risk Man.	Educator	Threat Sp.	Auditor	Non-tech
Cybersecurity Law & Data Sovereignty	5	Cybersecurity Law	3		Partial fit	Ideal fit	Strong fit				Partial fit
		Secure data handling	2		Partial fit	Ideal fit	Strong fit	Partial fit		Partial fit	Strong fit
Risk Management of Cyber-Physical Systems	5	Risk Management of Cyber-Physical Systems	5	✅ Yes	Strong fit	Strong fit	Strong fit				Partial fit
Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	✅ Yes			Ideal fit	Partial fit		Strong fit	Partial fit
Law, Compliance, Governance, Policy, and Ethics	10	Law, Compliance, Governance, Policy, and Ethics	5			Strong fit	Strong fit			Partial fit	Partial fit
Cybersecurity Education & Training Delivery I	5	Cybersecurity Teaching	3	✅ Yes				Ideal fit			Strong Fit
		Cyber Range Scenario Design	3	✅ Yes				Ideal fit	Partial fit		Partial fit
Cybersecurity Economics & Supply Chain	5	DORA Compliance and ICT Risk Management	3				Ideal fit			Strong fit	Strong fit
		Operational Resilience and Supply Chain Risk under DORA	2			Strong fit	Strong fit			Partial fit	Partial fit
Business Resilience, Incident Management and Threat Response	10	Business Resilience, Incident Management and Threat Response	5		Strong fit		Partial fit		Partial fit		Partial fit
Communication Design for Cybersecurit	5	Communication Design for Cybersecurity	5			Strong fit	Strong fit	Strong fit			Strong fit
Cybersecurity Culture, Strategy & Leadership	10	Cybersecurity Culture and Landscape	5	✅ Yes	Strong fit	Strong fit	Strong fit	Partial fit			Partial fit
		Cybersecurity Strategy and Leadership	5	✅ Yes							
CISO and Crisis Communication	5	CISO and Crisis Communication	5	✅ Yes	Ideal fit	Partial fit	Strong fit	Partial fit			Strong fit
Enterprise Architecture, Infrastructure Design and Cloud Computing	10	Enterprise Architecture, Infrastructure Design and Cloud Computing	5		Partial fit				Partial fit		Partial fit
AI & Emerging Topics in Cybersecurity	10	Trends in Cybersecurity	3	✅ Yes	Partial fit	Partial fit	Strong fit	Partial fit		Partial fit	Partial fit
Technological Foundations for CS & Security Controls	10	Security and Privacy for Managementng	2	✅ Yes		Partial fit	Partial fit	Partial fit		Partial fit	Strong fit

Fig. 5. Quality Evaluation of proposed micro-credentials with respective moudules.

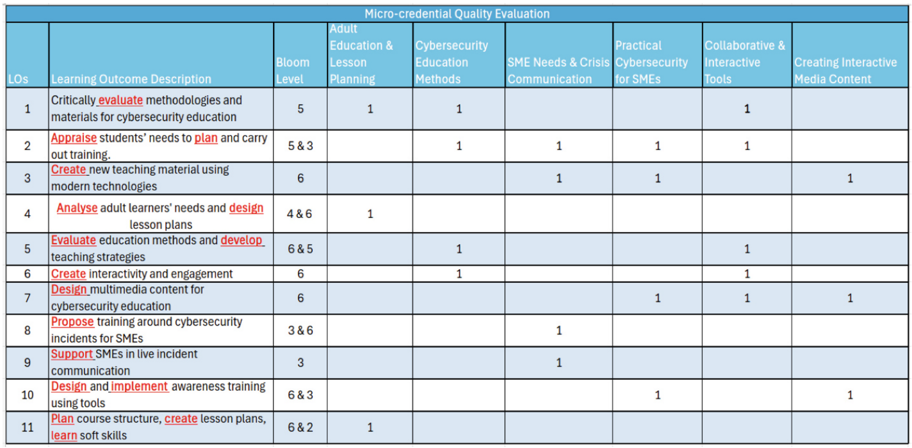
the'Training Focus', where the user selects which of the IT, cybersecurity, and soft skills areas is closest to him/her.

7 Case Study

In this section, we apply both the proposed micro-credential design and career path methodologies to the Digital4Security case study. Specifically, Sect. 7.1 presents the micro-credential design process, following the methodology described in Sect. 4, whereas Sect. 7.2 illustrates a career path design using the Cybersecurity Career Path Designer tool described in Sect. 6.

7.1 Micro-credential Design and Quality Evaluation

Following the skills needs analysis and the proposed methodology, 17 micro-credentials have been designed. Figure 5 presents a summary of the quality evaluation conducted on 17 proposed micro-credentials across 13 master's level modules. The figure displays the module titles with their corresponding ECTS credits, the aligned micro-credentials with assigned ECTS, and the degree of alignment with relevant ECSF role profiles (specified as either ideal, strong, or partial fit). Additionally, it indicates whether each micro-credential is designed for a non-technical audience. It is important to note that the table does not capture the full scope of the evaluation; a more detailed example of the assessment process is provided below for the "Cybersecurity teaching" micro-credential. Specifically, following the seven methodological steps outlined in Sect. 4:



Micro-credential Quality Evaluation								
LOs	Learning Outcome Description	Bloom Level	Adult Education & Lesson Planning	Cybersecurity Education Methods	SME Needs & Crisis Communication	Practical Cybersecurity for SMEs	Collaborative & Interactive Tools	Creating Interactive Media Content
1	Critically evaluate methodologies and materials for cybersecurity education	5	1	1			1	
2	Appraise students' needs to plan and carry out training.	5 & 3		1	1	1	1	
3	Create new teaching material using modern technologies	6			1	1		1
4	Analyse adult learners' needs and design lesson plans	4 & 6	1					
5	Evaluate education methods and develop teaching strategies	6 & 5		1			1	
6	Create interactivity and engagement	6		1			1	
7	Design multimedia content for cybersecurity education	6				1	1	1
8	Propose training around cybersecurity incidents for SMEs	3 & 6			1			
9	Support SMEs in live incident communication	3			1			
10	Design and implement awareness training using tools	6 & 3				1		1
11	Plan course structure, create lesson plans, learn soft skills	6 & 2	1					

Fig. 6. Bloom's level classification table for each Learning Outcome.

1. **Alignment of Learning Outcomes with Lesson Content:** Lessons were marked with a '1' where alignment was evident or empty where it was lacking, as shown in Fig. 6. This process ensured that each LO was addressed appropriately, with gaps and redundancies noted for revision.
2. **Application of Bloom's Taxonomy at Master's Level:** The action verbs within the LOs were analysed and classified according to Bloom's Taxonomy. The learning outcomes align strongly with Bloom's taxonomy, especially in the higher-order cognitive domains of Analyse, Evaluate, and Create.
3. **Assessment of Content Accessibility for a Non-Technical but Digitally Aware Learner:** Thematic analysis of lesson titles such as "Cybersecurity Teaching Methods (Games, Simulations)" and "SME Needs & Crisis Communication" confirmed a conceptual (rather than technical) focus. The use of accessible language and the absence of technical jargon supported the suitability of the content for non-specialist learners.
4. **Relevance of Content to Industry Roles:** A structured mapping was performed to identify roles supported by the micro-credential. Five relevant industry roles were identified: Education & Training, SMEs (Small and Medium Enterprises) Cybersecurity Awareness & Comms, Corporate Learning & Development, Public Sector / NGOs, Technology & Cyber Consulting Firms . These were derived through thematic analysis and cross-referencing with job role databases (e.g., ESCO, LinkedIn).
5. **Mapping to ECSF Role Profiles:** The content was mapped to ENISA's ECSF, confirming directly aligned with the Cybersecurity Educator.
6. **Evaluation of Content Flow, Quality, and Coverage:** The lesson sequence was reviewed to assess the coherence and progression of the topics. The quality of the content was validated by checking for clarity, consistency, and precision.

7. **Identification of Content Gaps Based on ECSF Alignment:** Additional insights were drawn from learner personas and peer programme comparisons, highlighting the need to integrate behaviour change frameworks such as COM-B or Fogg behaviour model to help educators design training that sticks.

7.2 Career Path Design

As a first step, the 17 designed micro-credentials were uploaded to the database using a standardised template containing key parameters (e.g. duration, ECTS, cost). Cybersecurity skills were automatically extracted using the AI-driven algorithm. The tool can be used to analyze ECSF coverage across the 17 designed micro-credentials. The proposed micro-credentials collectively support mainly the ECSF profiles: CISO, Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cybersecurity Educator, Cybersecurity Risk Manager, and Digital Forensic Investigator.

Figure 3 shows an example were a technical CV was uploaded and analysed. The user's extracted skills are shown on the left, while the right panel displays owned and missing skills for each ECSF profile, along with an overall coverage assessment (low, medium, high). This functionality helps learners identify the profiles that best align with their background. Based on this, the system recommends suitable courses as shown Fig. 4. In addition, the tool can offer strategic guidance for users with no previous cybersecurity experience by generating career pathways. For instance, we requested tailored pathways for three ECSF profiles, each limited to a maximum of four micro-credentials:

- **CISO Pathway:** Secure Data Handling + Cybersecurity Strategy and Leadership + Security and Privacy for Management;
- **Cyber Legal, Policy & Compliance Officer Pathway:** Cybersecurity Law + Cybersecurity in Industry;
- **Cybersecurity Educator Pathway:** Cybersecurity Teaching + Cybersecurity Culture and Landscape + Enterprise Architecture, Infrastructure Design and Cloud Computing.

8 Conclusions

This article presents a novel, good-practice methodology for the design of micro-credentials and an AI-driven solution for career path planning, leveraging the ECSF to align education with current market needs in cybersecurity. The proposed methodology ensures that micro-credentials not only address relevant ECSF skill groups but are also accessible to a wide range of learners, including nontechnical yet digitally literate individuals. In the AI-driven career path planning approach, learner CVs serve as input data for profiling, enabling targeted upskilling by identifying existing competencies and recommending optimal learning pathways based on ECSF role requirements and individual goals.

The application of this methodology in the Digital4Security case study demonstrates its feasibility and potential impact. Seventeen ECSF-aligned micro-credentials were developed and assessed, collectively covering a broad spectrum of cybersecurity roles. The system further supports strategic guidance for users with limited cybersecurity experience, providing coherent, ECSF-aligned learning pathways tailored to specific professional profiles.

Acknowledgements. This work was supported by the project DIGITAL4Security: A European Masters Programme in Cybersecurity Management & Data Sovereignty (URL: https://digital4security.eu), funded by the European Commission under the DIGITAL programme (call: DIGITAL-2022-SKILLS-03-SPECIALISED-EDU, grant no. 101123430, Feb 2024âĂŞJan 2028), and by the Ministry of the Interior of the Czech Republic under grant VJ03030003, within the IMPAKT 1 programme.

References

1. Ahsan, K., Akbar, S., Kam, B., Abdulrahman, M.D.A.: Implementation of micro-credentials in higher education: a systematic literature review. Educ. Inf. Technol. **28**(10), 13505–13540 (2023)
2. Berg, S., et al.: Ilastik: interactive machine learning for (bio) image analysis. Nat. Methods **16**(12), 1226–1232 (2019)
3. Dzurenda, P., Ricci, S.: R3.4.1 mapping the framework to existing courses and schemes (2022). https://rewireproject.eu/deliverables/
4. Dzurenda, P., Ricci, S., Sikora, M., Stejskal, M., Lendák, I., Adao, P.: Enhancing cybersecurity curriculum development: AI-driven mapping and optimization techniques. In: ARES'24: 19th International Conference on Availability. Reliability and Security, pp. 1–10. ACM, Vienna (2024)
5. Eibl, G., Jungbauer, C., Litvyak, O., Volkl, P., Luidold, C.: Proactive curriculum for cyber security education: a model of micro-credentials and active blended learning. In: CEEeGov '24: Central and Eastern European EDem and EGov Days 2024, pp. 234– 239. ACM, Budapest (2024)
6. ENISA: European cybersecurity skills framework role profiles (2022). https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
7. ENISA: Communication on the cybersecurity skills academy (2023). https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy
8. Grm, S.P., Bjørnåvold, J., Rusu, A.: Analysis and overview of NQF level descriptors in European countries. cedefop research paper. no 66. Cedefop-European Centre for the Development of Vocational Training (2018)
9. Grumbinait?, I., Colus, F., Carvajal, H.B.: Report on the outcomes and transformational potential of the European Universities initiative. Report ISBN 978-92-68-20047-6, European Commission, Directorate-General for Education, Youth, Sport and Culture, Luxembourg (2025). available at: https://www.vleva.eu/storage/1337/Report-European-Universities-Initiative.pdf (Accessed: 7/May/25)
10. ICS2: Cybersecurity workforce study (2024). https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

11. Kerver, B., Riksen, D.: Whitepaper on open badges and micro-credentials. whitepaper, SURFnet, Utrecht (2016). available at: https://www.surf.nl/files/2019-06/Whitepaper-on-open-badges-en-micro-credentials.pdf. Accessed 7 May 25
12. Lam, B.H., Tsui, K.T.: Curriculum mapping as deliberation-examining the alignment of subject learning outcomes and course curricula. Stud. High. Educ. **41**(8), 1371–1388 (2016)
13. Nurse, J.R., Adamos, K., Grammatopoulos, A., Di Franco, F.: Addressing the eu cybersecurity skills shortage and gap through higher education. European Union Agency for Cybersecurity (ENISA) Report (2021)
14. Papadimitriou, C.H., Steiglitz, K.: Combinatorial optimization: algorithms and complexity. Courier Corporation (1998)
15. Pipikaite, A., Bueermann, G., Joshi, A., Jurgens, J.: Global cybersecurity outlook 2022. In: Geneva: World Economic Forum (2022)
16. Publications Office of the European Union: Proposal for a COUNCIL RECOMMENDATION on a European approach to micro-credentials for lifelong learning and employability. EUR-Lex **Document SWD(2021) 367 final**(COM(2021) 770 final), pp. 1–21 (2021), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0770 (Accessed: 7/May/25)
17. Publications Office of the European Union: COUNCIL RECOMMENDATION of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability. EUR-Lex **Document 32022H0627(02)**(2022/C 243/02), 1–16 (2022). available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_243_R_0002. Accessed 7 May 25
18. Quality and Qualifications Ireland: A Brief Guide to the Irish National Framework of Qualifications (NFQ). Report Version 1.0, QQI, Ireland (2024). available at: https://www.qqi.ie/sites/default/files/2024-08/a-brief-guide-to-the-irish-national-framework-of-qualifications-nfq.pdf. Accessed 7 May 25
19. Somers, C.: D2.1 market needs analysis (2024). https://www.digital4security.eu/project-resources/
20. Somers, C., et al.: Systematic needs analysis of advanced digital skills for postgraduate computing education: the digital4business case. In: AIED 2024. CCIS, vol. 2150, pp. 179–191. Springer, Recife (2024)
21. Varadarajan, S., Koh, J.H.L., Daniel, B.K.: A systematic review of the opportunities and challenges of micro-credentials for multiple stakeholders: learners, employers, higher education institutions and government. Int. J. Educ. Technol. High. Educ. **20**(1), 13 (2023)
22. Werquin, P.: Case study France: Microcredentials for labour market education and training. First look at mapping microcredentials in European labour-market-related education, training and learning: take-up, characteristics and functions. Report, CEDEFOP, Thessaloniki (2023). available at: https://www.cedefop.europa.eu/files/france_microcredentials_mapping.pdf. Accessed 7 May 25
23. Wetzel, K.: Nice Framework Competencies: Assessing Learners for Cybersecurity Work. Tech. rep, National Institute of Standards and Technology (2021)