Project No. 101083594 Project start: 2022-12-01

Call: DIGITAL-2021-SKILLS-01 Project duration: 39 months

CyberSecPro

# D4.4

# Reports and Training Material on the Emerging Technologies Modules

| **Document Identification** | |
|---|---|
| Due date | 2026-02-28 |
| Submission date | 2026-02-27 |
| Version | 1.0 |

| | | | |
|---|---|---|---|
| Related WP | WP4 | Dissemination Level | PU |
| Lead Participant | PDMFC | Lead Author | Luis Miguel Campos |
| Contributing Participants | UNSPMF, SINTEF, GUF , UMA | Related Deliverables | D2.2, D.2.3, D3.1, D3.3, D3.4, D3.5, D.4.1, D5.1, D5.2, D5.3 |

**Abstract:** This deliverable reports on the implementation of training modules on emerging technologies developed within the CyberSecPro (CSP) project under Task T4.5 about "*Operating the training modules on emerging technologies*". It provides a consolidated overview of CSP modules implementation addressing cybersecurity in emerging digital technologies, critical infrastructure security, and software security. The document provides quantitative data on hosting sites, learner enrolment, backgrounds, learners and trainer evaluations, income, scholarships, training levels, delivery methods, and sector coverage in energy, health, maritime, and cybersecurity fields. It offers a comprehensive overview of training program metrics and sectoral focus areas.

The deliverable includes an initial descriptive analysis of training deployment, illustrating implementation patterns and participation across different module categories and sectors. Overall, the document serves as evidence of the effective deployment and reach of the CyberSecPro training programme on emerging technologies and supports the assessment of progress toward the project's capacity-building and skills development objectives.

**Co-funded by the European Union**

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594. 

## Executive Summary

This deliverable presents the results of Task T4.5 about "*Operating the training modules on emerging technologies*" of the CyberSecPro (CSP) project, focusing on the implementation of training modules addressing cybersecurity aspects of emerging digital technologies. The document reports on the delivery of CSP007 (Cybersecurity in Emerging Technologies), CSP008 (Critical Infrastructure Security), and CSP009 (Software Security) modules, providing an evidence-based overview of training activities carried out during the reporting period.

A total of 39 training modules were implemented across multiple sectors, including energy, health, maritime, and general cybersecurity, and delivered at both Basic and Advanced levels. The modules were offered through different formats, such as seminars, workshops, courses, and hackathons, and involved a wide range of academic, research, and industrial providers. Participation data indicate strong engagement across all module categories, with particularly high enrolment in cross-sectoral and seminar-based trainings.

The deliverable includes an initial quantitative analysis of the implemented modules, presenting distributions by module code, training level, module type, and industry sector, as well as corresponding learners enrolments. The analysis highlights balanced coverage across training levels, differentiated sectoral focus depending on module code, and broad outreach to diverse learner groups.

Overall, this deliverable demonstrates the successful implementation and deployment of CyberSecPro training modules on emerging technologies, contributing to the project's objectives of strengthening cybersecurity skills, enhancing sectoral readiness, and supporting the development of a skilled cybersecurity workforce across critical domains.

# Document information

## Contributors

| Name | Beneficiary |
|---|---|
| Luis Miguel Campos | PDMFC |
| Danijela Boberić Krstićev | UNSPMF |
| Nektaria Kaloudi | SINTEF |
| Atiyeh Sadeghi | GUF |
| Cristina Alcaraz | UMA |

## Reviewers

| Name | Beneficiary |
|---|---|
| Cristina Alcaraz, Javier Lopez | UMA |
| Ricardo Lugo | TALTECH |
| Thorsten Kliewe, Jeldo Meppen | ACEEU |

## History

| Version | Date | Contributor(s) | Comment(s) |
|---|---|---|---|
| 0.1 | 2025-11-02 | Luis Miguel Campos, Atiyeh Sadeghi | 1st Draft of ToC |
| 0.2 | 2026-01-09 | Danijela Boberić Krstićev | Initial version of deliverable |
| 0.3 | 2026-01-20 | Danijela Boberić Krstićev | Improvements after high level review |
| 0.4 | 2026-02-10 | Danijela Boberić Krstićev , Nektaria Kaloudi | Improvement based on the first review comments |
| 0.5 | 2026-02-17 | Danijela Boberić Krstićev | Improvement based on the second review comments |
| 0.6 | 2026-02-26 | Danijela Boberić Krstićev | Improvement based on final high level review |
| 1.0 | 2026-02-26 | Atiyeh Sadeghi | Final check, preparation and submission process |

# Table of Contents

# List of Figures



# List of Tables

# List of Acronyms

| | | |
|---|---|---|
| *A* | **A** | Advanced |
| | **ACEEU** | ACEEU GmbH |
| | **AIT** | AIT Austrian Institute of Technology GmbH |
| | **APIRO** | ApiroPlus Solutions Ltd |
| *B* | **B** | Basic |
| *C* | **C** | Course |
| | **C2B** | C2B Consulting |
| | **CISO** | Chief Information Security Officer |
| | **CNR** | Consiglio Nazionale Delle Ricerche (National Research Council) |
| | **CoA** | Certificate of Attendance |
| | **COFAC** | COFAC Cooperativa de Formacao e Animacao Cultural CRl |
| | **CS-E** | Cybersecurity exercise |
| | **CSP** | CyberSecPro |
| *D* | **D** | Deliverable |
| | **DAST** | Dynamic application security testing |
| | **DCM** | Dynamic Curriculum Management |
| *E* | **ECSF** | European Cybersecurity Skills Framework |
| | **EC** | European Comision |
| | **FCT** | Universidade NOVA de Lisboa (NOVA University of Lisbon) |
| *F* | **FTPS** | File Transfer Protocol Secure |
| | **FP** | Focal Point |
| *G* | **GUF** | Johann Wolfgang Goethe-Universitaet Frankfurt am Main (Goethe University Frankfurt) |
| *H* | **H** | Hackathon |
| | **HEIs** | Higher Education Institutions |
| *I* | **ITML** | Information Technology for Market Leadership |
| | **IMT** | Institute Mines-Telecom |

| | | |
|---|---|---|
| | **IT** | Information technology |
| *K* | **KA** | Knowledge Area |
| *L* | **LAU** | Laurea-Ammattikorkeakoulu Oy (Laurea University of Applied Sciences) |
| *M* | **MAG** | Maggioli Spa |
| | **MOOC** | Massive Open Online Course |
| *O* | **O** | Other |
| | **OT** | Operational technology |
| *P* | **PDMFC** | Projecto Desenvolvimento Manutencao Formacao e Consultadorialda |
| *S* | **S** | Seminar |
| | **SAST** | Static application security testing |
| | **SEA** | Social Engineering Academy |
| | **SFTP** | Secure File Transfer Protocol |
| | **SGI** | Serious Games Interactive ApS |
| | **SINTEF** | Sintef AS [SINTEF is not an acronym anymore, so the full name is SINTEF Aksjeselskap] |
| | **SLC** | Security Labs Consulting Limited |
| | **SS** | Summer School |
| | **SVN** | Subversion |
| | **T** | Task |
| | **TalTech** | Tallinna Tehnikaülikool (Tallinn University of Technology) |
| *T* | **TRUSTILIO** | trustilio B.V. |
| | **TUBS** | Technische Universität Braunschweig (Technical University of Braunschweig) |
| | **TUC** | Polytechneio Kritis (Technical University of Crete) |
| | **UCY** | University of Cyprus |
| | **UMA** | Universidad de Malaga (University of Malaga) |
| *U* | **UNINOVA** | Uninova-Instituto de Desenvolvimento de Novas Tecnologiasassociacao (UNINOVA - Institute for the Development of New Technologies) |
| | **UNSPMF** | University of Novi Sad Faculty of Sciences |

| | | |
|---|---|---|
| | **UPRC** | University of Piraeus Research Center |
| *V* | **VPN** | Virtual Private Network |
| | **W** | Workshop |
| *W* | | |
| | **WP** | Work Package |
| *Z* | **ZELUS** | Zelus IKE |

# Glossary of Terms

**C**

**Course**

A course is a set of classes or a plan of study on a particular subject, usually leading to an exam or qualification.

**Cybersecurity Exercise**

A cybersecurity exercise is a structured, simulated activity—ranging from tabletop discussions to live-fire technical drills—designed to test an organization's incident response plans, identify security gaps, and train teams on handling cyber threats like ransomware or phishing. These exercises enhance resilience, improve communication, and validate security procedures in a low-risk environment.

**H**

**Hackathon**

A Hackathon is an event at which a lot of people come together to write or improve computer programs

**S**

**Seminar**

A seminar is a formal, lecture-based event for knowledge sharing, focusing on presenting concepts and discussions with some Q&A.

**SS**

**Summer Schools**

an educational course that happens during the summer.

**W**

**Workshop**

A workshop is an interactive, hands-on session focused on practical skill development and active participation through activities and group work, often with a teacher-like facilitator guiding the doing. Seminars aim to build awareness or understanding, whereas workshops aim to build competence and application of skills.

# Terminology points

- There is a discrepancy between the terms "**students**" and "**learners**" as we followed the KPI terminology used in the call for proposals as well as terminology previously applied in the D4.1 template as it was in the first stage. In this context, however, we refer to the term "**learners**."
- There is a discrepancy between the term's "**participants**" and "**learners**," as we followed the terminology used in KPI tab in the EC SYGMA portal as well as follow-up Questionnaire terminology shared by EC regarding SO4 Indicator 3. However, in this context, we refer to "**learners**".
- "**Trainees**" is the original terminology used in the Grant Agreement, but it turned out that the rest of the project adopted the term "**learners**"

# 1 Introduction

The rapid evolution of emerging technologies is fundamentally reshaping the cybersecurity landscape, introducing both growing opportunities and complex security challenges. Within the CyberSecPro (CSP) project, dedicated training modules have been developed to address the security implications of these technologies, ensuring that professionals are equipped with the knowledge and skills required to identify, assess, and mitigate emerging cyber threats in determined application domains. This deliverable, therefore, reports on the implementation of the mentioned training modules, all of them focused on emerging technologies developed within the CyberSecPro project. It provides a consolidated overview of the delivered trainings, including the number of implemented modules, participation statistics, and sectoral distribution of the modules. The report aims to document the extent of training deployment and its reach across targeted sectors, thereby supporting the assessment of the project's progress toward its capacity-building and skills development objectives.

## 1.1 Purpose and Scope

The purpose of this deliverable is to document and report on the implementation of training modules on emerging technologies carried out under Task T4.5 of Work Package (WP) 4 within the CyberSecPro project. In alignment with the project Key Performance Indicators (KPIs), Task 4.5 aims to deliver 10 general and sector-specific training modules, offered at two proficiency levels (basic and advanced), and implemented by at least three EU higher-education institutions and two companies, in accordance with the plan defined in Deliverable D4.1.

Through the reporting of implemented CSP modules, this deliverable directly supports several WP4 objectives, including:

- the execution of scalable CyberSecPro training offerings,
- the engagement and training of external participants from diverse industries and sectors,
- the provision of training modules aligned with the CyberSecPro capability areas, in particular Cybersecurity in Emerging Digital Technologies,
- the collection of qualitative feedback from training providers to support continuous improvement.

The scope of this document is limited to the reporting and initial analysis of implemented training activities. It includes a structured overview of all delivered modules, quantitative data on the number of implemented modules and learners enrolments, and an initial descriptive analysis of training deployment by module code, training level, module type, industry sector and other criteria.

This deliverable does not aim to assess learning outcomes or training impact in detail, but rather to support monitoring of training execution and progress toward the project's capacity-building and skills development objectives. The reported results contribute to the overall evaluation framework of the CyberSecPro project and provide input for subsequent project activities and deliverables.

## 1.2 Relation to other Work Packages and Deliverables

This deliverable is developed within WP4 of the CyberSecPro project, which focuses on the planning, delivery, and monitoring of scalable cybersecurity training activities. WP4 aims to ensure the structured rollout of CyberSecPro modules, engagement of a critical mass of trainees, broad sectoral outreach, and continuous feedback collection to support the quality and relevance of the training programme.

WP4 builds upon content-oriented inputs from WP2, including defined knowledge areas and capability frameworks, and syllabus-oriented inputs from WP3, which provided guidance on training structure, learning objectives, and module design.

During the project implementation, WP4 interacted closely with other work packages. It received content-oriented information from WP2 and syllabus-related inputs from WP3. In turn, WP4 provided feedback and implementation-level information to WP5, including structured descriptions of implemented CyberSecPro modules.

This deliverable, *D4.4 – Reports and training material on the emerging technologies modules*, is closely related to several other project deliverables. Deliverables D2.2 (covering CSP Training Supply) and D2.3 (covering CSP Knowledge Areas) define the conceptual framework and knowledge foundations of the CSP training programme. Deliverables D3.1, together with D3.3, D3.4, and D3.5, provide the syllabus structure and detailed syllabus specifications for both general and sector-specific CSP training modules. In addition, D4.1 outlines the originally planned supply of modules across the defined CSP Knowledge Areas, forming the basis for the implementation reported in this deliverable. Furthermore, the data collected on the implementation of the training modules contributes to D5.1, which defines the project's evaluation and benchmarking methodology, to D5.2, which reports the consolidated evaluation analysis, and to D5.3 dealing with certification schemes. The information provided in this deliverable will support the identification and documentation of best practices in teaching cybersecurity.

## 1.3 Structure of the Deliverable

This deliverable is structured as follows.

Section 0 introduces the context of the CyberSecPro training activities on emerging technologies, outlines the purpose and scope of the deliverable, and describes its relation to other work packages and deliverables.

Section 2 presents an overview of the methodology applied to develop the template for documenting the implemented CSP modules and to automate the process of collecting and curating data on the implemented modules.

Section 3 provides an overview of the implemented CSP modules under Task T4.5, including key information such as module codes and titles, implementation periods, training levels, providers, sectoral focus, and the number of participating learners.

Section 4 provides an overview of the structure and outcomes of the implemented CSP modules, including initial implementation statistics as well as a summary of the managerial and logistical aspects of the modules.

Section 5 presents the MOOC relevant to the addressed knowledge areas, including its general description and syllabus.

Finally, Section 6 concludes the deliverable by summarizing the main findings and outlining their relevance to the objectives of the CyberSecPro project.

Annex A: Template for the Documentation of Implemented CSP Modules elaborates on the template utilized for documenting implemented CSP Modules. Annex B: Template for Planning the Offering of CSP Modules contains the template for offering CSP modules as provided in D3.1. Annex C: Reporting Method(s) introduces the reason of using Admin portal[1] as a method for documenting implemented CSP Modules. And lastly, Annex D provide all the templates used in the process of evaluation of implemented modules by trainees and trainers.

[1] https://admin.cybersecpro-project.eu/

# 2 Methodology

This section presents the approach used to document the implemented CSP modules, including the types of information recorded and the reporting procedures applied.

## 2.1 Data Collection Procedure

The template for documenting the implemented CSP modules was developed through a structured and iterative process to ensure methodological consistency and alignment with the relevant work package and task descriptions, as well as with European Commission requirements and reviewer feedback following the first periodic report.

The initial version of the template was based on the existing template for describing CSP modules presented in Deliverable D4.1, ensuring continuity with earlier project outputs while extending its scope to include implementation-specific aspects. Additional elements were incorporated to enable comprehensive documentation of implementation content, management and logistics, outcomes, financial aspects, and best practices that were not fully covered in the original template, in accordance with the relevant work package and task descriptions.

To ensure conceptual coherence across work packages and facilitate comparability between planned training activities and their actual implementation, the template was aligned with the training module descriptions defined in Deliverable D3.1.

The finalized template was implemented within the project's Admin portal (see Section 2.2 for further details), enabling structured data entry, centralized documentation, and efficient access to information on the implemented CSP modules.

In line with European Commission requirements, the KPIs specified in the project call were also subsequently integrated into the template. To ensure adequate coverage of these indicators, an additional questionnaire was developed for CSP providers to collect the necessary data from learners (see Annex D: CyberSecPro Evaluation Forms for further details). Reviewer feedback received after the Period 1 was also incorporated into the template.

All data from the implemented CSP modules were exported from the admin portal for analysis and preparation of the deliverable by 20 February 2026.

## 2.2 Data Collection Support by Portal for Reports by Module Implementation Provides

For the purpose of collecting and curating information on the implemented CSP modules, the project's administrative portal (https://admin.cybersecpro-project.eu/) was extended with additional functionalities supporting structured data entry, data management, and centralized storage of implementation-related information (cf. Figure 1). Initially, we planned to document the implemented CSP modules in the DCM system. However, when the documentation needed to start, the DCM was not available (see Annex C: Reporting Method(s) ). At later stage, it was decided to continue using this Admin portal for documenting the implemented CSP modules as it offers greater flexibility for trainers to report their outcomes than the DCM which is primary designed to support teaching actions.

The web-based platform enables CSP providers to submit, update, and manage documentation on implemented modules through standardized forms, ensuring consistency, traceability, and efficient access to the collected data. It also supports the monitoring of module implementation, reporting processes, and the generation of aggregated information required for project evaluation and analysis.

CSP providers are required to complete the template in the administrative portal immediately after the completion of the implementation phase, ensuring timely reporting, data accuracy, and effective monitoring. Providers are also expected to update the completed template whenever modifications or additional elements are introduced.

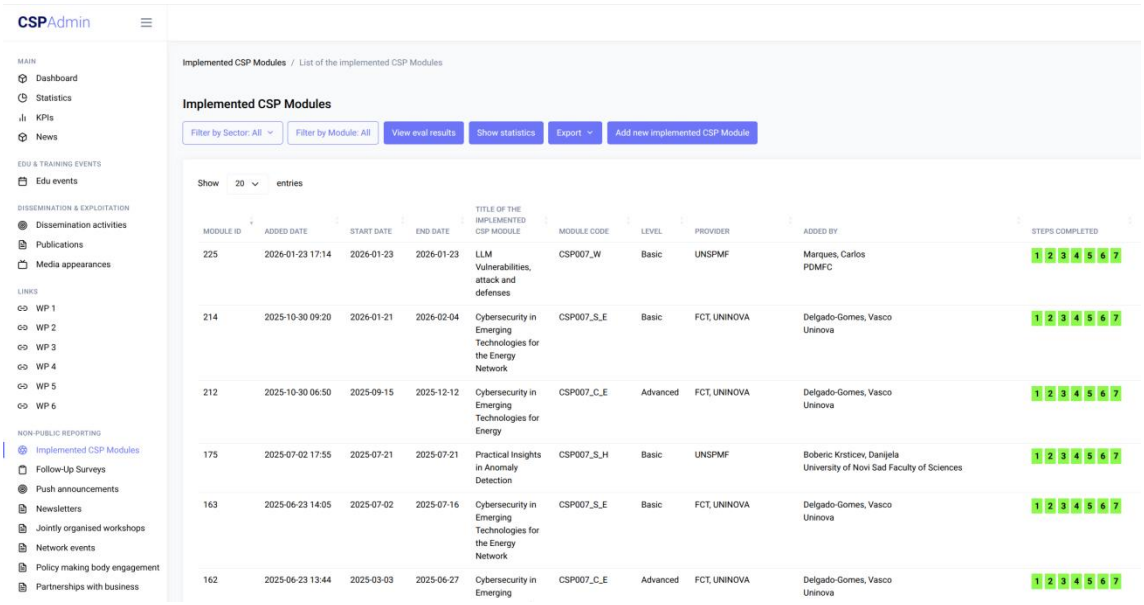


Figure 1: CyberSecPro admin panel

# 3 Implemented CSP Modules under T4.5

This section presents the CSP modules implemented under Task 4.5, providing an overview of their scope, structure, and key implementation characteristics.

## 3.1 CSP Modules on Cybersecurity in Emerging Digital Technologies

In this section, we briefly describe which CSP Modules are related to cybersecurity in emerging digital technologies and therefore to T4.5 titled *Operating the training modules on emerging technologies*. Based on Table 1, derived from deliverable D4.1, this task, T4.5, is responsible for the modules CSP007 Cybersecurity in Emerging Technologies, CSP008 Critical Infrastructure Security and CSP009 Software Security.

Table 1: The interrelation between CSP Knowledge Areas, Capabilities categories and Module(s)*

| CSP Knowledge Area | Capability Category | Module(s) |
|---|---|---|
| CSP Knowledge Area 1 – Cybersecurity Management | Cybersecurity Principles and Management | CSP001 Cybersecurity Essentials and Management |
| CSP Knowledge Area 2 – Human Aspects of Cybersecurity | Cybersecurity Principles and Management | CSP002 Human Factors and Cybersecurity |
| CSP Knowledge Area 3 – Cybersecurity Risk Management | Cybersecurity Tools and Technologies | CSP003 Cybersecurity Risk Management and Governance |
| CSP Knowledge Area 4 – Cybersecurity Policy, Process, and Compliance | Cybersecurity Principles and Management | |
| CSP Knowledge Area 5 – Network and Communication Security | Cybersecurity Tools and Technologies | CSP004 Network Security |
| CSP Knowledge Area 6 – Privacy and Data Protection | Cybersecurity Principles and Management | CSP005 Data Protection and Privacy Technologies |
| CSP Knowledge Area 7 – Cybersecurity Threat Management | Cybersecurity Tools and Technologies | CSP006 Cyber Threat Intelligence |
| CSP Knowledge Area 8 – Cybersecurity Tools and Technologies | Cybersecurity in Emerging Digital Technologies | CSP007 Cybersecurity in Emerging Technologies<br>CSP008 Critical Infrastructure Security<br>CSP009 Software Security |
| CSP Knowledge Area 9 – Penetration Testing | Offensive Cybersecurity Practices | CSP010 Penetration Testing<br>CSP011 Cyber Ranges and Operations |
| CSP Knowledge Area 10 – Cyber Incident Response | Offensive Cybersecurity Practices | CSP011 Cyber Ranges and Operations<br>CSP012 Digital Forensics |

* Cyan colour indicates the KAs covered by T4.5 and in this deliverable, D4.4.

### CSP007 Cybersecurity in Emerging Technologies

CPS007 training modules equip participants with the knowledge and skills needed to address the complex cybersecurity challenges that arise from integrating cutting-edge technologies across various industries. As organizations increasingly adopt innovations such as the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, 5G, and 6G, the need for robust and adaptive security measures becomes essential. The module provides a comprehensive understanding of the cybersecurity landscape within the context of these emerging technologies, combining theoretical insights with practical applications.

It is designed for IT professionals, developers, engineers, business leaders, and compliance or risk management specialists who are directly involved in implementing or overseeing systems based on emerging technologies. Through this module, participants have learnt to recognize cybersecurity risks,

understand the vulnerabilities and unique security characteristics of modern technologies, and apply best practices for protecting applications, data, and infrastructure. The modules also helped participants to identify, assess, and mitigate threats in technology-driven environments while offering hands-on experience with relevant tools, frameworks, and defensive techniques.

**CSP008 Critical Infrastructure Security**

The primary objective of the CSP008 module is to examine the security and resilience of application environments that are critical to society and the economy. It addresses the technical, organizational, social, procedural, and legal dimensions of cybersecurity, maintaining a consistent focus on the protection and continuity of critical infrastructures and their operational systems.

CSP008 training modules are designed for a diverse audience, bringing together professionals and learners from various domains who share a common interest in critical infrastructure security and resilience. It is particularly relevant for IT and OT professionals, administrators, engineers, and operators responsible for managing and securing operational networks and integrated information systems that support essential services. Security experts protecting organizations from sophisticated cyberattacks, such as Advanced Persistent Threats (APTs) and supply chain attacks, can also find the module highly beneficial. In addition, it addresses the needs of CISOs (Chief Information Security Officers) and business leaders seeking to understand the risks and costs of specialized cyberattacks targeting critical domains and applications.

Participants developed awareness of the importance of safeguarding essential infrastructures, gained insights into the sector-specific challenges and vulnerabilities, and became familiar with key national and international standards and frameworks. They also acquired practical skills in risk assessment, mitigation, incident response, recovery, and crisis management, while strengthening communication and collaboration among stakeholders to enhance the overall resilience of critical systems.

**CSP009 Software Security**

This CSP training module provides a comprehensive overview of software security concepts and principles within the context of modern software development. It examines the impact of insecure software on individuals, organizations, and society, as well as the relevant legal and regulatory frameworks governing software security. The module covers secure requirements engineering, threat modelling, and secure system design, integrating security practices throughout the entire software development lifecycle, including agile methodologies.

With CSP009, participants gained practical experience with code reviews, static and dynamic application security testing (SAST/DAST), web and mobile application security testing, and the interpretation and prioritisation of security findings. Participants are introduced to secure coding principles and best practices across multiple programming languages, including C, C++, Java, and Python, with particular emphasis on memory management vulnerabilities, input validation, sanitisation techniques, and the correct use of cryptographic libraries. Through hands-on cyber exercises, participants applied secure coding practices, analyse vulnerable software, develop security architectures and threat models, and conduct practical software security audits, while also exploring emerging trends and challenges in the field of software security.

## 3.2 Overview of Implemented CSP Modules under T4.5

This section provides an overview of the most relevant elements of all implemented CSP modules, organized according to T4.5. Table 2 and further details in Section 4 shows that the T4.5 requirements regarding the implementation of 10 general and sector specific training modules at two different levels in both EU HEIs and companies have been fully met. As shown in Table 2, it reports for each CSP module the module code and title, the implementation period indicated by the start and end dates, the level, the provider, and the corresponding sector. In addition, the number of participating learners is documented.

Table 2: Implemented CSP Modules under T4.5

| Module Code | Title of the implemented CSP module | Start Date | End Date | Level | Provider | Information on the sector | Number of learners |
|---|---|---|---|---|---|---|---|
| CSP008_C_E | Critical Energy Infrastructure Security | 2025-03-03 | 2025-06-27 | A | UNINOVA, FCT | Energy | 30 |
| CSP009_S_H | Secure Healthcare Software Development | 2024-04-19 | 2024-04-19 | B | PDMFC, UPRC | Health | 15 |
| CSP007_S_H | Practical Insights in Anomaly Detection | 2024-05-24 | 2024-05-24 | B | UNSPMF | Health | 7 |
| CSP008_S_H | Cascading Effects in Complex Health Networks | 2024-05-26 | 2024-05-26 | A | AIT | Health | 7 |
| CSP008_S_H | Healthcare sector cyber security | 2024-05-29 | 2024-05-29 | B | SLC, UPRC | Health | 30 |
| CSP009_S_M | Software Security for Maritime | 2024-06-21 | 2024-06-21 | A | TUC, UPRC | Maritime | 10 |
| CSP008_S_E | Protecting Charging Stations Against Specific Threats | 2024-06-22 | 2024-06-22 | A | AIT, UMA | Energy | 17 |
| CSP008_S_E | Introduction to the Cybersecurity in Electric Charging Stations | 2024-06-22 | 2024-06-22 | A | AIT, UMA | Energy | 17 |
| CSP009_S_H | Secure Healthcare Software Development | 2024-06-22 | 2024-06-22 | B | PDMFC | Health | 7 |
| CSP009_W_M | Software Security for Maritime | 2024-07-01 | 2024-07-13 | A | MAG, TUC | Maritime | 46 |
| CSP007_H | Suricata-Wazuh, MrRobot, BlackBox | 2024-07-01 | 2024-07-13 | A | PDMFC | Hackathon | 34 |
| CSP007_H | Setting up, Introduction to Linux, RavenCTF, Network Forensics | 2024-07-01 | 2024-07-13 | B | PDMFC | Hackathon | 34 |
| CSP007_S_E | Cybersecurity in Emerging Technologies for the Energy Network | 2024-07-01 | 2024-07-13 | B | PDMFC | Energy | 34 |
| CSP007_S | Advanced Cybersecurity Stack: Mastering Key Software Tools | 2024-07-01 | 2024-07-13 | A | PDMFC | General | 35 |
| CSP007_S | Cybersecurity Stack: Fundamental Software Tools | 2024-07-01 | 2024-07-13 | B | PDMFC | General | 34 |
| CSP007_S_M | AI and Cybersecurity Research in Maritime | 2024-07-01 | 2024-07-13 | A | SINTEF, PDMFC, UNSPMF | Maritime | 34 |
| CSP009_S_H | Secure Healthcare Software Development | 2024-07-01 | 2024-07-13 | B | PDMFC | Health | 34 |
| CSP009_W_M | Securing Maritime Web Applications | 2024-07-01 | 2024-07-01 | B | FP | Maritime | 25 |
| CSP009_W_H | Securing Healthcare Web Applications | 2024-07-02 | 2024-07-02 | B | FP | Health | 22 |
| CSP009_W_M | Securing Maritime Web Applications | 2024-07-05 | 2024-07-05 | B | FP | Maritime | 25 |
| CSP009_W_H | Securing Healthcare Web Applications | 2024-07-05 | 2024-07-05 | B | FP | Health | 25 |
| CSP007_S | Cybersecurity in Emerging Technologies, in particular explainable AI for Healthcare | 2024-07-12 | 2024-07-12 | A | LAU, UMA, Trustilio | General | 34 |
| CSP009_W | Software Security-OWASP Top 10 | 2024-09-01 | 2024-09-01 | B | FP | General | 13 |
| CSP009_S_E | Mechanics for Memory Corruption | 2024-09-01 | 2024-09-01 | B | UCY, FCT | Energy | 30 |
| CSP008_C_M | Critical infrastructure Security in Maritime | 2024-09-01 | 2024-09-01 | A | C2B, Trustilio, UPRC | Maritime | 6 |
| CSP007_S_E | Cybersecurity in Emerging Technologies for the Energy Network | 2025-07-02 | 2025-07-16 | B | UNINOVA, FCT | Energy | 15 |

Implemented CSP Modules under T4.5

| Module Code | Title of the implemented CSP module | Start Date | End Date | Level | Provider | Information on the sector | Number of learners |
|---|---|---|---|---|---|---|---|
| CSP008_S_M | Cascading Effects in Complex Maritime Networks and Supply Chains | 2024-11-19 | 2024-11-19 | A | AIT | Maritime | 5 |
| CSP007_S | Operating System Security | 2025-01-20 | 2025-01-20 | B | PDMFC | General | 55 |
| CSP007_H | Cybersecurity Fundamentals | 2025-01-25 | 2025-01-25 | A | PDMFC | Hackathon | 55 |
| CSP007_H | Ethical Hacking | 2025-01-25 | 2025-01-25 | A | PDMFC | Hackathon | 55 |
| CSP008_C_E | Protecting Charging Stations Against Specific Threats | 2025-04-07 | 2025-04-08 | A | AIT, UMA, UCY | Energy | 17 |
| CSP007_S_H | Practical Insights in Anomaly Detection | 2025-07-21 | 2025-07-21 | B | UNSPMF | Health | 41 |
| CSP007_C_E | Cybersecurity in Emerging Technologies for Energy | 2025-09-15 | 2025-12-12 | A | UNINOVA, FCT | Energy | 30 |
| CSP008_C_E | Critical Energy Infrastructure Security | 2025-09-15 | 2025-12-12 | A | UNINOVA, FCT | Energy | 25 |
| CSP007_C_E | Cybersecurity in Emerging Technologies for Energy | 2025-03-03 | 2025-06-27 | A | UNINOVA, FCT | Energy | 25 |
| CSP007_S_E | Cybersecurity in Emerging Technologies for the Energy Network | 2026-01-21 | 2026-02-04 | B | UNINOVA, FCT | Energy | 15, |
| CSP007_W | LLM Vulnerabilities, attack and defences | 2026-01-23 | 2026-01-23 | A | UNSPMF | General | 35 |
| CSP009_W | Software Security | 2025-12-06 | 2025-12-07 | A | FP | General | 24 |
| CSP009_W_M | Software Security | 2026-01-12 | 2026-01-12 | B | FP | Maritime | 5 |

# 4 Structure, Implementation, and Outcomes of Implemented CSP Modules

This section provides an overview of the structure and outcomes of the implemented CSP modules. The first subsection (Section 4.1) presents initial statistics on the modules implemented under Task T4.5 thereby offering a comprehensive view of the overall implementation. The second subsection (Section 4.2) summarizes the managerial and logistical aspects of the implemented CSP modules.

## 4.1 Statistics of Implemented CSP Modules

This section shows initial statistics of the implemented CSP modules under T4.5. The following subsections present a quantitative analysis of the implemented CSP modules. The data is structured across multiple dimensions in order to provide a clear and systematic overview of module implementation and participation. Specifically, the analysis covers the distribution of modules by module code, level, type, and sector, as well as combined classifications (e.g., level and code, type and code, sector and code). In addition, the number of enrolled learners is analyzed per module code and sector. The section concludes with an overview of modules implemented within seasonal schools. This structured breakdown enables a detailed understanding of the scope, diversity, and reach of the CSP educational activities. The presented figures are aligned with the CyberSecPro strategy, which aimed to implement at least one module in each knowledge area whenever possible, while the implementation of additional modules was driven by identified market demand.

### 4.1.1 Number of implemented CSP modules per module code

Figure 2 presents the distribution of implemented training modules by CSP module code. As shown, CSP007 accounts for the highest number of implemented modules (17), followed by CSP009 with 13 modules and CSP008 with 9 modules.

The distribution indicates a stronger emphasis on CSP007 modules within the implemented training programme, reflecting their broad applicability and relevance across multiple sectors. CSP008 and CSP009 modules also demonstrate substantial implementation, contributing to a balanced coverage of different cybersecurity topics within the CyberSecPro training framework.

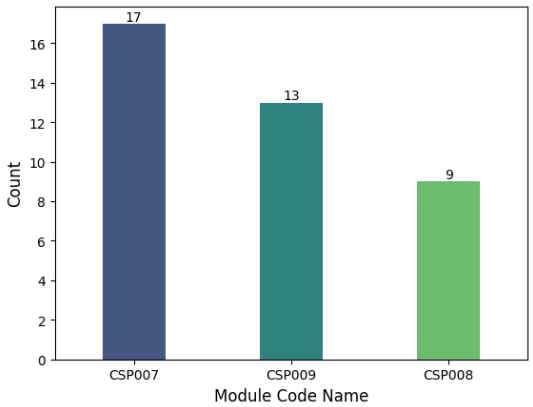


Figure 2: Number of implemented CSP modules per module code

### 4.1.2 Number of learners in implemented CSP modules per module code

Figure 3 illustrates the total number of learners enrolments across implemented CSP modules, grouped by module code. The data show that CSP007 modules attracted the highest number of learners, with a total of 567 learners, followed by CSP009 modules with 281 enrolments, while CSP008 modules recorded 149 learners.

This distribution reflects the strong uptake of CSP007 modules, which may be attributed to their broader thematic scope and applicability across multiple sectors. CSP009 modules

also demonstrate significant learners engagement, whereas CSP008 modules, while fewer in enrolments, contribute to the overall diversity of the training portfolio.

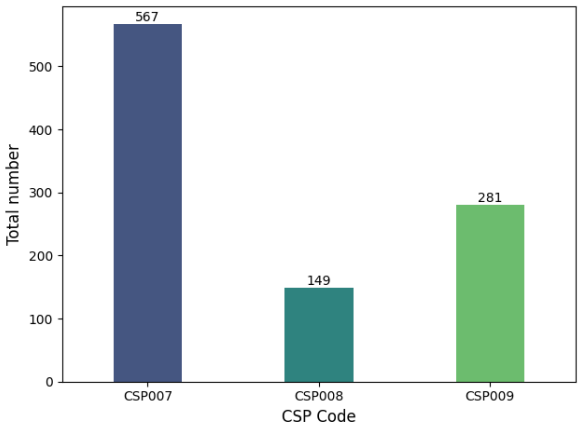


Figure 3: Number of learners in implemented CSP modules per module code

### 4.1.3 Number of implemented CSP modules per module level

Figure 4 presents the distribution of implemented CSP modules by training level. The results show a balanced implementation across levels, with 19 Advanced-level modules and 20 Basic-level modules delivered during the reporting period. This near-equal distribution indicates that the CyberSecPro training programme addresses the needs of learners with different levels of prior knowledge, supporting both foundational skill development and advanced specialization in emerging cybersecurity technologies.

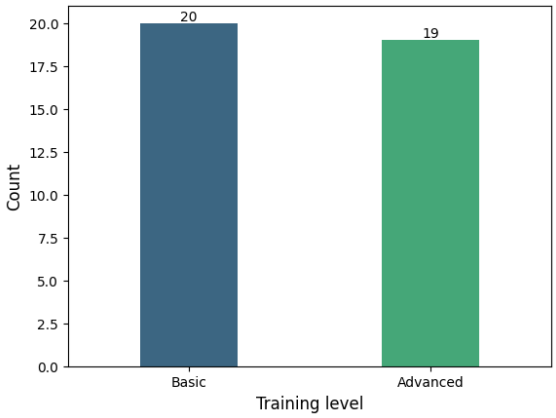


Figure 4: Number of implemented CSP modules per module level

### 4.1.4 Number of implemented CSP modules per module level and code

Figure 5 presents the distribution of implemented CSP modules by both module code and training level. The results show that CSP007 modules are relatively evenly distributed across Basic (9) and Advanced (8) levels, indicating a balanced provision of foundational and advanced training within this module category.

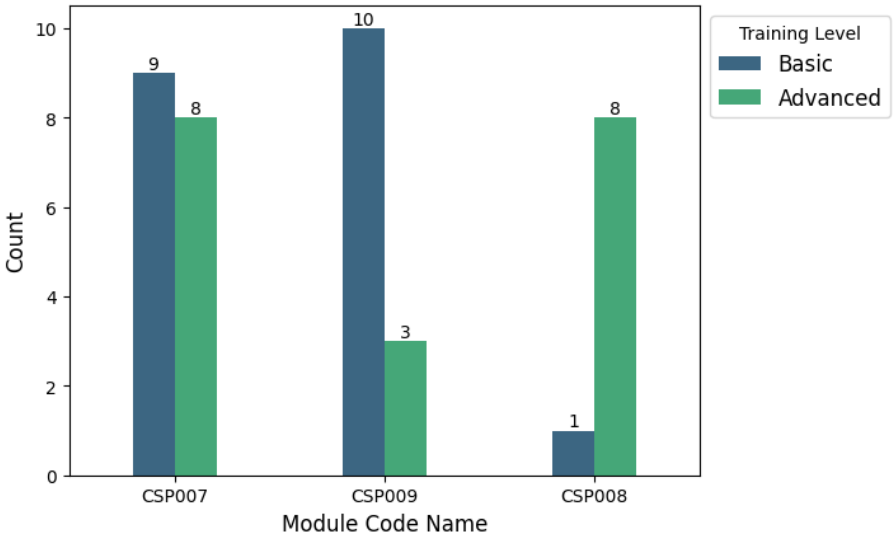


Figure 5: Number of implemented CSP modules per module level and code

In contrast, CSP008 modules are predominantly delivered at the Advanced level, with 8 Advanced modules compared to only 1 Basic module, reflecting a stronger focus on advanced topics within this code. Conversely, CSP009 modules are mainly offered at the Basic level, with 10 Basic modules and 3 Advanced modules, suggesting an emphasis on introductory and intermediate training within this category.

### 4.1.5 Number of implemented CSP modules per module type

Figure 6 presents the distribution of implemented CSP modules by module type. The results indicate that Seminars (S) represent the largest share, with 23 implemented modules, followed by 7 Workshops (W), 5 Courses (C) and, 4 Hackathons (H).

This distribution highlights a strong emphasis on seminar-based training within the CyberSecPro programme, complemented by hands-on formats such as workshops and hackathons. The combination of different module types supports diverse learning approaches, ranging from knowledge-oriented sessions to more practical and experiential training formats.

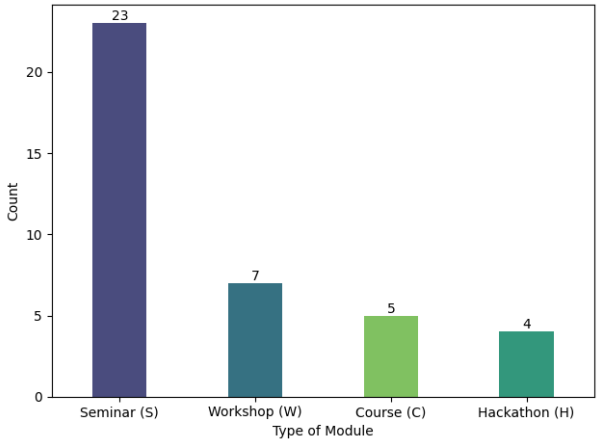


Figure 6: Number of implemented CSP modules per type

### 4.1.6 Number of implemented CSP modules per module type and code

Figure 7 presents the distribution of implemented CSP modules by module type and module code. The results indicate that seminars dominate across all CSP module codes, confirming their central role in the CyberSecPro training programme.

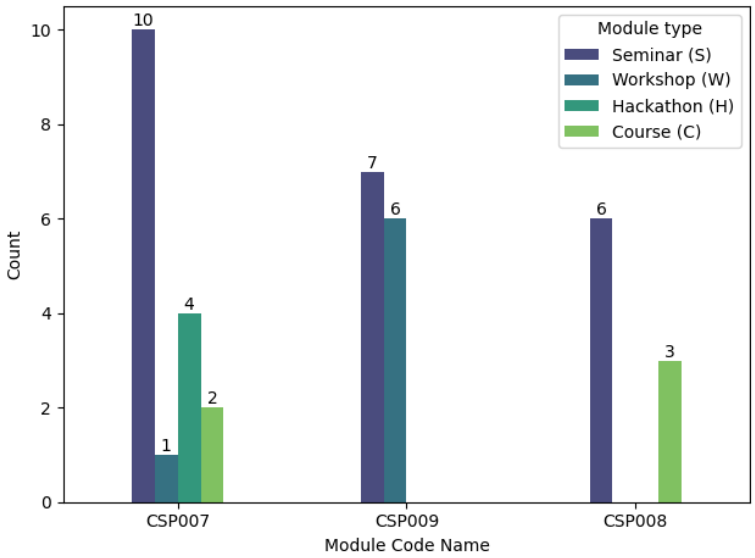


Figure 7: Number of implemented CSP modules per module type and code

For CSP007, seminars represent the largest share (10 modules), followed by hackathons (4) and courses (2), indicating a diverse mix of delivery formats within this module code. In the case of CSP009, seminars (7) and workshops (6) are the most frequently implemented module types, reflecting a balanced combination of theoretical and hands-on training. For CSP008, the implementation is almost exclusively seminar-based (6 modules), with a smaller number of courses (3) and no workshops or hackathons delivered under this code.

Overall, the distribution reinforces earlier findings regarding the prevalence of seminar-based modules while also highlighting variations in module type composition across different CSP codes.

### 4.1.7 Number of implemented CSP modules per module sector

Figure 8 presents the overall distribution of implemented CSP modules across industry sectors, independently of module code. The results show that the energy and health sectors each account for the highest number of implemented modules (11 and 10 modules respectively), followed by the general sector with 10 modules and the maritime sector with 8 modules.

This distribution confirms a strong focus of the CyberSecPro training programme on energy and health, which are critical and highly regulated sectors with significant cybersecurity challenges. At the same time, the presence of general and maritime modules demonstrates balanced sectoral coverage and supports cross-sectoral skill development.

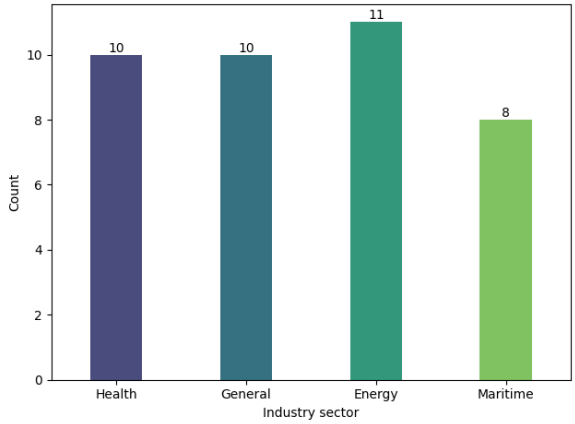


Figure 8: Number of implemented CSP modules per module sector

### 4.1.8 Number of learners in implemented CSP modules per module sector

Figure 9 presents the distribution of learners across CSP modules by industry sector. The results indicate that the general sector accounts for the highest number of enrolments (374), followed by the energy sector (245) and the health sector (222). The maritime sector records a lower, but still significant, number of enrolments (156).

This distribution reflects strong participant engagement in both cross-sectoral and sector-specific training activities. The high enrolment in general-sector modules aligns with their broad applicability, while the substantial participation in energy and health modules highlights the relevance of cybersecurity training in these critical sectors.

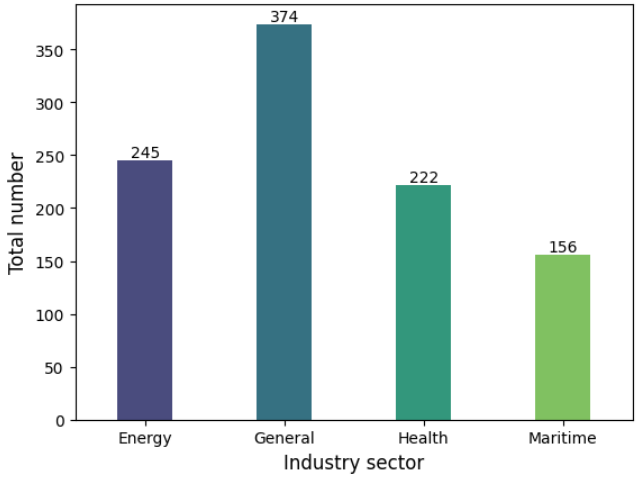


Figure 9: Number of learners in implemented CSP modules per module sector

### 4.1.9 Number of implemented CSP modules per module sector and code

Figure 10 presents the distribution of implemented CSP modules across industry sectors, grouped by module code. The results indicate distinct sectoral emphases for each CSP category.

For CSP009, the majority of implemented modules are concentrated in the health and maritime sector (5 modules), with limited representation in the general and energy sectors. CSP007 shows the broadest sectoral coverage, with a strong presence in general cybersecurity topics (8 modules), followed by the energy sector (5 modules), the health sector (3 modules), and a smaller number of maritime modules (1 module). In contrast, CSP008 modules are predominantly focused on the energy sector (5 modules), with additional implementation in the health (2 modules) and maritime sectors (2 modules), and no general-sector modules recorded under this code.

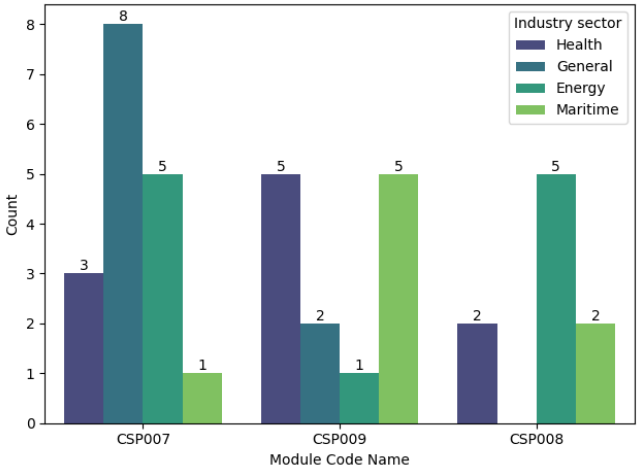


Figure 10: Number of implemented CSP modules per module sector and code

### 4.1.10 Number of implemented CSP modules per seasonal schools

Figure 11 shows that more than half of all modules were delivered through independent events, while the remaining modules were primarily concentrated in seasonal schools, particularly the Summer School 2024 Porto. This indicates that, although seasonal schools play an important role, flexible independent events represented the dominant dissemination channel.

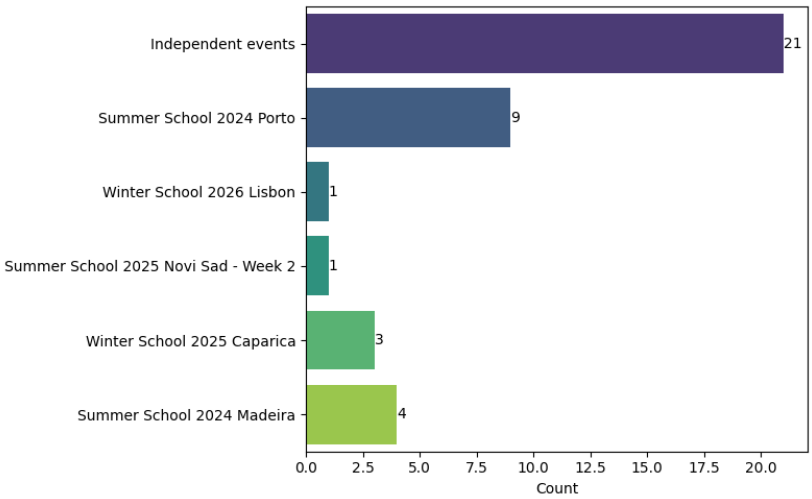


Figure 11: Number of implemented CSP modules per seasonal schools

## 4.2 Management and Logistical Aspects of CSP Implemented CSP Modules

This section presents the management and logistical aspects related to the implementation of the CSP modules, including strategies to attract and rewards learners, financial aspects of implemented modules and other operational considerations.

### 4.2.1 Actions to attract learners

To attract learners to participate in the CSP learning modules, several complementary actions were implemented. The modules were aligned with and integrated into well-established summer and winter schools (e.g. the IPICS Summer School), as well as incorporated into existing academic courses and study programmes, thereby increasing their visibility among students.

Participation was further supported through the identification of national and international funding opportunities, including Erasmus+ schemes, and by assisting trainees in securing financial support for travel and registration fees. Several events were organized with reduced participation fees, supported by sponsorships, while additional outreach efforts were conducted by partner higher-education institutions to promote the modules directly among their students.

Dissemination campaigns highlighted the relevance of the modules to labour-market needs, promoted training opportunities through communication channels and short promotional videos, and encouraged participation from underrepresented groups, particularly women. Furthermore, the availability of online learning through the DCM platform also enabled flexible participation, allowing learners to enrol even in individual courses. Finally, the possibility of earning ECTS credits upon successful completion of assignments further motivated student engagement.

### 4.2.2 Income and scholarship/sponsorships

There was no income generated from the implemented CSP module and seasonal schools. Scholarships and sponsorships were primarily provided for participation in seasonal schools, and further details are presented in table Table 3 below.

CyberSecPro, as the organizer of the seasonal schools did the following things and sometime supported by other sponsors confer in Table 3:

- Advertisement of the event in their lists and members,
- Participation of key personnel as speakers without pay and as attendees in the events,
- Having booths in the registration area,
- Financial support,
- Secretarial support,
- Support (technical, computer etc) during the event,
- Sending learners,
- Offering space and equipment.

Table 3: Scholarshipand sponsorships detail

| Seasonal schools | Sponsorship | Scholarship |
|---|---|---|
| **Summer School 2024 Madeira** | No sponsorships. | CyberSecPro organizer (UNINOVA) enabled 17 scholarships covering the admission-fee. |
| **Summer School 2024 Porto (IPICS 2024)** | Some students supported through Erasmus fellowships. | CyberSecPro organizers (PDMFC; COFAC) enabled 34 scholarships covering the admission-fee. |
| **Winter School 2025 Caparica** | Some students supported through Erasmus fellowships and private company.<br>Ten students from the University of Piraeus were supported through Erasmus funds.<br>Five students from Laurea University were supported through Erasmus funds. | CyberSecPro organizers (PDMFC, FCT, COFAC) enabled 49 scholarships covering the admission-fee. |
| **Summer School 2025-1 and 2 Novi Sad (IPICS 2025)** | Seven Greek students used Erasmus funds.<br>Two students from Finland were supported by LAU internal funds. | CyberSecPro organizers (PDMFC, UNSPMF, COFAC) enabled 33 scholarships in the first week and 40 scholarships in the second week covering the admission-fee. |
| **Winter School January 2026 Lisbon** | Students from Serbia were financially supported by company JetBrains and OSCE office in Serbia. Total number of Serbian students which were supported is 8. 10 students from the University of Piraeus and 6 students-cadets from the Hellenic Airforce Academy were supported through Erasmus fellowships (HAF cooperates with UPRC in the project through Prof. Antonios Andreatos). | CyberSecPro organizers (PDMFC, COFAC) enabled 38 scholarships covering the admission-fee. |

### 4.2.3 Registration process

Through the implementation of the CSP modules, four main types of registration procedures have been identified:

1. **No registration:** Some courses do not require any registration, such as open modules that are freely accessible.
2. **CyberSecPro organizer registration:** Registration is managed directly by the CyberSecPro consortium through dedicated registration pages. This applies to seasonal schools and similar activities, such as IPICS, Winter School 2025, Winter School 2026 and CyberSecPro DCM.
3. **University registration:** Registration is carried out through the hosting university's official systems, such as Moodle system of UNSPMF.
4. **Third-party registration:** Registration is managed by external organizations or platforms outside CyberSecPro. Examples include events accessed through the IEEE EDUCON 2024[2] Conference, RUSI Europe[3], the Symposium on Artificial Intelligence and its Impact on Future Communities[4], and the Digital Security Agency of Cyprus (DSA)[5].

### 4.2.4 Pre-requisites and Admission Criteria

In general, the prerequisites for the modules include basic IT literacy**,** fundamental knowledge of cybersecurity concepts**,** and introductory programming skills, with some modules additionally recommending familiarity with operating systems, networking concepts, and sector-specific environments (e.g., maritime or health). For a limited number of introductory modules, no specific prerequisites are required.

In addition, for one of the seasonal events, the host organized a configuration session one week prior to the start of the event to ensure that learners' computers were properly prepared for the practical exercises. Learners were informed that successful completion of the setup using basic guidance was required to attend, in order to avoid delays during the event; however, all registered learners successfully completed the configuration process.

The admission criteria for the modules were generally flexible and depended on the specific event. For the seasonal schools, applicants were typically required to submit a CV as part of the registration process. The hosting institution reviewed the submitted CVs and supporting information to decide on acceptance. The primary admission criterion was a demonstrated basic connection to, or interest in, cybersecurity, which was satisfied by all applicants, and therefore all submitted applications were accepted. In cases where the number of applications might exceed the available capacity, priority would be given to candidates with more relevant educational or professional backgrounds.

### 4.2.5 Tangible reward to learners

Certificates of attendance represent the most commonly used tangible reward across the implemented CSP modules. As shown in Figure 12, most modules issue certificates upon full attendance, while a smaller number require successful completion of an examination or other predefined criteria. In contrast, several modules do not provide certificates. Certificates are issued by multiple partner organizations, including UNINOVA, PDMFC, UNSPMF, Lusofona University. In addition to certificates, ECTS credits constitute another form of tangible recognition for learners offered by some events.

[2] https://2024.ieee-educon.org/registration
[3] https://my.rusi.org/our-offices/rusi-europe.html
[4] https://www.laurea.fi/en/current-topics/events/symposium-on-artificial-intelligence/
[5] https://dsa.cy/en/

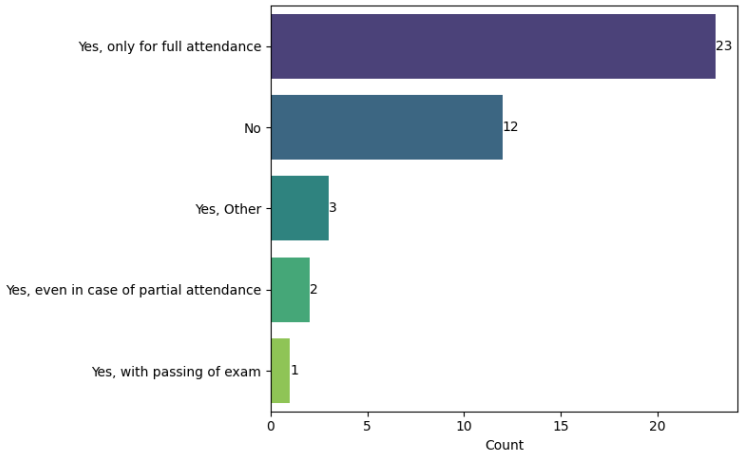


Figure 12: Distribution of certificates after modules implementation

As most of the tangible rewards are related to seasonal schools, all such rewards are listed below.

Table 4: Tangible reward to learners from seasonal schools

| Seasonal schools | ECTS rewarded | Certification and awarding organization |
|---|---|---|
| Summer School 2024 Madeira | No ECTS were awarded. | Learners got Certificate of attendance signed by UNINOVA |
| Summer School 2024 Porto (PICS 2024) | 4 ECTS awarded upon successful completion of the program (including the two-day long Hackathons) by COFAC | Learners got Certificate of attendance signed by COFAC |
| Winter School 2025 Caparica | 2 ECTS awarded upon successful completion of the program by COFAC | Learners got Certificate of attendance signed by UNINOVA and PDMFC |
| Summer School 2025-1 and 2 Novi Sad (IPICS 2025) | 2 ECTS awarded upon successful completion of the program by COFAC | Learners got Certificate of attendance signed by PDMFC and UNSPMF |
| Winter School January 2026 Lisbon | 2 ECTS awarded upon successful completion by COFAC | Learners got Certificate of attendance signed by COFAC |

### 4.2.6 Learning Outcomes

The learning outcomes of all implemented CSP modules are largely consistent with those designed in D3.1, with no significant deviations observed. It is copied here for ease of reference.

Table 5: Learning outcomes

| Related CSP to T4.5 | Learning Outcomes |
|---|---|
| **CSP007- Cybersecurity in Emerging Technologies** | Upon completing the course, trainees should be well-equipped to address the cybersecurity challenges posed by integrating AI, Cloud, and IoT technologies. They should possess a strong foundation of knowledge, practical skills, and ethical considerations necessary for securing interconnected systems in modern IT environments.<br>Trainees are able to demonstrate following specific learning target including:<br>**Knowledge**:<br>• In-depth understanding of various emerging technologies (IoT, cloud, blockchain, AI, etc.) and their inherent security risks.<br>• Comprehensive knowledge of specific vulnerabilities and attack vectors associated with each technology.<br>• Solid grasp of established security principles and best practices applicable to emerging technology environments.<br>• Awareness of relevant regulations and compliance requirements for securing emerging technologies.<br>• Knowledge of specialized security tools and methodologies for different emerging technology platforms.<br>• Understanding of evolving threats and trends in the emerging technology security landscape.<br>**Skills:**<br>• Critically analyse and evaluate the security implications of specific emerging technologies.<br>• Identify and understand unique vulnerabilities and attack vectors in different technology contexts.<br>• Apply established security principles and best practices to design and implement security solutions for emerging technologies.<br>• Develop and customize security strategies for various use cases across diverse emerging technologies.<br>• Utilise specialized security tools and techniques for securing specific platforms and applications.<br>• Effectively communicate and collaborate with stakeholders on emerging technology security challenges and solutions.<br>• Stay informed about new threats and trends, adapting security strategies and practices accordingly.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex emerging technology security scenarios.<br>• Ability to analyse and interpret technical information and develop data-driven security solutions.<br>• Effectively collaborate and communicate technical security concepts to diverse audiences.<br>• Adaptability and agility in responding to the ever-changing emerging technology security landscape.<br>• Strong decision-making skills based on comprehensive understanding of risks and best practices.<br>• Ethical mindset in applying security principles and protecting data privacy in emerging technologies.<br>• Leadership potential in guiding organizations towards secure adoption of emerging technologies |

| Related CSP to T4.5 | Learning Outcomes |
|---|---|
| **CSP008 - Critical Infrastructure Security** | By the end of the training, learners will have gained the following:<br>**Knowledge:**<br>• Acquire a comprehensive understanding of the strategies, and best practices involved in securing critical infrastructure systems against various threats and vulnerabilities.<br>• Acquire a comprehensive understanding of the main security and resilience challenges for the protection 24/7 of critical infrastructures, considering the diverse involved perspectives (technological, policy and legal).<br>• Knowledge of the most common vulnerabilities and particular threats to Critical Infrastructures, considering the drawbacks of maintaining legacy devices (and their protocols) and the real-time performance condition.<br>• Know how to interpret relationships between CIs and the effects that may cause threats, as well as identify possible risks and their management to establish governance, security, and resilience.<br>• Knowledge of the most current regulations and normatives associated with the CIs and their specific application sectors, as well as conduct and ethical criteria.<br>**Skills:**<br>• Identify essential services, threats and possible risks in a CI or between CIs.<br>• Visualise, interpret, and analyse relations and cascading effects to compute possible risks.<br>• Identify, adapt, configure, and deploy protection solutions/technologies to provide 24/7 real-time performance and operational guarantees.<br>• Create trustworthy environments, not only for the end user, but also between CIs, considering the need for situational awareness and resilience.<br>• Identify and apply standards, recommendations, and best practices, but also legal, social and privacy criteria.<br>**Competencies:**<br>• Know how to identify possible misconfigurations or errors in IT and OT devices and (industrial) communication protocols that may lead to significant security risks.<br>• Lead the design, configuration, and deployments of secure and resilient CIs.<br>• Know how to support organizations in implementing measures to harden their systems, ensuring the robustness and resilience of their critical infrastructures against potential and specific threats.<br>• know the existing security technologies, mechanisms, and protocols (of TCP/IP - related to module 4 of the CSP), useful to protect communications between IT-OT components within a CI or between CIs.<br>• Know how to apply standards, recommendations, and best practices, but also legal, social and privacy criteria |

| Related CSP to T4.5 | Learning Outcomes |
|---|---|
| **CSP009- Software Security** | By the end of the training, learners will gain the following:<br>**Knowledge:**<br>• In-depth understanding of common software vulnerabilities and their attack vectors (e.g., injection, XSS, CSRF, memory corruption).<br>• Solid grasp of secure coding principles and best practices in various programming languages.<br>• Knowledge of secure software development methodologies like Secure SDLC and OWASP Top 10.<br>• Understanding of static and dynamic analysis tools and techniques for vulnerability detection.<br>• Awareness of security architecture principles and their application in software design.<br>• Knowledge of risk assessment methodologies for software applications.<br>• Understanding of emerging trends and challenges in software security (e.g., IoT, cloud, blockchain).<br>**Skills:**<br>• Apply secure coding practices in various programming languages to write secure and resilient code.<br>• Perform static and dynamic analysis of software applications using industry-standard tools.<br>• Conduct threat modelling and risk assessment for software systems and applications.<br>• Develop and implement security architectures for secure software design.<br>• Effectively communicate software security risks and mitigation strategies to developers and stakeholders.<br>• Utilise secure coding frameworks and libraries to simplify secure coding practices.<br>• Stay informed about evolving software security threats and mitigation techniques.<br>• Hands-on experience with secure coding tools, vulnerability scanning tools, and penetration testing tools.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex software security scenarios.<br>• Ability to analyse code, identify vulnerabilities, and propose effective mitigation strategies.<br>• Strong analytical and technical skills to understand and apply various security tools and techniques.<br>• Effective communication and collaboration skills to work with developers and stakeholders on security issues.<br>• Adaptability and continuous learning to stay updated with the evolving software security landscape.<br>• Ability to prioritise risks and make informed decisions regarding software security measures.<br>• Leadership potential in promoting a culture of security within software development teams. |

### 4.2.7 Number of job-placements/internships carried out by the students

The results obtained from CyberSecPro Admin portal regaring those implemented module indicate that a total of **341 job placements** were recorded, with **254 placements (approximately 74%)** taking place in external organizations and **87 placements (approximately 26%)** within partner member organizations. These figures suggest that the implemented activities contributed primarily to employment opportunities beyond the consortium institutions, demonstrating a broader impact on the external labour market.

### 4.2.8 Background of learner

This subsection presents an overview of the demographic and professional background of learners participating in the CSP modules, including their gender distribution, age groups, educational background, and professional experience and affiliation.

#### 4.2.8.1 Number of learners in implemented CSP modules per gender

The gender distribution of learners (c.f Figure 13) shows that male learners constitute the majority, followed by female learners, while only a small proportion identified as non-binary or did not respond. Overall, the figure shows that female learners account for 27.48% percent of the total, positioning this share at the upper margin of the industry distribution standard.

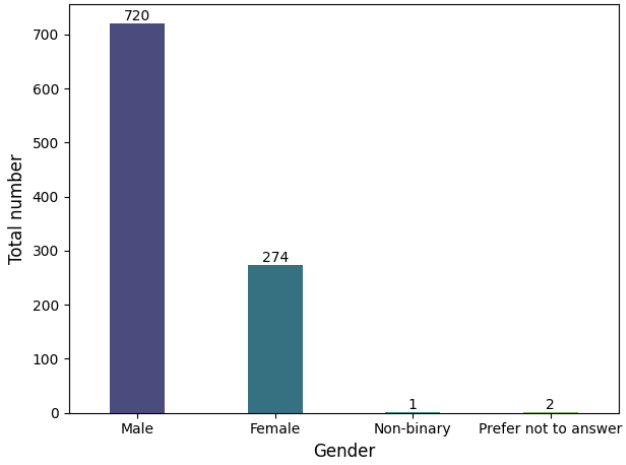


Figure 13: Number of learners in implemented implemented CSP modules per gender

#### 4.2.8.2 Number of learners in implemented CSP modules per Age

Figure 14 presents the distribution of learners across age groups. The majority of learners belong to the 18–24 age group (447 learners)**,** followed by the 25–34 age group (230 learners)[6]**.** Participation decreases significantly in older age categories. These results indicate that the CSP modules primarily attracted young learners and early-career learners, particularly students and young professionals.

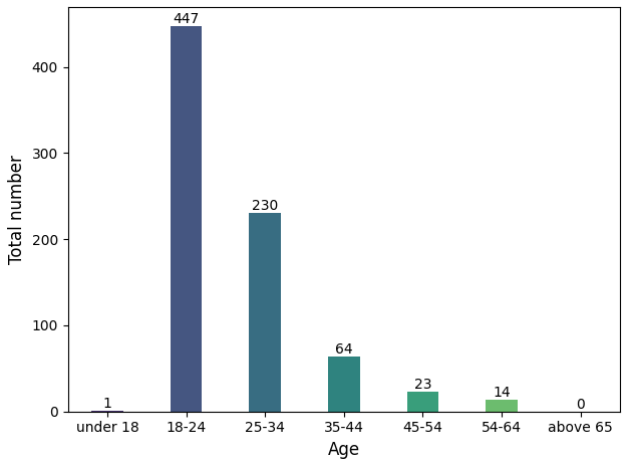


Figure 14: Number of learners in implemented CSP modules per age

[6] The age categorization was followed based on the KPIs from the Grant Agreement and KPI tab in the SYGMA EC portal. In the Grant Agreement, one KPI states that "more than 70 trainees will be over 45 years old." Also, the SYGMA portal includes a KPI specifying "people enrolled aged 25 years or younger."

#### 4.2.8.3 Number of learners in implemented CSP modules per Educational Background

The results presented in Figure 15 indicate that the CSP modules primarily attracted learners from higher education, particularly undergraduate and postgraduate learners.

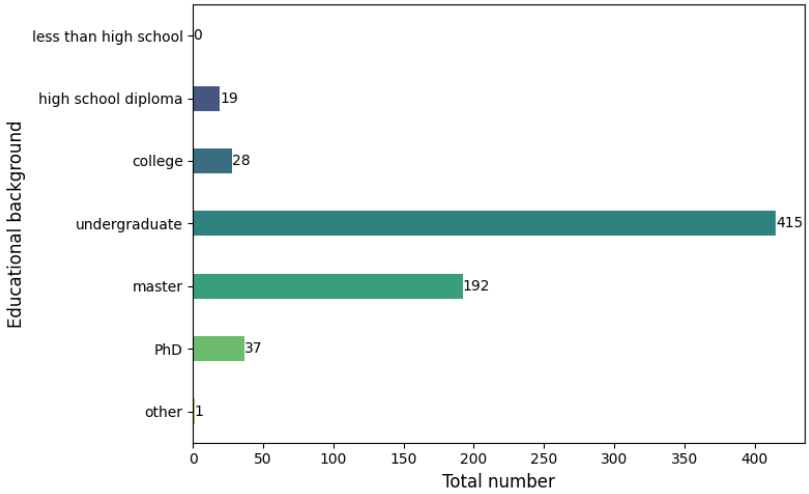


Figure 15: Number of learners in implemented CSP modules per Educational Background

#### 4.2.8.4 Professional Experience and Affiliation

The results presented in Figure 16 demonstrate that the CSP modules primarily attracted students, while also engaging a diverse range of professionals from industry and organizational environments.

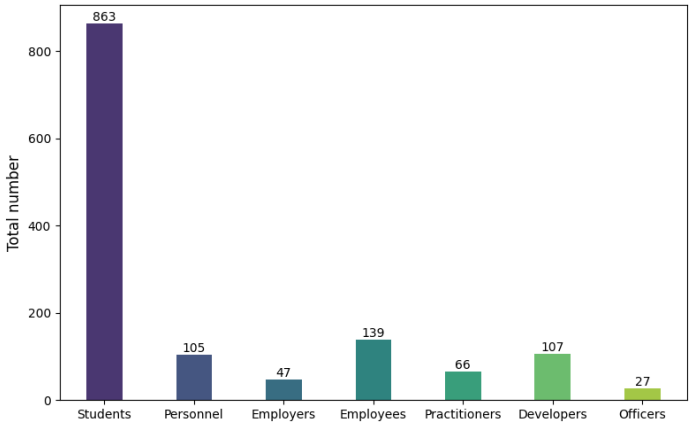


Figure 16: Professional Experience and Affiliation

### 4.2.9 Hosting site

Figure 17 shows that vast majority of CSP modules were organized by EU higher education institutions, while a smaller number were hosted by companies and other types of organizations. This indicates that higher education institutions played the primary role in delivering the CSP training activities, with additional contributions from industry and other stakeholders should be increased in the future.

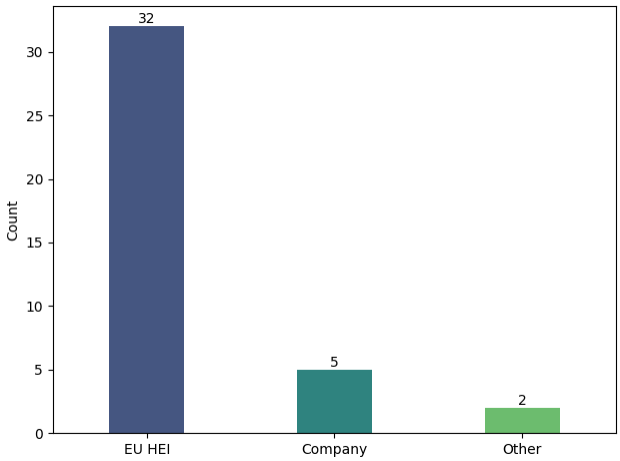


Figure 17: Module hosting sites

### 4.2.10 Evaluation forms of learners and trainers

Below, we introduce the evaluation forms developed within WP5 and implemented in the Admin portal to collect data online.

**CyberSecPro Learners Evaluation Form**

The evaluation is conducted from the learner's perspective through a digital "Evaluation Survey" integrated into the CSP Admin Portal, where trainers can independently design and customise surveys for each module by selecting relevant pre-defined questions covering areas such as content, structure, instruction, platform, interaction, impact, and overall insights; once finalised, the system automatically generates a unique URL and QR code to enable easy distribution of the survey to learners via multiple digital channels.

**CyberSecPro Trainer Evaluation Form**

The evaluation of the training implementation from the trainers' perspective is also conducted using the "Evaluation Survey" feature integrated into the CSP Admin Portal. This feature allows trainers to reflect on and assess their own experience in delivering the module, focusing on aspects such as ease of use of the training materials, interaction with learners, and overall satisfaction with the training implementation process. The trainer survey is automatically generated within the portal for each module implementation. As the survey is standardised, trainers do not need to create the survey from scratch as in the case for learners. The survey can be found under each respective module, allowing trainers to select and complete the survey relevant to their implementation. More information on the survey is provided in D5.1

**Follow-up survey**

As mentioned in Section 2.2, in order to respond to European Commission requirements regarding KPIs specified in the call, an additional questionnaire was developed for CSP providers to collect the relevant data from learners (see Annex D for further details).

We followed two approaches to ensure that we collected the required data as accurately as possible. In the first approach, individual module providers gather required data from their learners and completed the required information themselves by filling in the seventh tab of the Admin portal, labelled "Employment." A screenshot of this section of the admin portal is shown in Figure 18.

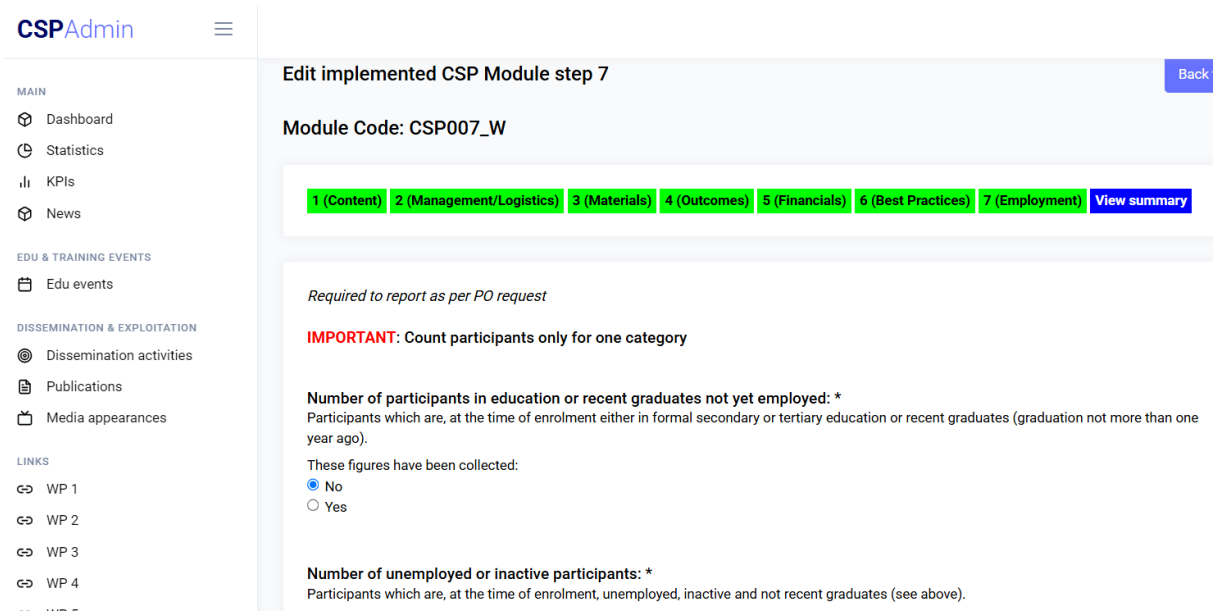


Figure 18: Screen shot of Follow-up survey in the admin portal

In the second approach, as described in D5.1, WP5 followed up with learners attending seasonal schools and collected all the required data. The questionnaire was implemented in the admin portal and completed online, with all responses automatically gathered and stored in the system. A screenshot of the implemented questionnaire in the admin portal is shown in Figure 19.


Figure 19: Follow up survey

# 5 MOOC

Within the CyberSecPro project, three MOOCs were developed to support cybersecurity capacity building. However, only one of these courses is directly aligned with the knowledge areas addressed in this deliverable. In particular, the selected MOOC presented in this deliverable covers the knowledge area KA8 – Cybersecurity Tools and Technologies. Therefore, the following section presents the basic information about the selected MOOC, including its structure, objectives, and syllabus.

## 5.1 MOOC – From Zero to Hero – A complete CyberSecurity Toolkit

The MOOC is freely available to all users who create an account on the project's DCM platform (https://moodle.cybersecpro.grisenergia.pt/course/view.php?id=154 ). The following section presents the MOOC description using the format and structure defined in Deliverable D3.1 for documenting individual modules. Two tables are included: Table 6 provides the general information about the MOOC, while Table 7 presents detailed information on the syllabus, including the topics and learning content covered by the course.

Table 6: General information about MOOC

| **MOOC Title**<br>*The title of the training module* | **From Zero to Hero – A complete CyberSecurity Toolkit** |
|---|---|
| **Alternative Title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | The Practical Cybersecurity Toolkilt: Learn, Practice, Defend<br><br>Hands-On Cybersecurity: Tools, Techniques, and Tactics<br><br>Cybersecurity in Practice<br><br>Cybersecurity Toolkits: Hands-On Experience with Practical Tools |
| **Training offering type**<br>*Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.* | Course (C) / MOOC |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Advanced |
| **MOOC overview**<br>*High-level MOOC overview* | This MOOC provides a practical introduction to essential cybersecurity concepts, tools, and practices. Designed for beginners, it walks learners step by step through building a foundational security toolkit—covering topics such as threat awareness, secure communication, password management, system hardening, and incident response basics. By the end, participants will be equipped with the knowledge and skills to confidently navigate the cybersecurity landscape and apply protective measures in real-world scenarios. |

| **MOOC Title**<br>*The title of the training module* | **From Zero to Hero – A complete CyberSecurity Toolkit** |
|---|---|
| **MOOC description**<br>*Indicates the main purpose and description of the MOOC.* | This MOOC is designed to guide beginners through the essentials of cybersecurity, covering foundational concepts, practical skills and advanced techniques to protect against cyber threats. As part of the CyberSecPro project, this MOOC attempts to empower learners with the knowledge and tools needed to build upon a career in cybersecurity, focusing on areas like network security, ethical hacking, and incident response. |
| **Learning outcomes and targets**<br>*A list of knowledge, skills and competences achieved by the participants as a result of taking a MOOC* | Upon successful completion of this MOOC, learners will be expected to be able to:<br>• **Remember & Understand**<br>  ○ Define fundamental cybersecurity concepts, including threats, vulnerabilities, attack vectors, and security controls.<br>  ○ Describe the purpose and functionality of common cybersecurity tool categories, such as network security, endpoint protection, vulnerability assessment, penetration testing, and digital forensics.<br>• **Apply**<br>  ○ Use industry-standard cybersecurity tools to perform basic security tasks, including network scanning, traffic capture, vulnerability identification, and controlled exploitation in safe environments.<br>  ○ Apply defensive security mechanisms to protect networks and systems, including firewalls, intrusion detection/prevention systems, and endpoint security solutions.<br>• **Analyze**<br>  ○ Analyse network traffic, scan results, and system artefacts to identify suspicious behaviour, misconfigurations, and potential security weaknesses.<br>  ○ Differentiate between attacker techniques and defensive controls by examining real-world attack and mitigation scenarios.<br>• **Evaluate**<br>  ○ Assess the security posture of systems and networks based on vulnerability scan outputs and monitoring data.<br>  ○ Evaluate risks and prioritize remediation actions based on impact, likelihood, and best practices.<br>• **Create**<br>  ○ Create clear and structured security reports summarising findings from scans, traffic analysis, and exploitation exercises.<br>  ○ Propose appropriate mitigation and prevention measures to improve the overall security of IT systems and applications. |

| **MOOC Title**<br>*The title of the training module* | **From Zero to Hero – A complete CyberSecurity Toolkit** |
|---|---|
| **Main topics and content list**<br>*A list of main topics and key content* | • Knowledge on red-teaming and ethical hacking<br>• Network scanning and enumeration<br>• Vulnerability scanning and assessment<br>• Intrusion detection and prevention system<br>• Packet analysis and network forensics<br>• Malware analysis and reverse engineering<br>• Incident response |
| **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | Assessment is based on self-evaluation and continuous learning verification through quizzes and practical challenges embedded throughout the MOOC. These assessment elements are designed to help participants actively check their understanding of key concepts and apply cybersecurity principles to realistic scenarios. Quizzes are used to reinforce theoretical knowledge and terminology, while challenges encourage problem-solving and decision-making in common cybersecurity situations. |
| **Training Provider**<br>*Name(s) of training providers.* | PDMFC |
| **Contact**<br>*Name(s) of the main contact person and their email address.* | Nuno Pedrosa (nuno.pedrosa@pdmfc.com) |
| **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the MOOC, as well as periodicity (e.g., even after the end of the CSP programme).* | Self-paced |
| **Duration**<br>*Duration of the training.* | Estimated at 130 hours, including exercises. |
| **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Virtual (through the DCM platform)<br>https://moodle.cybersecpro.grisenergia.pt/course/view.php?id=154 |

| **MOOC Title**<br>*The title of the training module* | **From Zero to Hero – A complete CyberSecurity Toolkit** |
|---|---|
| **Knowledge area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly<br>• KA8 – Cybersecurity Tools and Technologies<br>• KA9 – Penetration Testing<br>• KA10 – Cyber Incident Response |
| **Pre-requisites** | Cybersecurity Fundamentals |
| **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this MOOC training with ECSF. It also indicates which ECSF profiles needs this MOOC.* | Mainly:<br>• ECSF Profile: Digital Forensics Investigator<br>• ECSF Profile: Penetration Tester |
| **Tools to be used**<br>*A list of tools that will be used for the operation of this MOOC.* | Several tools may be applied such as: Burp Suite, Chain-of-custody templates, ClamAV, DNS (basic networking support), DVWA (Damn Vulnerable Web Application), Elasticsearch, EICAR test file, File integrity monitoring (FIM), Firewall logs, GnuPG / GPG, hping3, HTTP/HTTPS web browser, Hydra, Incident response templates, IOC tracking tables, Java (required by Burp Suite / Splunk), jq, Kali Linux, Kibana, Linux (Ubuntu recommended), Logstash, Metasploit Framework, Metasploitable 2, Modern web browser (Chrome, Firefox, Edge, or Safari), Nmap, OpenVAS, OpenVPN (conceptual / optional), PAM (Pluggable Authentication Modules), ParrotOS, pfSense, Ping / ICMP utilities, Presentation software (PowerPoint or Google Slides), Risk register template, RDP (Remote Desktop Protocol), SHA-256 hashing tool (sha256sum), SIEM-style log datasets, Snort, Splunk Enterprise, Spreadsheet software (Excel, Google Sheets, or LibreOffice Calc), SQLmap, SSH client/server, Suricata, Terminal / command line interface, Text editor, VirtualBox, VPN client software, Wazuh Agent, Wazuh Server (All-in-One OVA), Wireshark, Windows 10 or 11, Word processor (Word, Google Docs, or LibreOffice Writer). |
| **Language**<br>*Indicates the spoken language and the* | English |

| **MOOC Title**<br>*The title of the training module* | **From Zero to Hero – A complete CyberSecurity Toolkit** |
|---|---|
| *language for the material and the assessment/evaluation.* | |
| **ECTS**<br>*If applicable, the number of ECTS.* | 5 ECTS |
| **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | No (if attending as guest) |
| **MOOC enrolment dates**<br>*Indicates the enrolment dates for the operation of this MOOC.* | Self-paced |
| **Other important dates**<br>*If applicable, any other important dates for this MOOC (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the MOOC description.* | Refer and check online CyberSecPro DCM System for current information. |

Table 7: Syllabus

| **Main topics** | **Suggested Content (with bullet list)** |
|---|---|
| Topic-1: Introduction to Cybersecurity | Common offensive cybersecurity tools<br>Network security tools<br>Endpoint security tools<br>Vulnerability assessment tools<br>Forensics & incident response tools<br>Penetration testing tools |
| Topic-2: Introduction to Red Teaming and Ethical Hacking | Setting up the environment with Kali Linux<br>Steps on ethical hacking<br>Exploiting vulnerabilities with Metasploit<br>Intercepting traffic with Burp Suite<br>Brute forcing logins with Hydra |
| Topic-3: Network Scanning and Enumeration | What is network scanning?<br>Phases of network scanning<br>Essential network scanning tools |
| Topic-4: Vulnerability Scanning and Assessment | What is vulnerability scanning?<br>Types of vulnerability scans |

| Main topics | Suggested Content (with bullet list) |
|---|---|
| Topic-5: Introduction to Software Security for Health | Introduction to software security for health<br>Static application security testing (SAST) workflow |
| Topic-6: Intrusion Detection System | What is an intrusion detection and prevention system?<br>Intrusion detection systems<br>Intrusion prevention systems<br>Network-based intrusion detection and prevention system<br>Host-based intrusion detection and prevention system<br>Snort and Suricata<br>Triggering and analyzing alerts |
| Topic-7: Packet Analysis and Network Forensics | Key components of a packet<br>How packet analysis works?<br>Key uses of packet analysis<br>Security and ethical considerations<br>Wireshark – for analyzing suspicious traffic<br>Packet capture and analysis using tcpdump<br>Packet analysis lab |
| Topic-8: Malware Analysis and Reverse Engineering | What is malware analysis?<br>Types of malware<br>Essential tools for malware analysis<br>Inspecting malware without execution |
| Topic-9: Incident Response: SIEM – Splunk & Elk | Introduction to SIEM<br>Log collection and normalization<br>Real-time monitoring and reporting<br>Early threat detection |
| Topic-10: Cybersecurity Essentials and Management (Energy Sector) Foundations | Cyberattacks on energy<br>Case study: Colonial pipeline cyber attack<br>Smart grids and cybersecurity challenges |
| Topic-11: Cybersecurity Essentials and Management (Energy Sector) – Common vulnerabilities | Vulnerability assessment<br>Assets in energy domain and their cybersecurity challenges |

| Main topics | Suggested Content (with bullet list) |
|---|---|
| Topic-12: AI and Cybersecurity: Research in Maritime | AI for maritime cybersecurity<br>Adversarial AI<br>Defensive AI<br>Model inversion and perturbation attacks<br>Dataset poisoning for AIS |

# 6 Conclusion

This deliverable has presented a comprehensive report on the implementation of training modules on emerging technologies carried out under Task T4.5 of the CyberSecPro project. The document has provided an overview of the delivered CSP modules related to cybersecurity in emerging digital technologies, critical infrastructure security, and software security, supported by quantitative data on module implementation and student participation.

The analysis demonstrates that a total of 39 training modules were successfully implemented across multiple industry sectors, including energy, health, maritime, and general cybersecurity. The results show balanced coverage across training levels, a strong emphasis on seminar-based delivery formats, and substantial participant engagement in both sector-specific and cross-sectoral modules. The sectoral distribution of modules and enrolments confirms alignment with the project's focus on critical domains while maintaining broad applicability.

In addition to quantitative reporting, the deliverable has presented some data regarding organisational and logistic aspects of implemented modules.

Overall, this deliverable provides evidence of the effective deployment and reach of the CyberSecPro training programme on emerging technologies. The reported results contribute to monitoring project progress and offer valuable input for the refinement of future training activities, supporting the CyberSecPro project's objectives of strengthening cybersecurity skills and workforce readiness across critical sectors.

# References

[1] “Apache Subversion,” [Online]. Available: **https://subversion.apache.org/**. [Accessed 20 February 2024].

[2] OwnCloud GmbH," OwnCloud," [Online]. Available: **https://owncloud.com**. [Accessed 26 January 2024].

[3] NextCloud GmbH," NextCloud," [Online]. Available: **https://nextcloud.com**. [Accessed 26 January 2024].

[4] GitLab Inc., “GitLab,” [Online]. Available: **https://about.gitlab.com**. [Accessed 04 March 2024].

# Annex A: Template for the Documentation of Implemented CSP Modules

In this section, we have used the template for describing CSP modules from D4.1. We have added additional elements needed for the documentation of implemented CSP modules as shown in Table 8. We have also synchronized this template with the descriptions for training modules D3.1.

Table 8: Template for the documentation of implemented CSP Modules

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| **Code** | **Code** (mandatory)<br>*Code format:*<br>*For general modules: CSP[n]_x*<br>• *[n] is the CSP module number (currently between 001 and 012)*<br>• *x is the module offering type (see below)*<br>*For sector-specific modules: CSP[n]_x_y*<br>• *[n] is the CSP module number (currently between 001 and 012)*<br>• *x is the module offering type (see below) and y is the sector (E, H, M)* | |
| **Content** | **Module title as defined in the CSP catalogue** (mandatory)<br>*The title of the module as defined in the CSP catalogue (currently in D4.1)* | |
| | **Title of the implemented CSP module** (mandatory)<br>*The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned in D3.3, D3.4 or D3.5, but in any case, one that can be proven after the implementation, e.g. from local documentation.*<br>*In cases of multiple implementations in the different time, versioning will be applied at the end of the module title.* | |
| | **Description of the implemented CSP module** (mandatory)<br>*Usually, the module description from the syllabus (D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module* | |
| | **Related knowledge area(s)** (mandatory)<br>*Mapping to the 10 selected CSP knowledge areas* | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | *defined in D2.3* | |
| | **Indicate whether in the implemented CSP module, learners learned how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome** (mandatory)<br>*Yes (also if a part of the module covered this topic) or No (otherwise)* | |
| | **Category/ies of capabilities** (mandatory)<br>*Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.* | |
| | **Learning outcomes and targets** (mandatory)<br>*A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1* | |
| | **Type of the implemented CSP module (**mandatory)<br>*Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.* | |
| | **Affiliated (Summer/Winter) School**<br>*Indicates summer school affiliated, (CyberHot 2024, CyberHot 2025, Summer school 2024 Madeira, Summer school 2024 Porto, Winter school 2025 Lisbon, Summer school 2025 Novi Sad- Week 1, Summer school 2025 Novi Sad- Week 2, Winter school in Lisbon)* | |
| | **Information on the sector (**mandatory)<br>*Indicates General, Maritime, Health, or Energy* | |
| | **Pre-requisites** (mandatory)<br>*Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)* | |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)** | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | *An indicative relevance of the implemented CSP module within the ECSF (currently in this link). It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)* | |
| | **Provision type and location (**mandatory)<br>*Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website* | |
| | **Types of assignments**<br>*Programming task, essay, presentation, test-exam, mutual peer-review among students, other* | |
| | **Level** (mandatory)<br>*B (Basic), A (Advanced)* | |
| | **Language** (mandatory)<br>*Indicates the spoken and the language**s** for the material and the assessment/evaluation* | Spoken:<br>Material:<br>Assessment: |
| **Management /Logistics** | **Provider(s)** (mandatory)<br>*Name(s) of the providing organisation(s), e.g. beneficiary/ies* | |
| | **Hosted of the module**<br>*Select the type of organization that hosted this implemented module (EH HEI, Compony, other)* | |
| | **Host details**<br>*A freetext to provide additional details about the host organization (name, location, specific department, etc.)* | |
| | **Number of seminars/lectures held by industry experts: ***<br>*Required to report these KPIs in relation to the call.*<br>*Indicate number of "From members of the consortium" as well as number of "Not from members of the consortium"* | |
| | **Contact** (mandatory) | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | *Full name(s) of the main contact person(s) including their email address* | |
| | **Trainer(s)**<br>*All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training* | |
| | **Tool(s) used** (mandatory)<br>*A list of tools that have been used for the implemented CSP module*<br>*Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program"* | |
| | **Registration procedure**<br>*How (e.g. where and when registration of learner took place) did learner have to register*<br>*If there is no registration procedure, please write, "None"* | |
| | **Admission criteria**<br>*Limits of admission (if any), requirements and selection criteria, e.g. knowledge prerequisites, e.g. modules that learners need to have attended before or knowledge that is essential to understand the course (e.g. basics of cryptography or security management).*<br>*If there are no admission criteria, please write, "None"* | |
| | **The actions that were taken to attract learners especially those coming from disadvantaged groups, and the scholarships and mobilities included (if any)**<br>*If there are no actions, please write, "None"* | |
| | **ECTS**<br>*The number of ECTS*<br>*If there is no ECTS, please write, '0'* | |
| | **Calculation of number of ECTS e.g. (duration of implemented module [hours] + duration of self-study [hours])/25)** | |

| CSP Module Elements | CSP Module fields legend | | CSP Module information |
|---|---|---|---|
| | *Make sure that the number of ECTS matches the learning effort of the training (i.e. 1 ECTS is awarded per 25-30 hours of learning, depending on the national legislation)* | | |
| | **Certificate of Attendance (CoA)** (mandatory)<br>*Indicates Yes or No (and the conditions for yes, e.g. partial or full attendance, passing of exam)* | | |
| | **Provide explanation if Certificate of Attendance (CoA) not happened** | | |
| | **Exact dates, when offered** (mandatory)<br>*Indicates the dates* (year, month, day) *for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information* | | |
| | **Schedule and Duration**<br>(mandatory) | *Duration of the implemented CSP module (in hours)* | |
| | | *Duration of prefabricated teaching video(s) from the CSP module used in the implementation (in hours)* | |
| | | *Estimated duration for students online-interaction during the implemented CSP module (in hours)* | |
| | | *Duration of self-study (in hours)* | |
| | | *Frequency, duration (in hours), and rhythm of assignments if applicable* | |
| **Materials** | **Location of the learning and training materials, incorporating text and multimedia, e.g. manuals, video tutorials, and interactive guides**<br>*Link to DCM, otherwise other link* | | |
| | **Location of activity modules, such as forums, quizzes, and assignments**<br>*Link to DCM, otherwise other link* | | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | **Location of community support**<br>*Link to DCM, otherwise other link* | |
| | **Location of administrator documentation and configuration guides of tools used**<br>*Link to DCM, otherwise other link* | |
| | **Hours of hands-on training, making use of the equipment purchased/leased within the framework of this action**<br>*Type "0" if you didn't use equipment purchased/leased within the framework of this action*<br>*Required to report these KPIs in relation to the call.* | |
| | **Mention clearly the list of materials used to teach and study each training module and identify those that have been developed with project funds and their location (these must be public).** | |
| **Outcomes** | **Learners enrolled** (mandatory)<br>*Number of learners* | |
| | **Number of learners per gender** (mandatory)<br>*Indicate per female, male, non-binary, prefer not to answer* | |
| | **Number of learners per category** (mandatory)<br>*Covered categories: Students, academic personnel, employers, employees, practitioners, developers, officers (in absolute numbers). Each learner can belong to more than one category.* | |
| | **Learners' background** (mandatory)<br>*Provides characteristics of learners, especially the following details, as they relate to CSP's KPIs:*<br>• *Number of learners more than 45 years old*<br>• *Number of learners, who are non-ICT graduates*<br>• *Number of learners, who are cybersecurity self-trained*<br>*In the collection form this need to be 4 mandatory fields: One in free text to describe the scenario, 3 each asking for a figure to enable adding* | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | *up the figures for the KPIs.* | |
| | **Number of job-placements/internships carried out by the students *** <br> *Required to report these KPIs in relation to the call.* <br> *in the organization member of the consortium* <br> *in an external organization* | |
| | **Have you collected the *number of applications* to the education programme(s) per gender, age, educational background, country of origin?** <br> *Required to report these KPIs in relation to the call.* <br> *In case yes, Indicate gender, age, educational background* | |
| | **The *number of students enrolled* to the education programme(s) per Age** <br> *Required to report these KPIs in relation to the call.* | |
| | **The number of students enrolled to the education programme(s) per educational background** <br> *Required to report these KPIs in relation to the call.* | |
| | **The number of students enrolled to the education programme(s) per Country of origin** <br> *Required to report these KPIs in relation to the call.* | |
| | **Evaluation method(s)** (mandatory) <br> *Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | |
| | **Number of evaluation forms filled by learners** (mandatory) | |
| | **Evaluation forms of learners** (mandatory) <br> *The form that learners used to evaluate the course offer (reference or link)* | |
| | **Evaluation forms of trainers** (mandatory) <br> *The form that trainers used to evaluate the outcomes (reference or link)* | |
| | **Evaluation and verification of learning outcomes** <br> *Assessment elements and high-level process* | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | *to determine participants have achieved the learning outcomes (text or reference)*<br><br>*If there is no evaluation and verification of learning outcomes, please write, "None".* | |
| | **The number of people reporting an improved employment situation after the end of the training supported by the programme** | |
| **Financial information (possibly confidential depending on the decision of the provider)** | **Income** (mandatory) | |
| | **Scholarships/sponsorships** (mandatory)<br><br>*free text to describe the scenario* | |
| | **Waived registrations**<br><br>*In these two questions, each student should be counted only once. If a student gets a waived registration, they should be mentioned in the first field. If the student provides something in addition to the waived registration, please add them to the second one. Please ensure that a student counted in the first field is not counted in the second one.*<br><br>• **Number of waived (payable) registrations ***<br><br>• **In addition to the number of waived (payable) registrations, number of students benefiting from the support (financial or other) from the education institutions *** | |
| | **Number of female participants benefitting from financial support** | |
| | **Cost-benefit analysis of the modules**<br><br>*The amount of money paid for the course and the amount of income earned from the course*<br><br>*If there is no money in and no money our and no cost-benefit analysis of the module, please write, "None".* | |
| **Recommendations for Best Practices**<br><br>**Brief suggestions to enhance the effectiveness of CSP training (Lessons learnt)** | **Recommendations for improving the module**<br><br>*Brief practical suggestions to elevate and improve the future CSP training module quality* | *For example:*<br><br>• *Enhance the training module with more interactive exercises.*<br><br>• *Continuously update the module with the latest cybersecurity* |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | | *trends.* |
| | **Recommendations for expanding the reach of the module**<br>*Brief practical suggestions to expand the reach to a wider audience and diversifying delivery methods* | *For example:*<br>• *Partner with industry.*<br>• *Promote the module through targeted marketing.* |
| | **Recommendations for future initiatives**<br>*Brief practical suggestions and future recommendation for proactive strategies to further strengthen cybersecurity training initiatives and address emerging challenges* | *For example:*<br>• *Implement Standard Cybersecurity Framework in syllabi.*<br>• *Foster collaboration with industry clusters for ongoing professional development opportunities for the participants of the training.*<br>• *Foster EU member state collaboration on cybersecurity training offerings.* |
| **Employment** | **Number of participants in education or recent graduates not yet employed**<br>*Participants which are, at the time of enrolment either in formal secondary or tertiary education or recent graduates (graduation not more than one year ago).*<br>*If the answer is yes, indicate the figure by gender.* | |
| | **Number of unemployed or inactive participants**<br>*Participants which are, at the time of enrolment, unemployed, inactive and not recent graduates (see above).*<br>*If the answer is yes, indicate the figure by gender.* | |
| | **Number of employed participants**<br>*Participants which are, at the time of enrolment, in employment.*<br>*If the answer is yes, indicate the figure by gender.* | |
| | **Number of participants in education or recent graduates not yet employed who found a job after completing the educational programme/training** | |

| CSP Module Elements | CSP Module fields legend | CSP Module information |
|---|---|---|
| | **activities/job placement**<br>*This includes partial or full employment, self-employment or similar.*<br>*If the answer is yes, indicate the figure by gender.* | |
| | **Number of unemployed or inactive participants who found a job after completing the educational programme/training activities/job placement**<br>*This includes partial or full employment, self-employment or similar.*<br>*If the answer is yes, indicate the figure by gender.* | |
| | **Number of employed participants who improved their employment situation after completing the educational programme/training activities/job placement**<br>*This includes transit from precarious to stable employment or from underemployment to full employment or transit to a job requiring higher competences/skills/qualifications and/or more responsibilities or a promotion to a higher-level job.*<br>*If the answer is yes, indicate the figure by gender.* | |

# Annex B: Template for Planning the Offering of CSP Modules

A draft template for the offering of CSP Modules was provided in D3.1 "*CyberSecPro programme main components and procedures*". It is copied here for ease of reference.

Table 9: Template for Planning the Offering of CSP Modules

| CSP Module Elements | CSP Module [Fields legend] | CSP Module Information |
|---|---|---|
| **Overview** | **Code**<br>*Mandatory field. Code format:*<br>*For general modules: CSP[n]_x*<br>• *[n] is the CSP module number (currently between 001 and 012)*<br>• *x is the module offering type (see below)*<br>*For sector-specific modules: CSP[n]_x_y*<br>• *[n] is the CSP module number (currently between 001 and 012)*<br>• *x is the module offering type (see below) and y is the sector (E, H, M)* | |
| **Content** | **Module title as defined in the CSP catalogue**<br>*Mandatory field. The title of the module as defined in the CSP catalogue (currently in D4.1)* | |
| | **Title of the implemented CSP module**<br>*Mandatory field. The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned in D3.3, D3.4 or D3.5, but in any case, one that can be proven after the implementation, e.g. from local documentation.* | |
| | **Description of the implemented CSP module**<br>*Mandatory field. Usually, the module description from the syllabus (D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module.* | |
| | **Related knowledge area(s)**<br>*Mandatory field. Mapping to the 10 selected CSP knowledge areas defined in D2.3.* | |
| | **Indicate whether in the implemented CSP module, learners will learn how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome**<br>*Mandatory field. Yes (also if a part of the module* | |

| | | |
|---|---|---|
| | *covered this topic) or No (otherwise)* | |
| | **Category/ies of capabilities**<br>*Mandatory field. Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.* | |
| | **Learning outcomes and targets**<br>*Mandatory field. A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1* | |
| | **Type of the implemented CSP module**<br>*Mandatory field. Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.* | |
| | **Information on the sector**<br>*Mandatory field. Indicates General, Maritime, Health, or Energy* | |
| | **Pre-requisites**<br>*Mandatory field. Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)* | |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of the implemented CSP module within the ECSF (currently in this link). It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)* | |
| | **Provision type and location**<br>*Mandatory field. Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website* | |
| | **Types of assignments**<br>*Programming task, essay, presentation, test-exam,* | |

| | | |
|---|---|---|
| | *mutual peer-review among students, other* | |
| | **Level**<br>*Mandatory field. B (Basic), A (Advanced)* | |
| | **Language**<br>*Mandatory field. Indicates the spoken and the languages for the material and the assessment/evaluation* | Spoken:<br>Material:<br>Assessment: |
| **Management/ Logistics** | **Provider(s)**<br>*Mandatory field. Name(s) of the providing organisation(s), e.g. beneficiary/ies* | |
| | **Contact**<br>*Mandatory field. Full name(s) of the main contact person(s) including their email address* | |
| | **Trainer(s)**<br>*All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training* | |
| | **Tool(s) to be used**<br>*Mandatory field. A list of tools that are to be used for the implemented CSP module.*<br>*Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program".* | |
| | **Registration procedure**<br>*How (e.g. where and when registration of learner will take place) will learner have to register.* | |
| | **Admission criteria**<br>*Limits of admission (if any), requirements and selection criteria, e.g. knowledge prerequisites, e.g. modules that learners need to have attended before or knowledge that is essential to understand the course (e.g. basics of cryptography or security management).* | |
| | **ECTS**<br>*The number of ECTS* | |

| | | | |
|---|---|---|---|
| | **Certificate of Attendance (CoA)**<br>*Mandatory field. Indicates Yes or No (and the conditions for yes, e.g. partial or full attendance, passing of exam)* | | |
| | **Exact dates, when offered**<br>*Mandatory field. Indicates the dates (year, month, day) for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information* | | |
| | **Schedule and duration**<br>*Mandatory field.* | *Duration of the implemented CSP module (in hours).* | |
| | | *Duration of prefabricated teaching video(s) from the CSP module that will be used in the implementation (in hours).* | |
| | | *Estimated duration for students online-interaction during the implemented CSP module (in hours).* | |
| | | *Frequency, duration (in hours), and rhythm of assignments if applicable.* | |
| **Materials** | **Location of the learning and training materials, incorporating text and multimedia, e.g. manuals, video tutorials, and interactive guides**<br>*Link to DCM once available, otherwise other link.* | | |
| | **Location of activity modules, such as forums, quizzes, and assignments**<br>*Link to DCM once available, otherwise other link.* | | |
| | **Location of community support**<br>*Link to DCM once available, otherwise other link.* | | |
| | **Location of administrator documentation and configuration guides of tools used**<br>*Link to DCM once available, otherwise other link.* | | |
| **Outcomes** | **Evaluation method(s)**<br>*Mandatory field. Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.).* | | |

| | | |
|---|---|---|
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes (text or reference).* | |
| **Financial information (possibly confidential depending on the decision of the provider)** | **Price/Fee** | |
| | **Scholarships/sponsorships**<br>*Number of offered cost free registrations*<br>*In the collection form some free text to describe the scenario, e.g. discount options and the respective conditions, is useful.* | |
| **Data Protection** | *Conditions of data collection and processing by the module provider, e.g. with respect to GDPR compliance, purpose of collection (e.g. monitoring progress or gathering feedback), processing (analytics) tools, receiver of data, duration of storage, protection tools* | |

# Annex C: Reporting Method(s)

One of the challenges found during the operation phase of the project has been to precisely establish the type of resource, method or tool necessary for the collection of data documenting the implemented CSP modules and its sharing without depending on external management entities. Sensitive data, such as financial data, scholarships or restrictions of each entity, must be protected in several aspects, taking care of the confidentiality, integrity and availability of such data.

At least for the time, until the DCM became available, a provisional method was needed to document the implemented CSP modules. Exploring the various existing mechanisms without dependence on external entities and based on collaborative solutions (e.g., web forms, online excels or docs, online repositories, etc.), we found several strategies that can be adapted for our purpose, such as:

- Strategy 1: Sharing information using the most common means such as e-mail.
- Strategy 2: Setting up security mechanisms to establish secure point-to-point communications for information transference (e.g., a Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), File Transfer Protocol Secure (FTPS), etc.).
- Strategy 3: Install or depend on on-premises repositories such as the SubVersioN (SVN) [1] provided by the coordinator for the CyberSecPro project or other similar ones such as OwnCloud [2] or NextCloud [3]. In this way, entities can centralise their information on a common server, and manage their own data at all times. Moreover, among the services offered by NextCloud, one can find remote collaboration applications that also benefit cooperation and interaction.
- Strategy 4: Implement centralised but customised ad hoc solutions according to the needs of the moment, and through a private server under limited access. This feature benefits the process of expanding capabilities or services that may be required to cover particular solutions that may arise at any given time.
- Strategy 5: Expanding Strategy 4 but focusing on a dynamic web platform, such as the DCM platform, which can be accessible under controlled policies and procedures.
- Strategy 6: Using a platform like GitLab [4] or any other web frontend for git, as it would combine the advantages of Strategies 4 and 5 with the possibility to use standard clients such as git.

Beyond these solutions and their corresponding advantages, there were also further aspects to be considered:

- General: It turned out that the EC and the reviewer asked for additional information to be reported, often on unexpected content, that then needed to be collected (additionally), so the collection tool needed to be flexible for updates.
- Strategies 1 and 2: Both scenarios were not suitable for the CyberSecPro project, which is composed of several partners interacting. They must cooperate to lead common purposes that must be transparent for all those involved, for example, in a common training module. Any constraints that may deviate from centralization and the provision of (semi-)interactive solutions may lead to unforeseen delays, conflicts, confusions or overlaps.
- Strategy 3: This scenario favours the centralisation of data, but does not allow the use of interactive solutions (with the exception of certain applications such as NextCloud) that facilitate the updating of such data from a collaborative and non-overlapping perspective. Moreover, Strategies 2 and 3 require entities/end users to install, maintain and apply client software components, which can be cumbersome or tedious to use.
- Strategies 4, 5, and 6: Fortunately, all three strategies are well suited for CyberSecPro since they facilitate to create customized solutions according to the needs. However, any

customisation process involves costs in terms of effort and time, especially in the case of Strategy 5, where the implementations must cover a wide range of technical requirements.

For this reason, and while the DCM platform was being finalised and tested, we chose Strategy 4 by extending the capacities of the CSP internal web (https://admin.cybersecpro-project.eu) and implementing the template described in Section 2.2 via a (semi-)interactive tool for module providers. Figure 1 shows the screenshot from the system provided by ACEEU, which is also available via:

https://admin.CyberSecPro-project.eu/implementedmodules/listimplementedmodules

If providers of modules liked to combine the content of several modules into one programme (or course or similar, depending on local terminology), then for each module, whose content is used, one entry was to be made in the system.

# Annex D: CyberSecPro Evaluation Forms

## CyberSecPro Learner Evaluation Form

**CyberSecPro Learner Evaluation Form**

Start time: ……. End time: …….
Title (add the name of the course): …….
Description (add further information on the course, e.g. course dates): …….

**Survey Questions**
Note: The checkbox determines whether the question will be included in the survey. The dropdown shows the question's scale. It is just for your information, not to select anything.

**Mandatory Questions**
These questions are included in all surveys.

**General Overview**
How would you rate your overall satisfaction with the training module?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Course content and structure: How satisfied are you with …**
the overall quality of instructional materials?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the clarity of instructional materials?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the practical relevance of the content (e.g. needed practical skills, real-world scenarios, professional contexts, and industry standards)?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the alignment of course design and content with the intended learning objectives?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Instructor(s): How satisfied are you with …**

the instructor(s)'s knowledge and competence brought into the training module?
- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the instructor(s)'s responsiveness and support?
- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the instructor(s)'s teaching approach?
- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Impact**

How relevant are the skills and knowledge gained to your current or desired job role?
- Not Relevant at All
- Low Relevant
- Slightly Relevant
- Somewhat Relevant
- Moderately Relevant
- Very Relevant
- Extremely Relevant

To what extent did this course enhance your knowledge and skills?
- Not at All
- To a Very Small Extent
- To a Small Extent
- To a Moderate Extent
- To a Fairly Large Extent
- To a Large Extent
- To a Very Large Extent

How likely are you to further explore the topic of the module (e.g. through self-learning or another course)?
- Extremel Unlikely
- Unlikely
- SlightlyUnlikely
- Neutral
- Slightly Likely
- Likely
- Extremely Likely

**Optional Questions**

Please select the questions you want to include in this survey by checking the box.

**Learning Platform: How satisfied are you with …**

the accessibility of the learning platform?
- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the ease of navigation of the learning platform?
- Strongly Dissatisfied

- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the performance and reliability of the platform (e.g. no errors and quick loading times)?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the visual appeal of the platform?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the interactivity of & engagement opportunities on the platform (e.g., quizzes, discussion forums, gamification)?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Community / Interaction: How satisfied are you with …**

the interaction facilitated between learners and external actors (e.g. invited experts)

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the interaction facilitated between learners?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Evaluation & Recognition: How satisfied are you with …**

the transparency of the examination process?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

the fairness of the examination process?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied

- Very Satisfied

the value the (attendance) certificate and potentially awarded credit provides in your professional or academic field?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Closing Questions**

These questions are included in all surveys.

**Final questions**

How likely are you to recommend this learning experience to someone looking to improve skills in the cybersecurity field?
0 - Not at all likely 1 2 3 4 5 6 7 8 9 10 - Extremely likely
How could the overall learning experience be enhanced? ……
Any further comments you like to share: ……

# CyberSecPro Trainer Evaluation Form

**CyberSecPro Trainer Evaluation Form**

**Thank you for answering this survey!**

**Data Protection:** By submitting this survey, you agree to the collection of your anonymous responses and technical data (IP address, browser information) for research and evaluation purposes. Read our full Data Protection Notice.

**Section 1: Introduction**

Overall, how satisfied are you with the effectiveness and efficiency of designing a training based on CSP training materials?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

Overall, how satisfied are you with the implementation of the CSP training module?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Section 2: Course content and structure**

Based on your experience with this course, how satisfied are you as a trainer with the adaptability of the CSP training materials to fulfil the needs of your learners?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

How practically relevant do you think the training materials were for your learners in the training you offered?

- Not Relevant at All
- Low Relevant
- Slightly Relevant
- Somewhat Relevant
- Moderately Relevant
- Very Relevant
- Extremely Relevant

**Section 3: Learner's experience**

To what extent did learners effectively engage with the course materials and activities?

- Not at All
- To a Very Small Extent
- To a Small Extent
- To a Moderate Extent
- To a Fairly Large Extent
- To a Large Extent
- To a Very Large Extent

How many of your trainees do you think put in sufficient effort in this module to succeed?

- No student
- Few trainees
- Some trainees
- About half of them
- Many trainees
- Most trainees
- All students

Do you think the trainees had a chance to practice what they were learning and received sufficient feedback during the training module?.....

Do you have any suggestions that could improve this?

To what extent did learners demonstrate understanding and application of the concepts during the training?

- Not at All
- To a Very Small Extent
- To a Small Extent
- To a Moderate Extent
- To a Fairly Large Extent
- To a Large Extent
- To a Very Large Extent

**Section 4: Learning Platform (optional)**

How satisfied are you with the performance and reliability of the platform (e.g. no errors and quick loading times) from the trainer's perspective?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

How satisfied are you with the ease of navigation of the learning platform?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

How satisfied are you with the interactivity of & engagement opportunities on the platform (e.g., quizzes, discussion forums, gamification)?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Section 5: Community / Interaction (optional)**

How satisfied are you with the ability of the CSP training materials to facilitate interaction between you and the learners?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied

- Very Satisfied

How satisfied are you with the ability of the CSP training materials to facilitate interaction among participants?

- Strongly Dissatisfied
- Dissatisfied
- Somewhat Dissatisfied
- Neutral
- Somewhat Satisfied
- Satisfied
- Very Satisfied

**Section 6: Impact on students**

To what extent do you think this course enhanced the knowledge and skills of students?

- Not at All
- To a Very Small Extent
- To a Small Extent
- To a Moderate Extent
- To a Fairly Large Extent
- To a Large Extent
- To a Very Large Extent

**Section 7: Recommendation**

How likely are you to recommend other cybersecurity trainers to use CSP training material for their trainings? 0 - Not at all likely 1 2 3 4 5 6 7 8 9 10 - Extremely likely

How likely are you to host future trainings based on the CSP training materials?

- Extremel Unlikely
- Unlikely
- SlightlyUnlikely
- Neutral
- Slightly Likely
- Likely
- Extremely Likely

How could the CSP training materials be improved? (Please provide at least 2-3 sentences) …….

What aspects of the course delivery could be revised in future implementations? (Please provide at least 2-3 sentences) …… ……

Any further comments you like to share: …….

# Additional CyberSecPro Evaluation Template

**Additional CyberSecPro Training Module Evaluation Template: Enrolled learner**

What is your age?

- Under 18
- 18- 25
- 26-34
- 35-45
- 45+-54
- 55-65
- More than 65

What is your gender?

- Male
- Female
- Non-Binary
- Prefer not to answer

What is the highest level of education you have completed?

- Less than high school
- High school
- Diploma or equivalent
- Some college, no degree
- Undergraduate degree (Bachelor's)
- Master's degree
- Doctoral (PhD)
- Other

What is your Country of origin (the country where you were born)? _____

If you agree to being contacted in the future to follow up on your progress, could you please provide your email address? _____

Please indicate if you belong to any of the following categories (you may select more than one):

- Student
- Academic personal
- Employer
- Employee
- Practitioner
- Developer
- Officer
- In education or a recent graduate not yet employed (either in formal secondary or tertiary education or a recent graduate (graduation not more than one year ago))
- Unemployed, inactive and not a recent graduate

Are you an ICT graduate? Yes No
Are you self-trained in cybersecurity without any formal training in Cybersecurity topic? Yes No
Have you successfully completed this educational program/training activities? Yes No

**Additional CyberSecPro Training Module Evaluation Template: Enrolled learner who agreed to being contacted in the future to follow up on their progress**

1.What is your gender?

- Male
- Female
- Non-Binary
- Prefer not to answer

2.Have you carried out a job-placement/internship? Yes No
3.If yes, please indicate in which company? _____
4.Have you experienced an improvement in your employment situation since completing the training supported by the program? Yes No
5.Which of the following best describes your change of situation after completing the educational programme/training activities/job placement?

- You were in education or a recent graduate/ not yet employed before educational programme/training activities/job placement and found a job after completing the educational programme/training activities/job placement (This includes partial or full employment, self-employment or similar)
- You were unemployed or inactive before educational programme/training activities/job placement and found a job after completing the educational programme/training activities/job placement (This includes partial or full employment, self-employment or similar)
- You were employed before educational programme/training activities/job placement and improved your employment situation after completing the educational programme/training activities/job placement (This includes transit from precarious to stable employment or from underemployment to full employment or transit to a job requiring higher competences/skills/qualifications and/or more responsibilities or a promotion to a higher-level job)
- Other

6.Have you participated virtually in a full online course and completed it? Yes No
7.If the answer of question 6 is yes, have you received certification after the successful completion of the full online course? Yes No
8.If yes, please answer the following questions:
What is your age?

- Under 18
- 18- 25
- 26-34
- 35-44
- 45+-54
- 55-65
- More than 65

What is the highest level of education you have completed?

- Less than high school
- High school
- Diploma or equivalent
- Some college, no degree
- Undergraduate degree (Bachelor's)
- Master's degree
- Doctoral (PhD)

- Other

What is your Country of origin (the country where you were born)? _____

**Only apply for Big CSP training activities: Collected from the applicants**

What is your age?

- Under 18
- 18- 25
- 26-34
- 35-44
- 45-54
- 55-65
- More than 65

What is your gender?

- Male
- Female
- Non-Binary
- Prefer not to answer

What is the highest level of education you have completed?

- Less than high school
- High school
- Diploma or equivalent
- Some college, no degree
- Undergraduate degree (Bachelor's)
- Master's degree
- Doctoral (PhD)
- Other

What is your Country of origin (the country where you were born)? _____