Project No. 101083594
Call: DIGITAL-2021-SKILLS-01

Project start: 2022-12-01
Project duration: 39 months

CyberSecPro

D4.2
Reports and Training Material on the Cybersecurity Principles and Management Training Modules

Document Identification	
Due date	2026-02-28
Submission date	2026-02-27
Version	1.21

Related WP	WP4	Dissemination Level	PU
Lead Participant	GUF	Lead Author	Atiyeh Sadeghi, Kai Rannenberg (GUF)
Contributing Participants	ACEEU, SINTEF, UMA	Related Deliverables	D2.2, D.2.3, D3.1, D3.3, D3.4, D3.5, D4.1, D4.3 D4.4, D4.5, D5.1, D5.2, D5.3

Abstract: This deliverable presents the outcomes of T4.3 up to the conclusion of CyberSecPro in Month 39 (February 2026). Hence, it comprehensively records all CSP modules corresponding to the capability category Cybersecurity Principle and Management implemented by the end of February 2026. The document presents quantitative information on hosting site, learners enrolled, background of learners, evaluation forms of learners, evaluation forms of trainers, income, scholarship/sponsorships, training levels, delivery formats, and sectoral coverage across energy, health, maritime, and general cybersecurity domains. The deliverable includes descriptive analysis of training deployment, illustrating implementation patterns and participation across different module categories and sectors. Moreover, it describes the context of the documentation task and the documentation methodology including the definition of a record comprising the relevant information per module.

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 outcomes of Task T4.3 “Operating the training modules on Cybersecurity Principles and Management” up to the conclusion of CyberSecPro in Month 39 (February 2026). It documents all CSP modules corresponding to the capability category “Cybersecurity Principle and Management” implemented by the end of February 2026.
The document reports on the delivery of CSP001 “Cybersecurity Essentials and Management”, CSP002 “Human Factors and Cybersecurity”, CSP005 “Data Protection and Privacy Technologies”, CSP003 “Cybersecurity Risk Management and Governance” (partially by T4.3 and this deliverable, D4.2, partially by T4.4 and D4.3) modules, providing an evidence-based overview of training activities carried out during the reporting period. Moreover, it describes the context of the documentation task and the documentation methodology including the definition of a record comprising the relevant information per module.
In order to develop D4.2, we followed the process specified below:

- We used the template for describing CSP modules from D4.1 and added the additional elements for the purposes of D4.2, i.e. the documentation of implemented CSP modules, KPIs related to project and European Commission requirements from the call for proposal[1] as well as European Commission (EC) requirements and reviewer feedback following the first periodic review.
- We then documented the CSP modules covering the Cybersecurity Principles and Management capability and implemented by M39. For this documentation we used the the online tool[2] developed by ACEEU.

A total of 47 CSP modules were implemented across multiple sectors, including energy, health, maritime, and general, and delivered at both basic and advanced levels. The modules were offered through different formats, such as seminars, workshops, courses, and cybersecurity exercise, and involved a wide range of academic, research, and industrial providers. Enrolment data indicate strong engagement across all module categories.

[1]https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2021/call-fiche_digital-2021-skills-01_en.pdf

[2] https://admin.cybersecpro-project.eu/implementedmodules/listimplementedmodules

Document information

Contributors

Name	Beneficiary
Atiyeh Sadeghi, Kai Rannenberg	GUF
Thorsten Kliewe, Jeldo Meppen	ACEEU
Nektaria Kaloudi	SINTEF
Cristina Alcaraz	UMA

Reviewers

Name	Beneficiary
Javier Lopez, Cristina Alcaraz	UMA
Sebastian Pape	SEA
Danijela Boberic Krsticev	UNSPMF
Jeldo Meppen	ACEEU (as QM)

History

Version	Date	Contributor(s)	Comment(s)
0.01	2023-11-13	Kai Rannenberg, Atiyeh Sadeghi	1st Draft of ToC
0.02	2023-11-17	Kai Rannenberg, Atiyeh Sadeghi	Improved ToC reflecting comments and feedback from partners
0.03	2023-12-07	Kai Rannenberg, Atiyeh Sadeghi	Update on Section 2
0.04	2023-12-20	Vasco Delgado-Gomes, Kai Rannenberg, Atiyeh Sadeghi	WP3-WP4 Alignment template
0.05	2024-01-09	Nineta Polemi, Christos Douligeris	High-level review
0.06	2024-01-11	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on high-level review comments
0.07	2024-02-08	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on the 1st review comments
0.08	2024-02-22	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on the 2nd review comments
0.09	2024-03-01	Kai Rannenberg, Atiyeh Sadeghi	Further improvement, especially based on a re-review of the KPIs in the GA
1.0	2024-03-07	Atiyeh Sadeghi	Final check, layout refinement and submission process
1.1	2025-06-10	Atiyeh Sadeghi	Update ToC
1.2	2025-11-17	Atiyeh Sadeghi	Update ToC
1.3	2025-12-08	Kai Rannenberg, Atiyeh Sadeghi	Further improvement on ToC
1.4	2025-12-28	Atiyeh Sadeghi	Providing Annex D
1.5	2025-12-30	Atiyeh Sadeghi	Providing section 4
1.6	2025-12-31	Atiyeh Sadeghi	Further improvement
1.7	2026-01-02	Kai Rannenberg, Atiyeh Sadeghi	Further improvement

1.8	2026-01-12	Atiyeh Sadeghi	Further improvement based on PSTM feedback
1.9	2026-01-13	Atiyeh Sadeghi	Further improvement for first review
1.10	2026-01-26	Sebastian Pape, Cristina Alcaraz, Danijela Boberic Krsticev, Jeldo Meppen	First review feedback
1.11	2026-01-28	Atiyeh Sadeghi	Applied first review feedbacks and further improvement
1.12	2026-01-30	Kai Rannenberg, Atiyeh Sadeghi	Further improvement based on reviewer feedback
1.13	2026-02-03	Atiyeh Sadeghi	Further improvement for the second review
1.14	2026-02-04	Danijela Boberic Krsticev, Sebastian Pape, Cristina Alcaraz	Second review feedback
1.15	2026-02-06	Atiyeh Sadeghi	Applied second review feedbacks and further improvement
1.16	2026-02-13	Kai Rannenberg, Atiyeh Sadeghi	Further improvement
1.17	2026-02-13	Nektaria Kaloudi	Provide input on MOOCs
1.18	2026-02-15	Kai Rannenberg, Atiyeh Sadeghi	Further improvement
1.19	2026-02-20	Atiyeh Sadeghi	Further improvement
1.20	2026-02-21	Atiyeh Sadeghi	Further improvement in section 4
1.21	2026-02-24	Atiyeh Sadeghi	Applied High Level review feedback and prepared for submission

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
	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
	DCM	Dynamic Curriculum Management
E	**EC**	European Commission
	ECSF	European Cybersecurity Skills Framework
F	**FCT**	Universidade NOVA de Lisboa (NOVA University of Lisbon)
	FP	Focal Point
	FTPS	File Transfer Protocol Secure
G	**GUF**	Johann Wolfgang Goethe-Universitaet Frankfurt am Main (Goethe University Frankfurt)
H	**H**	Hackathon
	HEIs	Higher Education Institutions
I	**IMT**	Institut Mines-Telecom
	ITML	Information Technology for Market Leadership
K	**KA**	Knowledge Area
L	**LAU**	Laurea-Ammattikorkeakoulu Oy (Laurea University of Applied Sciences)
M	**MAG**	Maggioli Spa
O	**O**	Other
P	**PDMFC**	Pdm e fc Projecto Desenvolvimento Manutencao Formacao e Consultadorialda
S	**S**	Seminar
	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	**T**	Task
	TalTech	Tallinna Tehnikaülikool (Tallinn University of Technology)
	TRUSTILIO	trustilio B.V.
	TUBS	Technische Universität Braunschweig (Technical University of Braunschweig)
	TUC	Polytechneio Kritis (Technical University of Crete)
U	**UCY**	University of Cyprus
	UMA	Universidad de Malaga (University of Malaga)

	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	**W**	Workshop
	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**

A summer school is 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

This deliverable presents the outcomes of Task T4.3 "Operating the training modules on Cybersecurity Principles and Management" up to the conclusion of CyberSecPro project in Month 39 (February 2026). It documents all CSP modules corresponding to the capability category "Cybersecurity Principle and Management" implemented by the end of February 2026.

The category "Cybersecurity Principles and Management" serves as the foundational module, providing basic knowledge and skills required for understanding cybersecurity in a comprehensive manner. This category encompasses human, organizational, and regulatory aspects, ensuring that learners gain a holistic perspective on the factors influencing cybersecurity. By covering basic subjects, it offers a broad understanding of cybersecurity principles and management, equipping learners with the knowledge and comprehension necessary to navigate both technical and managerial dimensions of the field.

This deliverable reports on the 47 implementations of the four training modules (CSP003 partially by T4.3 and this deliverable, D4.2, partially by T4.4 and D4.3) on Principles and Management developed within the CyberSecPro (CSP) project and covered by T4.3. Actually, this document reports on the delivery of CSP001 "Cybersecurity Essentials and Management", CSP002 "Human Factors and Cybersecurity", CSP005 "Data Protection and Privacy Technologies", and CSP003 "Cybersecurity Risk Management and Governance".

The module CSP003 "Cybersecurity Risk Management and Governance" is related to both Knowledge Area 3 (KA3) and Knowledge Area 4 (KA4) covering the capability category "cybersecurity tools and technologies" and "Cybersecurity Principles and Management", respectively. Therefore, the module CSP003 "Cybersecurity Risk Management and Governance" is covered partially by T4.3 and this deliverable, D4.2, partially by T4.4 and D4.3. T4.4 is responsible for operating the training modules on Cybersecurity tools. Documentation of the implemented CSP modules related to Knowledge Area 4 is covered in this deliverable, and documentation of the implemented CSP modules related to Knowledge Area 3 is covered in D4.3.

The document provides a consolidated overview of the implemented CSP modules, including the number of implemented modules, learners' 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 Background

Cybersecurity will persist be as a major issue in the foreseeable future for organisations and industries across all sectors: Due to the massive digitalisation of all aspects of business life, increasing shortage of skilled professionals capable of fulfilling specific roles and duties within cybersecurity could be foreseen. It is crucially important to provide comprehensive training for the next generation of professionals in order to effectively address the demanding and continually expanding cybersecurity landscape. By bridging the gap between academia and industry, CyberSecPro aims for improved education and training in cybersecurity, supporting a safer and more secure future for all.

Hence, the CyberSecPro project aims to introduce a distinctive professional training program featuring cutting-edge hands-on training modules. These modules are to cater to diverse training requirements and proficiency levels, encompassing both general and sector-specific modules for sectors such as maritime, health, and energy industries.

1.2 Purpose and Scope

This deliverable is produced within the context of CyberSecPro Work Package 4, titled "Operating CyberSecPro Professional Training Program". Its high-level objective is to establish the documentation for each CSP module offer. This deliverable document the implemented CSP modules managed by T4.3, which are the modules on Cybersecurity Principles and Management capabilities (CSP003 partially by T4.3 and T4.4 due to the overlap with the capabilities on cybersecurity tools and technologies).

Through the documenting of implemented CSP modules, this deliverable directly reports on several WP4 objectives, including:

- the execution of scalable CyberSecPro training offerings,

- the engagement and training of external participants from diverse industries and sectors in different level,
- the provision of training modules aligned with the CyberSecPro capability areas, in particular Cybersecurity Principles and Management,
- the collection of qualitative feedback from training providers to support continuous improvement.

To carry the goal of this deliverable and document all implemented CSP modules, an online tool developed by ACEEU, known as the Admin Portal, was established. This portal enables implemented CSP module providers to enter, update, and manage documentation for implemented CSP modules.

The scope of this deliverable is documenting and analysis of all implemented modules under T4.3. It includes a structured overview of all implemented modules, quantitative data on the number of implemented modules and learners, and descriptive analysis of training deployment by module code, training level, module type, and industry sector. In addition, the deliverable document all information on management and logistical aspects of implemented modules such as actions to attract learners, income, scholarship and sponsorship, registration process, prerequisites and admission criteria, tangible reward to learner, learning outcome, number of job-placement/internship, background of learner, hosting site and evaluation form of learners and trainers.

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.

1.3 Relation to other Work Packages and Deliverables

The primary objective of Work Package 4 "Operating CyberSecPro Professional Training Program" is to plan in detail the scalable offering and the operation of the CyberSecPro modules. This WP interacted with the other CyberSecPro work packages as follows: it received content-oriented information (e.g., knowledge areas) from WP2 and syllabus-oriented information from WP3. In turn, WP4 delivered information to WP3 about the templates to describe implemented CyberSecPro modules. WP4 implemented CSP modules as well as provided the template for the follow-up questionares for WP5 and WP5 in return, conduceted analysis of the evaluation forms filled by learners and trainers, as well as a compilation of best practices from the implemented CSP modules.

This deliverable is related to D2.2 (related to CSP training supply), D2.3 (related to CSP knowledge areas), D3.1 (including logistics, syllabus aspects of the templates and final CSP module design), D3.3, D3.4, D3.5 (provide the syllabus structure and detailed syllabus specifications for sector-specific CSP training module), D4.1 (including originally planned supply of modules in the CSP knowledge areas), D4.3, D4.4, D4.5 (on synchronization structure of deliverables and template for the implemented CSP modules) D5.1, D5.2 (on evaluation forms and support the identification and documentation of best practices in teaching cybersecurity), D5.3 (on certification schemes).

1.4 Structure of the Deliverable

The deliverable is organized as follows:

Section 1 introduces the context of the CyberSecPro training activities on "Cybersecurity Principles and Management", outlines the purpose and scope of the deliverable, and describes its relation to other work packages and deliverables.

Section 2 explains the overall methodological approach. Subsection 2.1, describes the process of data collection and Subsection 2.2, explains data collection support by Admin Portal for reports by module implementation provides.

Section 3, subsection 3.1 provides a brief overview of the CSP modules that are relevant to "Cybersecurity Principles and Management", thereby aligning with T4.3. In addition, Subsection 3.2 provide a brief overview of implemented modules on "Cybersecurity Principles and Management" implemented by M39, including key information such as module codes and titles, implementation periods, training levels, module implementation providers, sectoral focus, and the number of learners.

Section 4 provides structure, implementation, and outcomes of CSP modules which is included in two subsections. Subsection 3.1 provides statistics from all CSP modules implemented under T4.3. It includes a set of descriptive statistics and visualizations illustrating the distribution of modules and learners by module code, training level, module type, and industry sector. Subsection 3.2, includes information on management and logistical aspects such as actions to attract learners, income, scholarship and sponsorship, registration, prerequisites and admission criteria, tangible reward to learners, learning outcome, number of job-placement/internship, background of learners, hosting site and evaluation form of learners and trainers.

Section 5 provides the description and syllabus tables of two CSP-related MOOCs associated with Task T4.3: "CyberSecPro: Cybersecurity Fundamentals" and "Human Factors of Cybersecurity".

Section 6 concludes the document 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. In Annex B: Template for Planning the Offering of CSP Modules, reference is made to the template for offering CSP modules as provided in D3.1. Annex C: Reporting Method(s) introduces the reason of using Admin Portal as a method for documenting implemented CSP Modules. Finally, Annex D: CyberSecPro Evaluation Forms provides all CyberSecPro evaluation forms which had provided and analysed in WP5. Annex E: illustrates some additional statistics of the implemented CSP modules.

2. Methodology

2.1Subsection 2.1 describes the approach adopted to collect and document the implemented CSP modules and outline the specific information documented. Subsection 2.2 describes data collection support by portal for reports by module implementation provides.

2.1 Data Collection Procedure

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

- First, the development of the template was based on the existing template for describing CSP modules provided in D4.1, ensuring continuity with earlier project outputs while extending its scope to cover implementation-specific aspects.
- Additional elements required for the comprehensive documentation of implemented CSP modules were incorporated to capture implementation content, management and logistics, outcomes, financials and etc. that were not fully addressed in the original template, in line with the relevant work package and task descriptions.
- The template was aligned with the training module descriptions presented in D3.1 to ensure conceptual coherence across work packages and to facilitate comparability between planned training activities and their actual implementation.
- The template was implemented within the project's Admin Portal (see Subsection 2.1 for further details), enabling structured data entry, centralized documentation, and efficient access to information on implemented CSP modules.
- Subsequently, the KPIs specified in the call for proposal, as well as the SO4 Indicator 3, were integrated into the template in response to EC requirements. Also, to ensure adequate coverage of these KPIs and the SO4 indicator 3, an additional questionnaire was developed for CSP module implementation providers to collect the relevant data from CSP learners (see Annex D: CyberSecPro Evaluation Forms for further details).
- Following the Period 1 periodic report, reviewer and EC feedback also were integrated into the template.
- All these additional elements were updated on a regular basis in the Admin Portal and CSP module implementation providers are required to complete the template for the documentation of implemented CSP modules in the Admin Portal immediately upon completion of the implementation phase, thereby ensuring timely reporting, data accuracy, and effective monitoring. In addition, module implementation providers are expected to update the completed template whenever modifications or additional elements are introduced.

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

Figure 1: provides an overview of the entire process:

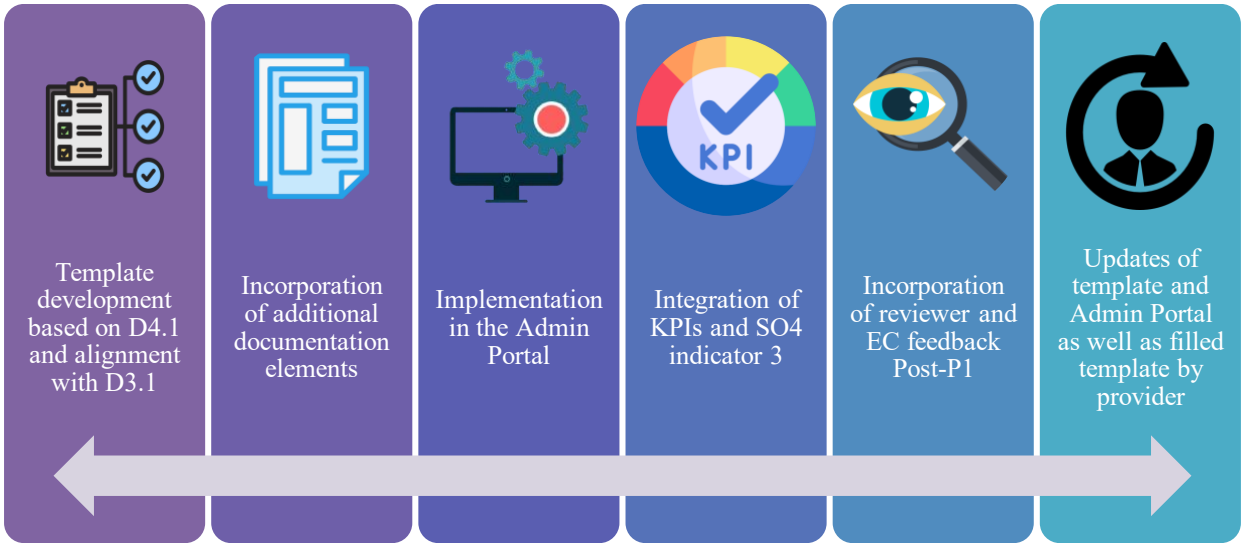


Figure 1: Data collection procedure

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

By extending the capabilities of the CyberSecPro internal Admin Portal (https://admin.cybersecpro-project.eu) and implementing the template described in Annex A: Template for the Documentation of Implemented CSP Modules for documenting implemented CSP modules, Admin Portal has been established that allows module implementation providers to complete the documentation template for the implemented modules as shown in Figure 2.

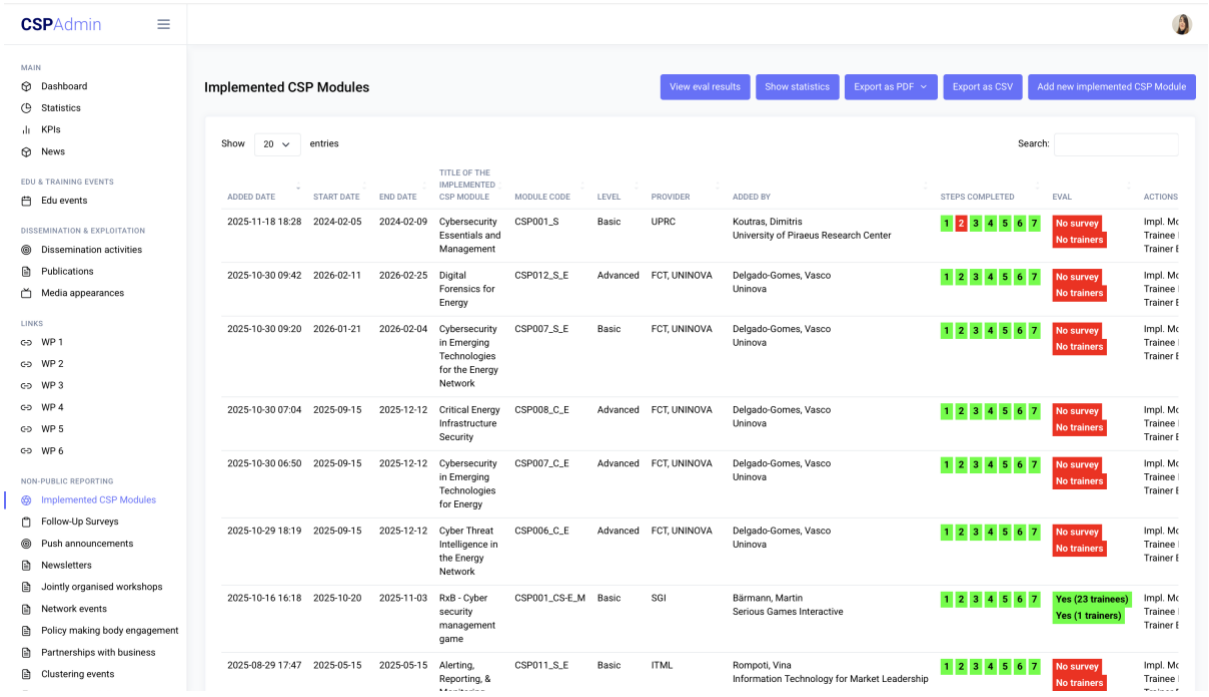
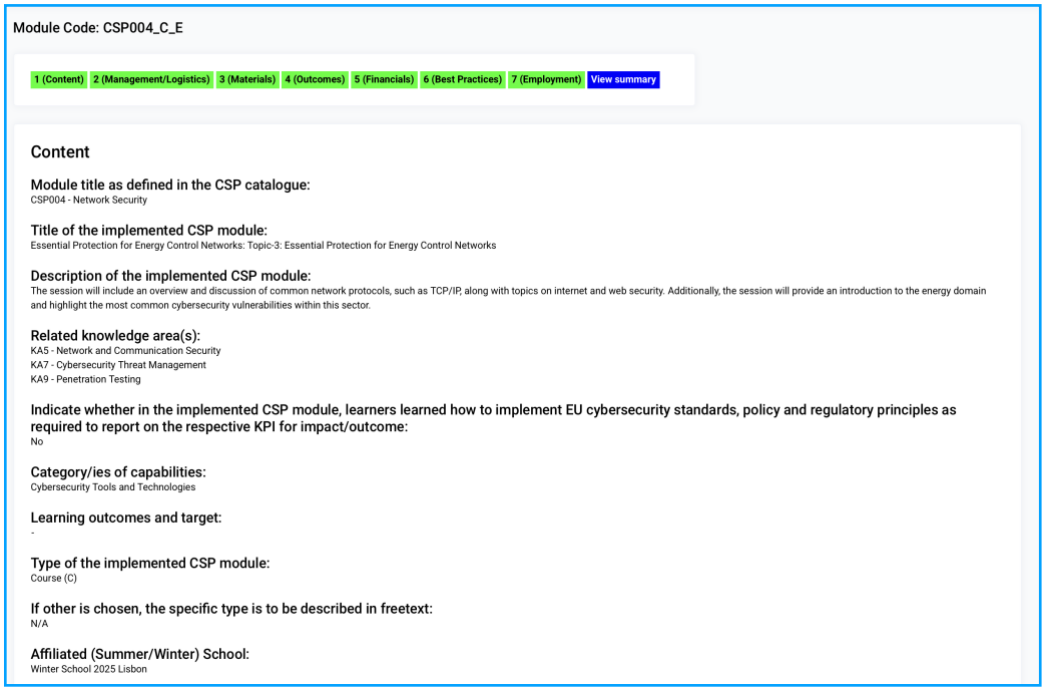


Figure 2: CyberSecPro Admin Portal

This platform, accessible via https://admin.cybersecpro-project.eu/implementedmodules/listimplementedmodules, enables authenticated module implementation providers to enter, update, and manage information pertaining to each implemented CSP module.

As illustrated in Figure 3: Screenshot of template for the documentation of implemented CSP modules, the final template consists of five tabs—content, management and logistics, outcomes, financials, best practices, and employment—with all fields detailed in Annex A: Template for the Documentation of Implemented CSP Modules.



Module Code: CSP004_C_E

1 (Content) 2 (Management/Logistics) 3 (Materials) 4 (Outcomes) 5 (Financials) 6 (Best Practices) 7 (Employment) View summary

Content

Module title as defined in the CSP catalogue:
CSP004 - Network Security

Title of the implemented CSP module:
Essential Protection for Energy Control Networks: Topic-3: Essential Protection for Energy Control Networks

Description of the implemented CSP module:
The session will include an overview and discussion of common network protocols, such as TCP/IP, along with topics on internet and web security. Additionally, the session will provide an introduction to the energy domain and highlight the most common cybersecurity vulnerabilities within this sector.

Related knowledge area(s):
KA5 - Network and Communication Security
KA7 - Cybersecurity Threat Management
KA9 - Penetration Testing

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:
No

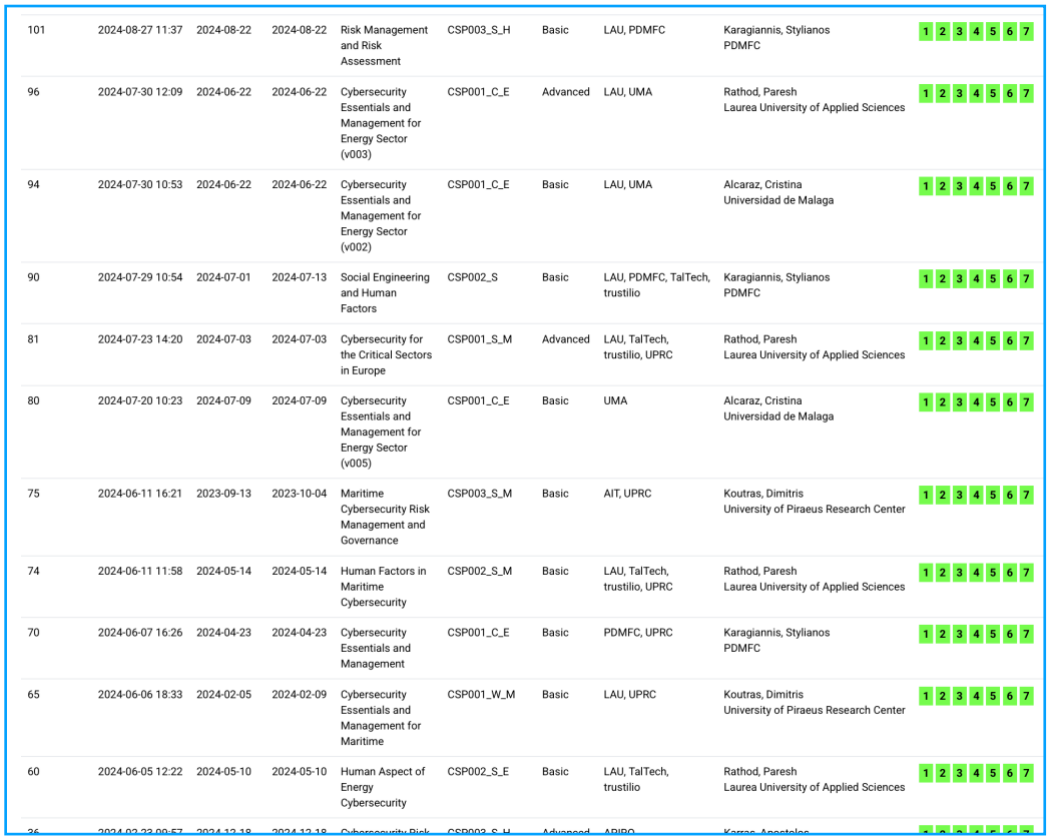
Category/ies of capabilities:
Cybersecurity Tools and Technologies

Learning outcomes and target:
-

Type of the implemented CSP module:
Course (C)

If other is chosen, the specific type is to be described in freetext:
N/A

Affiliated (Summer/Winter) School:
Winter School 2025 Lisbon



101	2024-08-27 11:37	2024-08-22	2024-08-22	Risk Management and Risk Assessment	CSP003_S_H	Basic	LAU, PDMFC	Karagiannis, Stylianos PDMFC	1 2 3 4 5 6 7
96	2024-07-30 12:09	2024-06-22	2024-06-22	Cybersecurity Essentials and Management for Energy Sector (v003)	CSP001_C_E	Advanced	LAU, UMA	Rathod, Paresh Laurea University of Applied Sciences	1 2 3 4 5 6 7
94	2024-07-30 10:53	2024-06-22	2024-06-22	Cybersecurity Essentials and Management for Energy Sector (v002)	CSP001_C_E	Basic	LAU, UMA	Alcaraz, Cristina Universidad de Malaga	1 2 3 4 5 6 7
90	2024-07-29 10:54	2024-07-01	2024-07-13	Social Engineering and Human Factors	CSP002_S	Basic	LAU, PDMFC, TalTech, trustilio	Karagiannis, Stylianos PDMFC	1 2 3 4 5 6 7
81	2024-07-23 14:20	2024-07-03	2024-07-03	Cybersecurity for the Critical Sectors in Europe	CSP001_S_M	Advanced	LAU, TalTech, trustilio, UPRC	Rathod, Paresh Laurea University of Applied Sciences	1 2 3 4 5 6 7
80	2024-07-20 10:23	2024-07-09	2024-07-09	Cybersecurity Essentials and Management for Energy Sector (v005)	CSP001_C_E	Basic	UMA	Alcaraz, Cristina Universidad de Malaga	1 2 3 4 5 6 7
75	2024-06-11 16:21	2023-09-13	2023-10-04	Maritime Cybersecurity Risk Management and Governance	CSP003_S_M	Basic	AIT, UPRC	Koutras, Dimitris University of Piraeus Research Center	1 2 3 4 5 6 7
74	2024-06-11 11:58	2024-05-14	2024-05-14	Human Factors in Maritime Cybersecurity	CSP002_S_M	Basic	LAU, TalTech, trustilio, UPRC	Rathod, Paresh Laurea University of Applied Sciences	1 2 3 4 5 6 7
70	2024-06-07 16:26	2024-04-23	2024-04-23	Cybersecurity Essentials and Management	CSP001_C_E	Basic	PDMFC, UPRC	Karagiannis, Stylianos PDMFC	1 2 3 4 5 6 7
65	2024-06-06 18:33	2024-02-05	2024-02-09	Cybersecurity Essentials and Management for Maritime	CSP001_W_M	Basic	LAU, UPRC	Koutras, Dimitris University of Piraeus Research Center	1 2 3 4 5 6 7
60	2024-06-05 12:22	2024-05-10	2024-05-10	Human Aspect of Energy Cybersecurity	CSP002_S_E	Basic	LAU, TalTech, trustilio	Rathod, Paresh Laurea University of Applied Sciences	1 2 3 4 5 6 7

Figure 3: Screenshot of template for the documentation of implemented CSP modules

Initially, we planned to have a full documentation of the implemented CSP modules in the DCM system; however, the DCM is designed to support teaching actions and that is why we decided to have another platform for documenting the implemented CSP modules (described in the Annex C: Reporting Method(s)), as it offers greater flexibility for trainers to report their outcomes than the DCM, which was needed for the flexibilty, as the KPIs and reporting duties changed several times mandated by the EC and the reviewer, and it was not clear whether and how often they would change again.

3. Implemented CSP Modules under T4.3

Subsection 3.1 describes CSP Modules related to "Cybersecurity Principles and Management" and its related Knowledge area. Subsection 3.2 provides key information on all implemented CSP modules, organized according to T4.3. It documents each implemented CSP module with its corresponding code and title, the implementation period indicated by the start and end dates, the level, the module implementation provider, and the corresponding sector. In addition, the number of learners is documented.

3.1 CSP Modules on Cybersecurity Principles and Management

This section briefly describe which CSP Modules are related to "Cybersecurity Principles and Management" and therefore to T4.3 titled "Operating the training modules on Cybersecurity Principles and Management". Based on Table 1, derived from D4.1, this task, T4.3, is responsible for the modules CSP001 "Cybersecurity Essentials and Management", CSP002 "Human Factors and Cybersecurity", and CSP005 "Data Protection and Privacy Technologies". As shown in Table 1, the module CSP003 "Cybersecurity Risk Management and Governance" is related to both Knowledge Area 3 (KA3) and Knowledge Area 4 (KA4) covering the capability category "cybersecurity tools and technologies" and "Cybersecurity Principles and Management",respectively. Therefore, the module CSP003 "Cybersecurity Risk Management and Governance" is covered partially by T4.3 and this deliverable, D4.2, partially by T4.4 and D4.3 (see more details below). T4.4 is responsible for operating the training modules on "Cybersecurity tools and Technologies". Documentation of the implemented CSP modules related to Knowledge Area 4 is covered in this deliverable, and documentation of the implemented CSP modules related to Knowledge Area 3 is covered in D4.3.

Table 1: The interrelation between CSP Knowledge Areas, capability category 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 CSP008 Critical Infrastructure Security CSP009 Software Security

CSP Knowledge Area 9 – Penetration Testing	Offensive Cybersecurity Practices	CSP010 Penetration Testing CSP011 Cyber Ranges and Operations
CSP Knowledge Area 10 – Cyber Incident Response	Offensive Cybersecurity Practices	CSP011 Cyber Ranges and Operations CSP012 Digital Forensics

* Cyan colour indicates the KAs covered by T4.3 and in this deliverable, D4.2.

CSP001 "Cybersecurity Essentials and Management"

This module is related to the CSP KA1: "Cybersecurity Management". This area delves into the principles and practices associated with the oversight of cybersecurity risks and programmes. Additionally, this module is related to the knowledge areas "Cybersecurity Management Systems, Cybersecurity Principles, and Cybersecurity Education and Training", among others.

CSP002 "Human Factors and Cybersecurity"

This module is related to the CSP KA2: "Human Aspects of Cybersecurity". This area explores the impact of human behaviour on cybersecurity and underscores the importance of security awareness training. Additionally, this general module is related to knowledge areas "Cybersecurity Education and Training, Soft and Transferable Skills", among others.

CSP003 "Cybersecurity Risk Management and Governance"

This module is related to the CSP KA3: "Cybersecurity Risk Management" and the CSP KA4: "Cybersecurity Policy, Process and Compliance". These areas involve recognising, evaluating, and mitigating cybersecurity risks, as well as the creation and implementation of cybersecurity policies and procedures and the management of cybersecurity compliance, respectively. Additionally, this module is related to the knowledge areas "Cybersecurity Risk Assessment and Management", "Cybersecurity Regulations and Compliance, Legal and Auditing Training", among others. This deliverable, D4.2, only covers the part related to CSP KA 4 (cf. Table 1).

CSP005 Data Protection and Privacy Technologies

This module is related to the CSP KA6: "Privacy and Data Protection". This area addresses the principles and strategies aimed at preserving the privacy and confidentiality of data. Additionally, this module is related to the knowledge area "Data Protection and Security", among others.

3.2 Overview of Implemented CSP Modules under T4.3

This subsection provides an overview of the key information of all implemented CSP modules, organized according to T4.3. Table 2: Overview of implemented CSP modules under T4.3 and further detail on Section 4 shows that the T4.3 requirements regarding the implementation of general and sector-specific training modules at two different levels in both EU HEIs and companies have been fully met, and the required number of learners has been completely fulfilled. Table 2 reports each CSP module with its corresponding code and title, the implementation period indicated by the start and end dates, the level, the module implementation provider, and the corresponding sector. In addition, the number of learners is documented.

In total, 47 implemented CSP modules related to Cybersecurity Principles and Management had been implemented during the reporting period. The modules were delivered at different proficiency levels (advanced and basic) and provided by a wide range of academic, research, and industrial partners, demonstrating strong collaboration within the CyberSecPro consortium.

Table 2: Overview of implemented CSP modules under T4.3

Module Code	Module Name	Start	End	Level	Provider	Industry Sector	Learner No
CSP001_C	Programming Foundations for CyberSecurity	25-01-14	25-05-11	B	LAU	General	33
CSP001_C_E	Cybersecurity Essentials and Management for Energy Sector (v001)	24-05-07	24-07-16	B	LAU, PDMFC, SGI, TalTech, trustilio, UMA	Energy	11
CSP001_C_E	Cybersecurity Essentials and Management	24-04-23	24-04-23	B	PDMFC, UPRC	Energy	20
CSP001_C_E	Cybersecurity Essentials and Management for Energy Sector (v005)	24-07-09	24-07-09	B	UMA	Energy	34
CSP001_C_E	Cybersecurity Essentials and Management for Energy Sector (v002)	24-06-22	24-06-22	B	LAU, UMA	Energy	22
CSP001_C_E	Cybersecurity Essentials and Management for Energy Sector (v003)	24-06-22	24-06-22	A	LAU, UMA	Energy	22
CSP001_C_E	Cybersecurity Essentials and Management for Energy Sector (v004)	25-01-20	25-01-20	B	UMA	Energy	55
CSP001_CS-E_E	RxB - Cyber security management game	24-05-28	25-10-01	B	SGI	Energy	34
CSP001_CS-E_H	RxB - Cyber security management game	24-05-28	25-10-01	B	SGI	Health	34
CSP001_CS-E_M	RxB - Cyber security management game	24-05-28	24-10-01	B	SGI	Maritime	34
CSP001_CS-E_M	RxB - Cyber security management game	25-10-20	25-11-03	B	SGI	Maritime	34
CSP001_S	Cybersecurity Essentials and Management	24-02-05	24-02-09	B	UPRC	General	50
CSP001_S_M	Cybersecurity for the Critical Sectors in Europe	24-07-03	24-07-03	A	LAU, TalTech, trustilio, UPRC	Maritime	34
CSP001_W	Foundations of Cybersecurity	25-07-14	25-07-14	B	PDMFC	General	41
CSP001_W_H	Cybersecurity Essentials and Management for Health Sector	25-03-13	25-03-13	B	UPRC	Health	72
CSP001_W_H	Cybersecurity Essentials and Management for Health Sector	25-03-11	25-03-11	B	UPRC	Health	200
CSP001_W_M	Cybersecurity Essentials and Management for Maritime	24-02-05	24-02-09	B	LAU, UPRC	Maritime	50
CSP002_CS-E_E	HATCH	25-05-30	25-05-30	B	SEA	Energy	18
CSP002_S	Social Engineering and Human Factors	24-07-01	24-07-13	B	LAU, PDMFC, TalTech, trustilio	General	34
CSP002_S	Communication in Cyber Incident Response	24-09-09	24-09-09	A	LAU, TalTech, trustilio, UPRC	General	27
CSP002_S	Human-AI Interactions in Cybersecurity	25-05-22	25-05-22	B	TalTech, trustilio	General	17
CSP002_S	Information and Deception	25-05-27	25-05-27	B	TalTech, trustilio	General	49
CSP002_S_E	Human Aspect of Energy Cybersecurity	24-05-10	24-05-10	B	LAU, TalTech, trustilio	Energy	10
CSP002_S_E	Human Factors and Cybersecurity Energy	24-08-23	24-08-23	B	LAU, TalTech, trustilio, UPRC	Energy	35
CSP002_S_H	Human Aspects of Cybersecurity	24-01-15	24-02-05	B	TalTech, trustilio	Health	40
CSP002_S_M	Human Factors in Maritime Cybersecurity	24-05-14	24-05-14	B	LAU, TalTech, trustilio, UPRC	Maritime	18
CSP002_S_M	Human Centric and Secure Maritime Ecosystems	24-05-15	24-05-16	B	trustilio	Maritime	30

Module Code	Module Name	Start	End	Level	Provider	Industry Sector	Learner No
CSP002_S_M	Human Aspects of Cybersecurity: Social Engineering, Personality, and Vulnerability	25-07-17	25-07-17	A	TalTech, trustilio	Maritime	41
CSP002_S_M	The weaponization of OSINT in Maritime	24-09-10	24-09-10	B	TalTech	Maritime	27
CSP002_S_M	Human Aspects of Maritime Cybersecurity	25-05-21	25-05-21	B	TalTech, trustilio	Maritime	17
CSP002_S_M	Hacking the Human	25-07-23	25-07-23	B	TalTech	Maritime	22
CSP002_W	Human Factors and Cybersecurity	25-05-27	25-05-27	B	LAU, TalTech	General	49
CSP003_S_E	Cybersecurity Risk Management and Governance in the Energy sector	24-12-17	24-12-17	A	APIRO, SLC	Energy	16
CSP003_S_E	Cybersecurity Risk Assessment and Management for Energy Sector	24-06-27	24-06-27	B	CNR, UMA	Energy	17
CSP003_S_E	Cybersecurity Risk Assessment and Management for Energy Sector	24-11-22	24-11-22	B	CNR, UMA	Energy	8
CSP003_S_E	Cybersecurity Risk Assessment and Management for Energy Sector (v003)	25-07-02	25-07-02	B	CNR, UMA	Energy	15
CSP003_S_E	Cybersecurity Risk Management and Governance in the Energy sector	25-07-30	25-07-30	A	APIRO	Energy	14
CSP003_S_H	Cybersecurity Risk Management and Governance in the Healthcare sector	24-12-18	24-12-18	A	APIRO	Health	11
CSP003_S_H	Cybersecurity Risk Management and Governance in the Healthcare sector	26-01-16	26-01-16	A	APIRO	Health	9
CSP003_S_M	Maritime Cybersecurity Risk Management and Governance	23-09-13	23-10-04	B	AIT, UPRC	Maritime	30
CSP005_S_E	Data Protection and Privacy Technologies for Energy	26-02-13	26-02-13	B	APIRO	Energy	14
CSP005_S_H	Data Protection and Privacy Technologies for healthcare.	24-09-09	24-09-09	B	ZELUS	Health	30
CSP005_S_M	Data Protection and Privacy Technologies for Maritime	25-01-22	25-01-22	B	MAG, SLC	Maritime	32
CSP005_W	Data Protection Impact Assessment	25-07-16	25-07-16	B	Ionian University	General	41
CSP005_W	Data Security and Anonymity	25-07-16	25-07-16	B	Lonian University	General	41
CSP005_W	An Introduction to Cryptography and Cryptocurrencies	25-07-18	25-07-18	B	KU Leuven	General	41
CSP005_W	Database Security	26-01-19	26-01-19	B	PDMFC	General	35

4. Structure, Implementation, and Outcomes of CSP Modules

This section provides an overview of the structure and outcomes of the implemented CSP modules. Subsection 4.1 presents statistics on implemented CSP modules under T4.3 (also including CSP003 modules related to T4.4 in order to provide a comprehensive picture of the implementation in CSP003). Subsection 4.2, summarizes the managerial and logical aspects of the implemented CSP modules. The outcomes align with the CyberSecPro strategy, which aimed to have at least one implementation for each CSP module in each sector, while beyond that responding to market demand (e.g. invitation) and supply conditions.

4.1 Statistics of Implemented CSP Modules

This subsection shows statistics of the implemented CSP modules under T4.3 (also including CSP003 modules related to T4.4 in order to provide a comprehensive picture of the implementation in CSP003). The presented figures illustrate key information of the implemented CSP modules, including the following subsections:

- 4.1.1 Number of implemented CSP modules per module code
- 4.1.2 Number of learners in implemented CSP modules per module code
- 4.1.3 Number of implemented CSP modules per module level
- 4.1.4 Number of implemented CSP modules per module level and code
- 4.1.5 Number of implemented CSP modules per module type
- 4.1.6 Number of implemented CSP modules per module type and code
- 4.1.7 Number of implemented CSP modules per module sector
- 4.1.8 Number of learners in implemented CSP modules per module sector
- 4.1.9 Number of implemented CSP modules per module code and sector
- 4.1.10 Number of implemented CSP modules per seasonal schools

These visualizations are to support a transparent and clear presentation of the implementation data, and indeed intermediate versions served as a basis for ongoing evaluations during the project execution.

4.1.1 Number of implemented CSP modules per module code

Figure 4 illustrates the number of implemented CSP modules by module code. CSP001 shows the highest level of implementation with 17 modules, followed by CSP002 with 15 modules. As CSP003 is related to two tasks, T4.3 and T4.4, its implementation figures are distinguished per task: Seven implemented modules related to T4.4 and eight implemented modules realted to T4.3 indicating almost balanced level of implementation across the two tasks. CSP005 has the lowest number of implemented modules, with a total of 7. The distribution shows an emphasis on CSP001, CSP002, and CSP003, which shows a strong demand for Cybersecurity essentials and management, as they are typical introductory courses. CSP005 implementation figures, while lower, still demonstrate substantial implementation of more advanced topics, contributing to a balanced coverage of different cybersecurity topics within the CyberSecPro framework.

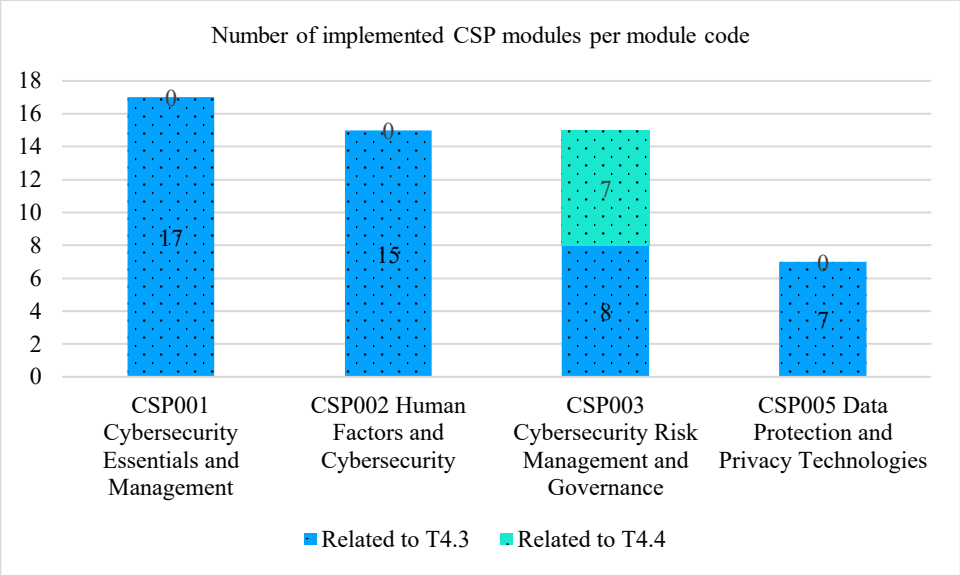


Figure 4: Number of implemented CSP modules per module code

4.1.2 Number of learners in implemented CSP modules per module code

Figure 5 illustrates the total number of learners across implemented CSP modules, grouped by module code. The data shows that following market demand and supply conditions the CSP001 module had the highest number of learners, with a total of 780 learners, followed by the CSP002 modules with 434 learners and CSP003 modules with 120 learners, while the CSP005 modules recorded 234 learners. Furthermore, the high volume of implemented modules provided a robust evidence base for the comprehensive evaluation conducted in WP5.

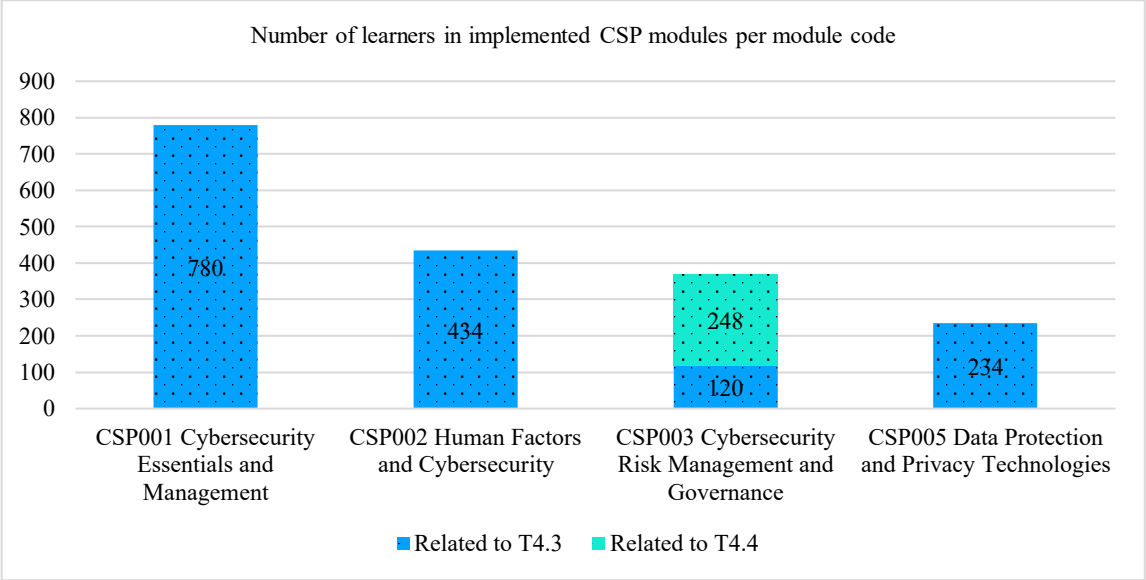


Figure 5: Number of learners in implemented CSP modules per module code

4.1.3 Number of implemented CSP modules per module level

Figure 6 shows the distribution of implemented CSP modules by training level. Following market demand and supply conditions, basic-level modules dominate the CSP implementation in T4.3, with 39 basic-level implementations compared to 8 implementations of advanced-level modules. When CSP003 modules related to T4.4 are included, the number of basic modules increases further to 45, while the number of advanced

modules rise slightly to 9. However, these results show a mixed level of implementation across training levels, with the distribution highlighting a strong demand for introductory and foundational modules in Cybersecurity Principles and Management. The results confirm that the CyberSecPro implemented CSP modules successfully engages learners at different stages of competency development.

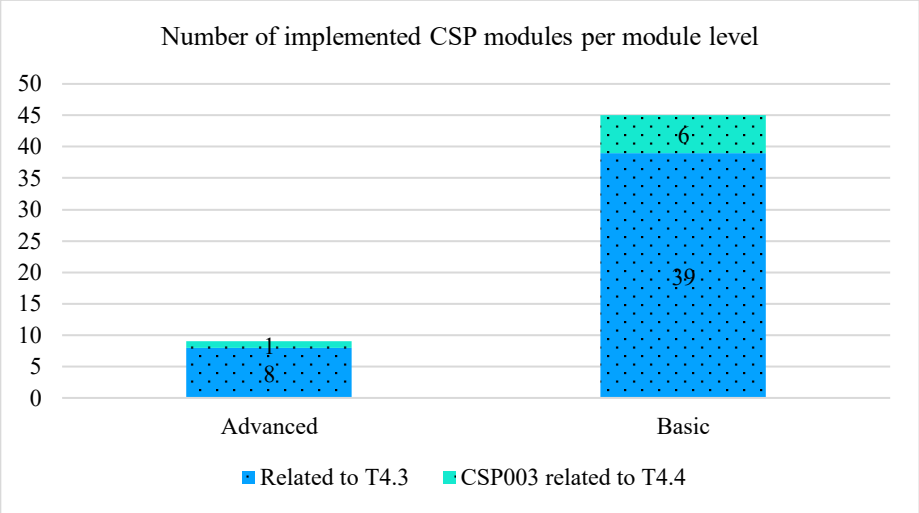


Figure 6: Number of implemented CSP modules per module level

4.1.4 Number of implemented CSP modules per module code and level

Figure 7 presents the distribution of implemented CSP modules by both module code and level. The results shows that CSP001 following market demand and supply conditions includes a total of 17 modules, the large majority of which are implemented at basic level (15 modules), with only a small number of implemented advanced modules (2) showing an emphasis on introductory and intermediate training within this CSP category. A similar pattern is visible for CSP002, which has 15 modules in total, comprising 13 basic and 2 advanced modules.

For CSP003 (related to T4.3), there are 8 implemented CSP modules, with indicating balanced implementation. In contrast, CSP003 related to T4.4 consists of 7 modules, but is more clearly oriented towards the basic level, with 6 basic and 1 advanced module. CSP005 includes 7 modules, all of which are implemented at the basic level, with no advanced modules implemented reflecting a stronger focus on basic topics within this CSP category.

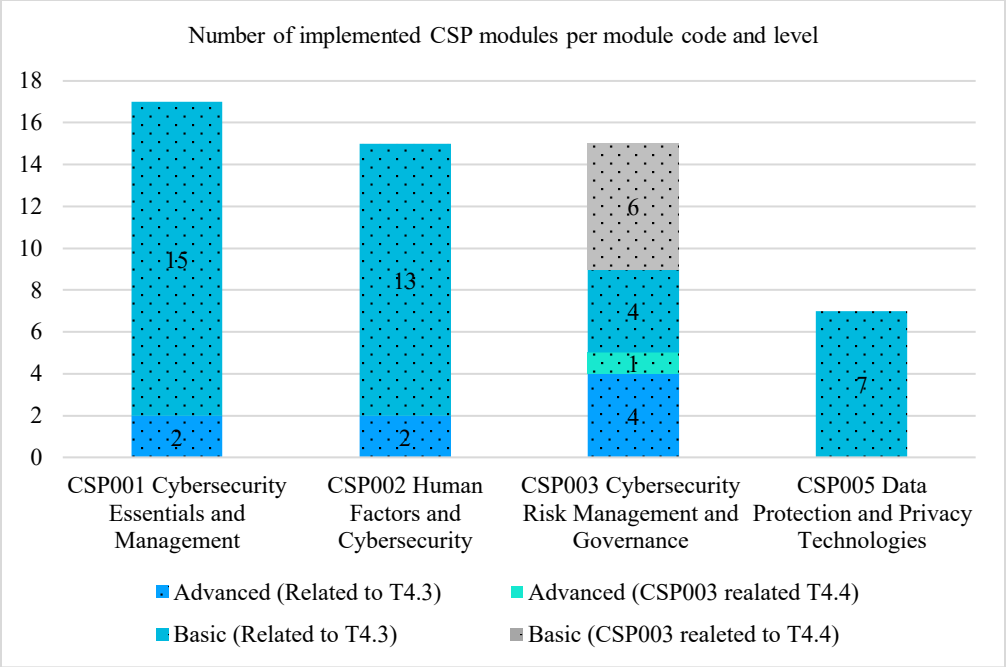


Figure 7: Number of implemented CSP modules per module code and level

4.1.5 Number of implemented CSP modules per module type

Figure 8 presents the distribution of implemented CSP modules by module type. Seminars constitute the largest share of implemented CSP modules, with a total of 26, followed by workshops with 9 modules and courses with 7 modules. When CSP003 (related to T4.4) is also taken into account, these numbers increase to 28 seminars, 13 workshops, and eight courses. Cybersecurity exercises account for a smaller portion, with 5 implemented modules, while no hackathons are shown in the data.

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

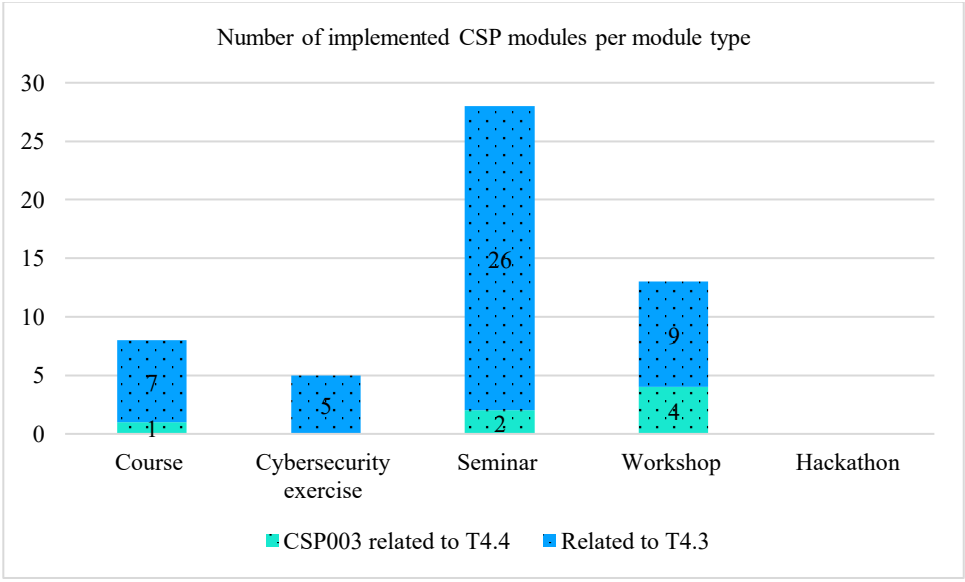


Figure 8: Number of implemented CSP modules per module type

4.1.6 Number of implemented CSP modules per module type and code

Figure 9 illustrates the distribution of implemented CSP modules by module type and module code. The results indicate that seminars dominate across CS0002 and CSP003 (related to T4.3). For CSP001, the implementation is relatively diverse, comprising 7 courses, 4 workshops, 2 seminars, and 4 cybersecurity exercises, reflecting a balanced combination of theoretical and hands-on training. For CSP002, seminars represent the largest share (13 out of 15 modules). CSP003 related to T4.3 is even more seminar-based, with all 8 implemented modules being seminars. In contrast, CSP003 related to T4.4 demonstrates a more varied structure, including 1 course, 4 workshops, and 2 seminars. CSP005 also consisting of 4 workshops and 3 seminars, with no courses and cybersecurity exercises. Overall, the distribution reinforces earlier findings regarding the prevalence of seminar-based modules while also highlighting variations in module type composition across different CSP category.

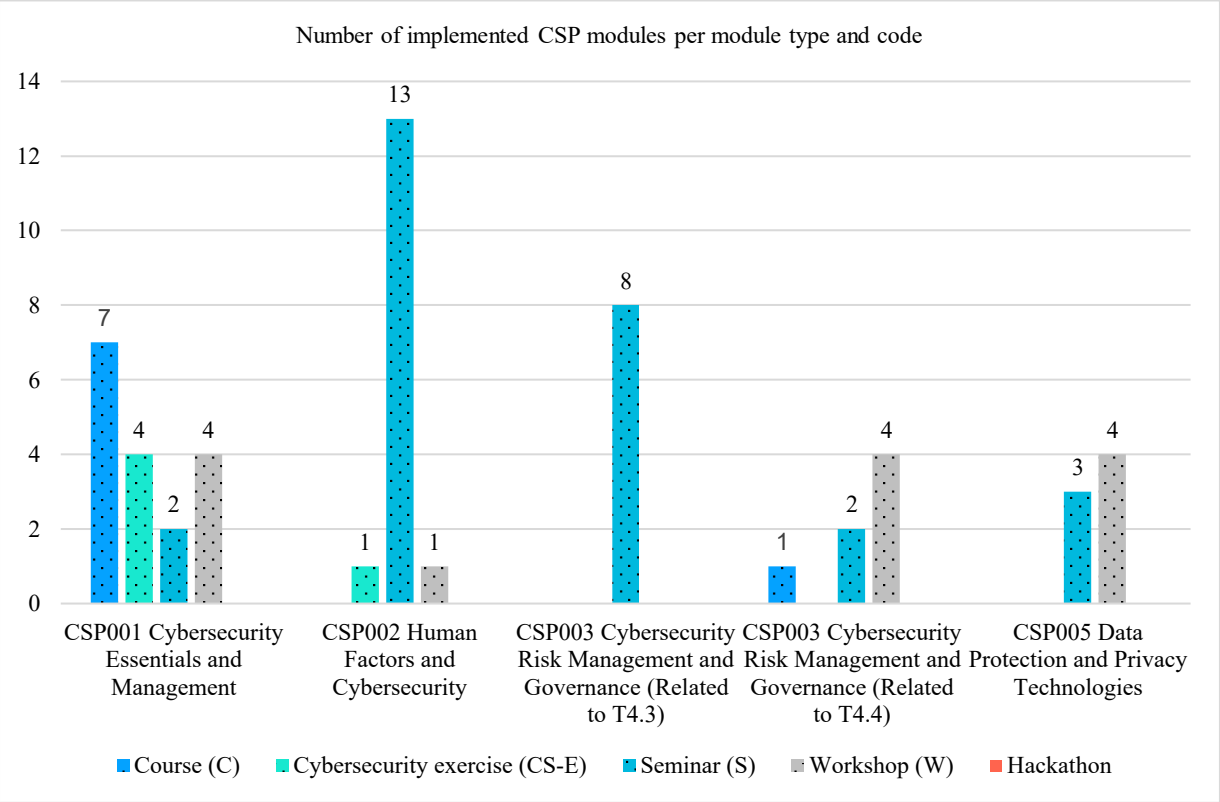


Figure 9: Number of implemented CSP modules per module type and code

4.1.7 Number of implemented CSP modules per module sector

Figure 10 shows the distribution of implemented CSP modules across industry sectors. The results indicate that the general and energy sectors account for the highest number of implemented modules, with 16 and 12 modules respectively, followed by the maritime sector (12). The health sector shows a smaller overall number of implementations, with a total of 7 modules.

In the energy and maritime sector, all modules are related to Task 4.3, whereas the general sector includes a combination of modules related to T4.3 (12 modules) and CSP003 in T4.4 (5 modules). The health sector modules include seven modules related to T4.3 and two modules related to CSP003 in T4.4.

This distribution confirms a strong focus of the CyberSecPro module implementation on energy and maritime, which are critical and highly regulated sectors with significant cybersecurity challenges. At the same time, the presence of general and health modules demonstrates a somewhat balanced sectoral coverage and supports cross-sectoral skill development. Interestingly the number of learners (see Figure 11) shows a slightly different picture.

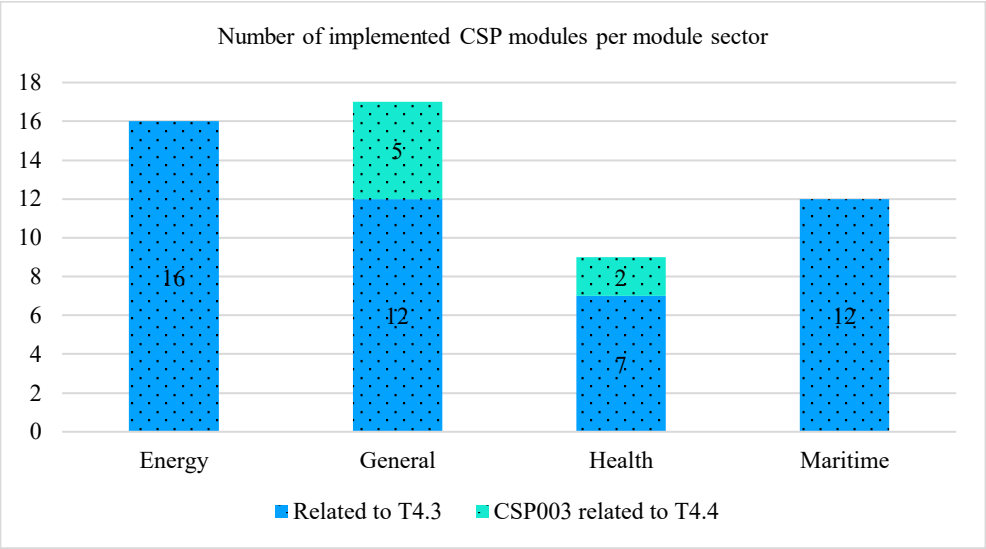


Figure 10: Number of implemented CSP modules per module sector

4.1.8 Number of learners in implemented CSP modules per module sector

Figure 11 presents the distribution of learners across CSP modules by industry sector. The results indicate that among sectors the health sector accounts for the highest number of learners (396) which when CSP003 (related to T4.4) is also taken into account, these numbers increase to 486 learners. The energy, maritime, show comparable levels of participation, with around 345 to 369 learners respectively. Also, the general modules account for 458 learners, increasing to 616 learners when CSP003 related to T4.4 is included.This distribution reflects strong learners' engagement in both cross-sectoral and sector-specific training activities and also shows that the fewer implemented modules in the health sector attracted a higher average number of learners.

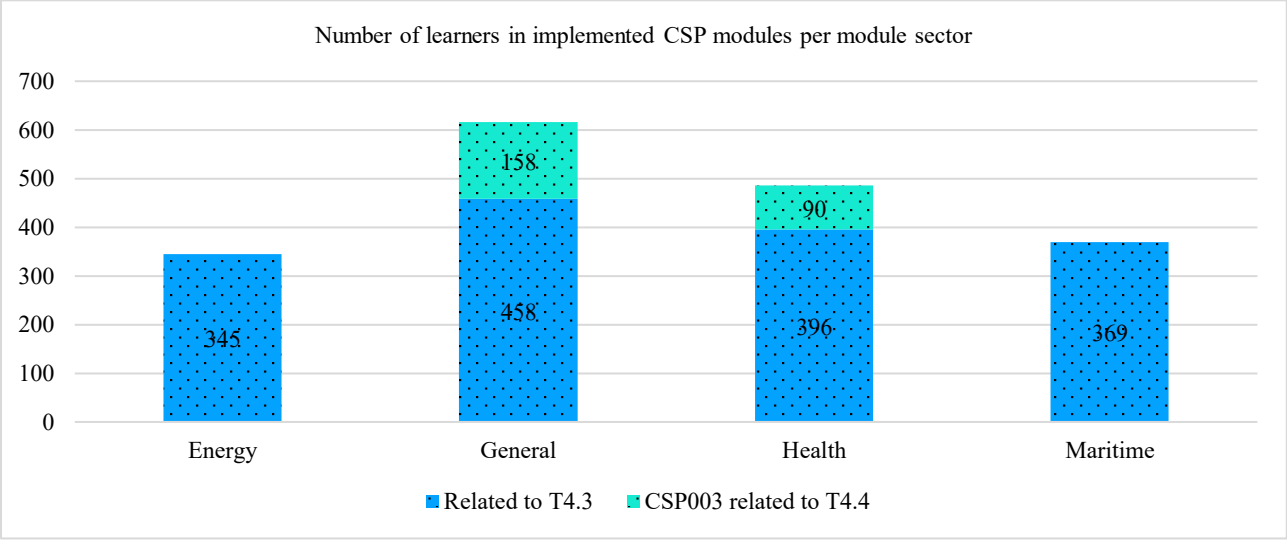


Figure 11: Number of learners in implemented CSP modules per module sector

4.1.9 Number of implemented CSP modules per module code and sector

Figure 12 presents the distribution of implemented CSP modules across industry sectors, grouped by module code. The results indicate distinct sectoral emphases for each CSP category.

CSP001 displays a broad sectoral coverage, with the highest number of modules in the energy sector (7), followed by maritime (4) and general modules (3), and health (3).

The majority of implemented modules of CSP002 are concentrated in the maritime sector (6 modules), alongside a substantial number of general modules (5) with limited representation in energy (3) and health sector (1). CSP003 related to T4.3 shows high number in the energy sector, accounting for 5 out of 8 modules, while health and maritime are minimally represented, and no general modules are included.

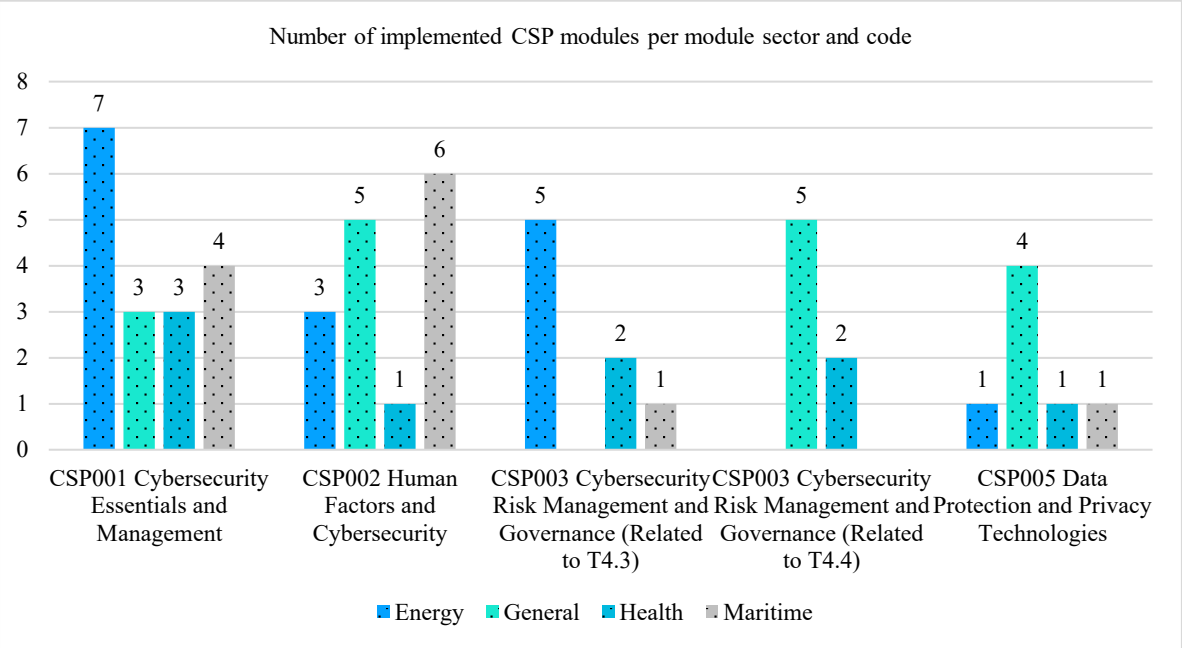


Figure 12: Number of implemented CSP modules per module sector and code

In contrast, CSP003 related to T4.4 is strongly oriented towards general topics, with 5 general modules, complemented by a small number of health modules (2) and no maritime or energy modules. CSP005 is consisting mainly of general modules (4), with one module each in health, maritime, and energy sector.

4.1.10 Number of implemented CSP modules per seasonal schools

Figure 13 shows the number of implemented CSP modules across different seasonal schools happened during CyberSecPro Project in T4.3 and CSP003 related to T4.4. Highest number observed during the Summer School 2025 in Novi Sad (Week 1). The figure shows that 31 independents modules in T4.3 and 3 independent modules in CSP003 related to T4.4 implemented.

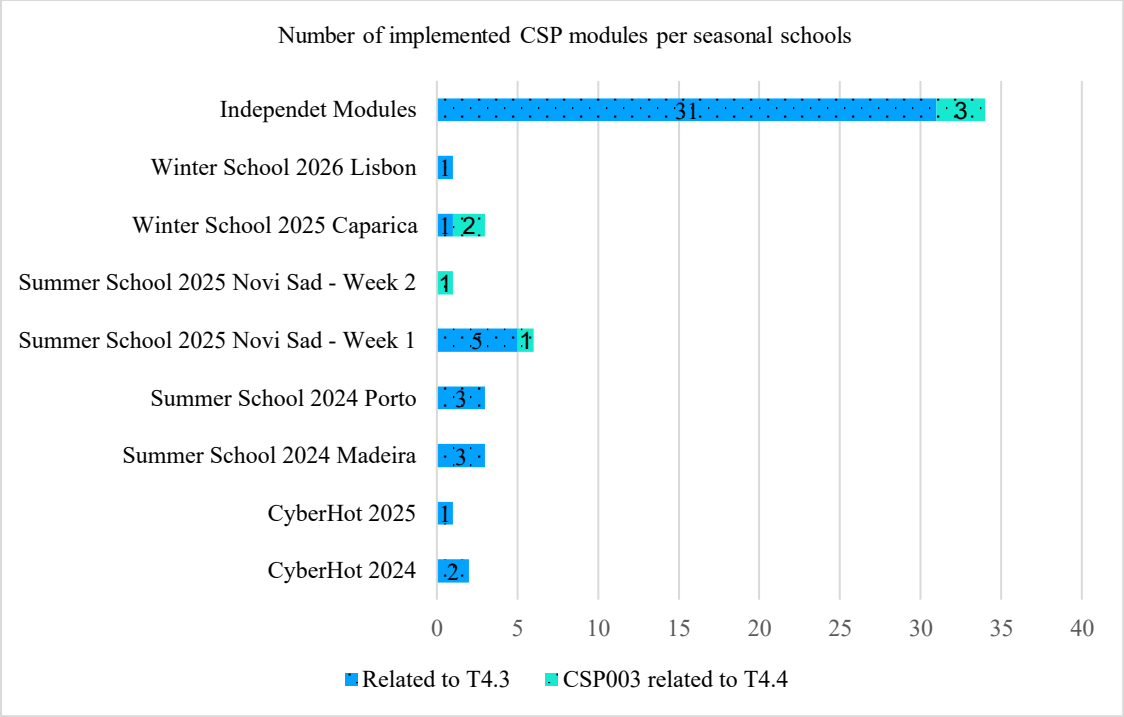


Figure 13: Number of implemented CSP modules per seasonal schools

4.2 Management and Logistical Aspects of CSP Implemented CSP Modules

This subsection includes information on management and logistical aspects as following:

- 4.2.1 Actions to attract learners
- 4.2.2 Income and scholarship/sponsorships
- 4.2.3 Registration process
- 4.2.4 Pre-requisites and Admission Criteria
- 4.2.5 Tangible rewards to learners
- 4.2.6 Learning Outcomes
- 0 Number of job-placements/internships carried out by the students
- 4.2.8 Background of the learners
- 4.2.9 Hosting sites
- 4.2.10 Evaluation forms of learners and trainers

4.2.1 Actions to attract learners

The actions adopted to attract learners classified into four categories, as described below:

1. Strategic Partnerships and Academic Integration:

This category includes actions that leverage institutional reputation and formal education structures.

- Aligning and contributing with reputed summer schools e.g. the IPICS Summer School,
- IPICS - Intensive Programme on Information and Communication Security had co-organized and prepared a CSP Winter School as a process step to establish a CSP event,
- Integrating CSP modules into exciting academic courses and programmes,
- Physical events that had remote participation component,
- Effort made by the HEI participants to attract their students,
- Winter School in Caparica 2025 invited private companies and public institutions to send their staff to the event,

- Encouraged Women participation by encouraging from the degree programmes.
- Student are also often disadvantage specially in some European countries like Serbia.

2. Promotion, Marketing and Communication

This category includes awareness-raising and targeted communication efforts.

- Enlighten target groups about the relation of the CSP modules to the actual market needs. Post messages in the dissemination channels (as shown in Figure 14) highlighting how the CSP modules (and the subsequent learning outcomes) address the needs identified from the market analysis (WP2),
- Use the CSP short videos in the promotion of CSP training offer for advertisement,
- Ensured all learners had the opportunity to access and view video teasers and training advertisements disseminated via various communication channels available to learners as well as Internal company Channels.

Figure 14: Post messages in the dissemination channel (CyberSecPro project LinkedIn and X/Twitter)

3. Financial Accessibility and Funding Support

This category focuses on reducing financial barriers and facilitating access.

- CyberSecPro organized different events, such as the IPICS 2024 and the CyberSecPro Cybersecurity Winter School 2025 and 2026 with very low fees to attract students. At IPICS 2024 the registration fee for 2 weeks including hotel room and lunches was €1000, and similar fees held for other events. This was achieved by finding sponsors for the events. In addition, CSP provided assistance to candidates on finding funding for the fees and travel expenses,

- Based on the list of Funding Programs collected by PDMFC each partner was asked to add entries relative to their own countries. The idea is to make it easier for us to help learners (and Trainers) to find funding to attend on events with CSP modules.

4. Flexible and Digital Access

This category relates to accessibility through online and hybrid formats.

- Maximized the potential of online learning, exploiting the capabilities of the DCM platform. Learners were able to join the DCM platform, even if they wanted to attend only a single course.

4.2.2 Income and scholarship/sponsorships

Regarding the income, there is mostly no income achieved from the implemented CSP module under T4.3 and seasonal schools, except for the below ones. APIRO has received the below amount from the National Standardization Organization as payment for for the provisionof training on the two modules listed below, which will be declared as income/ revenue in the final financial statement of the project according to article 22 of the GA.

- **CSP003_S_E:** Cybersecurity Risk Management and Governance in the Energy sector: 1.250 EUR
- **CSP003_S_H:** Cybersecurity Risk Management and Governance in the Healthcare sector, 1.250 EUR

However, in terms of the scholarship/sponsorships, Table 3 presents the scholarships and sponsorships awarded within the CyberSecPro project.
Cybersecro, 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: Scholarship/sponsorships provided in the CyberSecPro seasonal schools

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.
CyberHOT 2024 Piraeus	Projects :SecOPERA, Phoenix, Eddeless, Rewire, synapse, FAITH, CustodesNERO, THEMIS5.0, ReScale, 6GXell, CyberSecDome. Companies/Institutions: Technical University of Crete, University of Piraeus Research Center, Trustilio, Focal Point, Dienekes IKE.	CyberSecPro organizer (University of Piraeus) enabled 20 scholarships covering the admission-fee.

Seasonal schools	Sponsorship	Scholarship
Winter School 2025 Caparica	Some students supported through Erasmus fellowships and private company. Ten students from the University of Piraeus were supported through Erasmus funds. Five students from Laurea University were supported through Erasmus funds.	CyberSecPro organizers (PDMFC, FCT, COFAC) enabled 49 scholarships covering the admission-fee.
CyberHOT Week 2025 Crete	Projects: SecOPERA, Phoenix, Eddeless, Rewire, synapse, FAITH, CustodesNERO, THEMIS5.0, ReScale, 6GXell, CyberSecDome, Elastic, CyberSynchrony, Eudoros. Companies/Institutions: Technical University of Crete, University of Piraeus Research Center, Trustilio, Focal Point, Dienekes IKE. 2 students were supported by the French Erasmus programme.	CyberSecPro organizers (Technical University of Crete) enabled 9 scholarships covering the admission-fee and CyberSecPro organizers (University of Piraeus) enabled 4 scholarships covering the admission-fee. Also, there were lower admission fees for all students.
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	Seven Greek students used Erasmus funds. 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 identified:

1. **No registration:** Some courses did not require any registration, such as open modules that were freely accessible.
2. **CyberSecPro organizer registration:** Registration managed directly by the CyberSecPro consortium through dedicated registration pages. This applied mainly to the the seasonal schools, such as Summer School 2024 Madeira, Summer School 2024 Porto, CyberHOT 2024 Piraeus, Winter School 2025 Caparica, CyberHOT 2025 Crete, Summer School 2025-1 and 2 Novi Sad and Winter School January 2026 Lisbon. Table 4 presents a detailed overview of the registration process for CSP Seasonal Schools. Furthermore, Figure 15 presents screenshot from the registration pages of the from Winter school 2025 and Summer School 2025- 1 and 2 Novi Sad, highlighting key elements of the registration process. Additionally, some modules also registered via CyberSecPro DCM.

Table 4: Registration process of CSP seasonal schools

Seasonal schools	Registration process of CSP seasonal schools
Summer School 2024 Madeira	There were two types of registration fees: • Registration fee was €550 included CSP summer school Kit, all CSP Summer school sessions, coffee breaks, lunches, summer school social events • Registration fee was €1200 included CSP summer school + ICE conference Kit, all CSP summer school | ICE | DT summit sessions, coffee breaks, lunches, one paper on ICE IEEE/ITMC 2024, ICE IEEE/ITMC 2024 proceedings and all social events. The page is accessible via the following link: https://cybersecpro.digit-madeira.pt/#about
Summer School 2024 Porto (IPICS 2024)	There were three types of registration fees: • July 1st – 6th: Registration fee was €550 which included six day summer school lunches, social event and corresponding dinner, hotel room (double occupancy with breakfast) between June 30th and July 7th. • July 8th – 13th: Registration fee was €550 which included six day summer school lunches, social event and corresponding dinner, hotel room (double occupancy with breakfast) between July 7th and July 14th. • July 1st – 13th: Registration fee was €1000 which included twelve day summer school lunches, two social events and corresponding dinners, hotel room (double occupancy with breakfast) between June 30th and July 14th. The page is accessible via the following link: https://research.pdmfc.com/event/ipics-2024-summer-school-co-organized-by-csp-and-cyballiance/
CyberHOT 2024 Piraeus	Early registration was €135 until August 20th 2024 and Late registration was €185 - After August 20th, 2024 which included coffee breaks and lunch. A cancellation fee was €50. No cancellation was allowed after August 20th, 2024. If registrants could not attend, they would be able to transfer the registration to another person. The organizers reserved the right to cancel CyberHOT if there were fewer than 20 registrations, in which case there would be a full refund of solely the registration fee. Registration was through dedicated website by filling a form in and proceeding with the payment. The page is accessible via the following link: https://sites.google.com/cyberhot.eu/cyberhot2024/home
Winter School 2025 Caparica	The registration fee was €500, with an 80% discount for students. 49 scholarships covered the remaining 20% for students who successfully complete the program. Also, a refundable €20 reservation fee applied to the social dinner when learners attended the event. The page is accessible via the following link: https://research.pdmfc.com/event/winter-school-2025-cyber-security-winter-school/
CyberHOT 2025 Crete	General admission was for €400 and student admission was €300 which included coffee breaks and lunch. A cancellation fee was €50. No cancellation allowed after May 1st, 2025. If registrants could not attend, they would be able to transfer the registration to another person. The organizers reserved the right to cancel CyberHOT if there were fewer than 20 registrations, in which case there would be a full refund of solely the registration fee. Registration was through dedicated website by filling a form in and proceeding with the payment. The page is accessible via the following link: https://sites.google.com/cyberhot.eu/cyberhot2025
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	The early registration fee was €400 for one week or €750 for both weeks. This fee included accommodation in a double room, breakfast, lunches, coffee breaks, and one social dinner per week. The page is accessible via the following link: https://research.pdmfc.com/event/ipics-2025/
Winter School January 2026 Lisbon	The registration fee was €150. However, for the student, it was entitled to a full scholarship. Regarding lodging, learners managed themself. The page is accessible via the following link: https://research.pdmfc.com/event/winter-school-2026-cyber-security-winter-school/

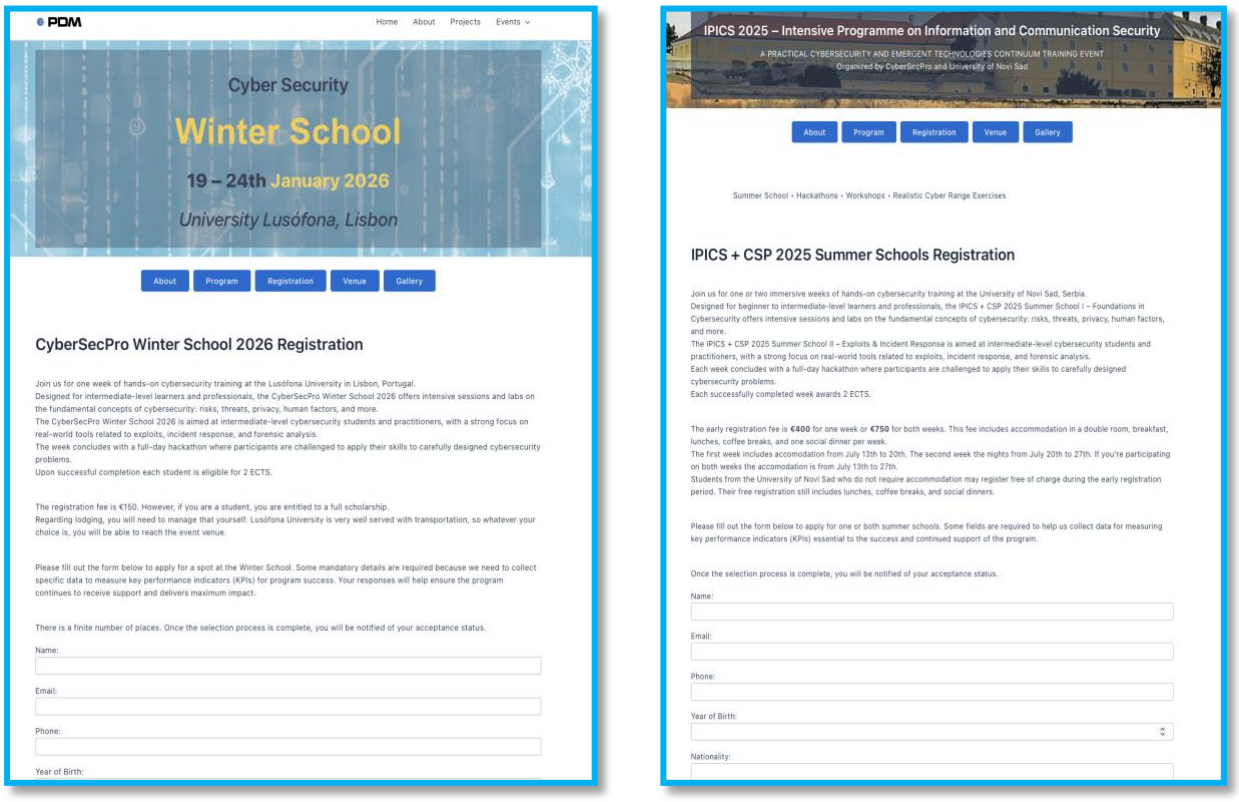


Figure 15: Screenshot of CyberSecPro seasonal school registration page

3. **University registration:** Registration was carried out through the hosting university's official systems, such as the Laurea Pakki System, etc.
4. **Third-party registration:** Registration was managed by external organizations or platforms outside CyberSecPro. Examples include events accessed through the IEEE EDUCON 2024[3] Conference, RUSI Europe[4], the Symposium on Artificial Intelligence and its Impact on Future Communities[5], and the Digital Security Agency of Cyprus (DSA)[6].

4.2.4 Pre-requisites and Admission Criteria

In general, the prerequisites for the implemented CSP modules included the basic IT and Security Knowledge as well as fundamental knowledge of cybersecurity concepts. In the few modules, fundamental knowledge on operating systems, networking and programming was needed. For a limited number of introductory modules, no specific prerequisites was required. In addition, pre-requisites for each CSPs module is defined in D3.1. Additional details on the admission criteria for the seasonal schools are provided Table 5.

[3] https://2024.ieee-educon.org/registration

[4] https://my.rusi.org/our-offices/rusi-europe.html

[5] https://www.laurea.fi/en/current-topics/events/symposium-on-artificial-intelligence/

[6] https://dsa.cy/en/

Table 5: Admission criteria of seasonal schools

Seasonal schools	Admission Criteria
Summer School 2024 Madeira	None. All applied learners were accepted.
CyberHOT 2024 Piraeus	
CyberHOT 2025 Crete	
Summer School 2024 Porto (IPICS 2024)	The host of seasonal schools received and reviewed the CVs and the provided information and then decides whether to accept or reject the application. The main criterion was having at least a basic connection to or interest in cybersecurity, and all received CVs met this requirement and were therefore accepted. It was planned that if the number of applications exceeded the room capacity, applicants with more relevant backgrounds would be selected.
Winter School 2025 Caparica	
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	
Winter School January 2026 Lisbon	In addition of above action regarding CV reviewing, in this winter school the host organized a configuration session one week in advance to ensure that learners' computers were properly set up to complete the exercises during the event. The host informed learners that if they were unable to complete the configuration with some basic information, they should not attend the event in order to avoid losing time. However, all learners successfully completed the setup.

4.2.5 Tangible rewards to learners

Certificates of attendance was mostly used as the tangible rewards across the implemented CSP modules. As illustrated in Figure 16, the majority of modules awarded certificates upon full attendance, while a smaller number also link with passing exam, or other defined criteria. In contrast, 21 modules related to T4.3 did not provide certificates. This number increases to 28 modules when CSP003, related to T4.4, is also taken into account.

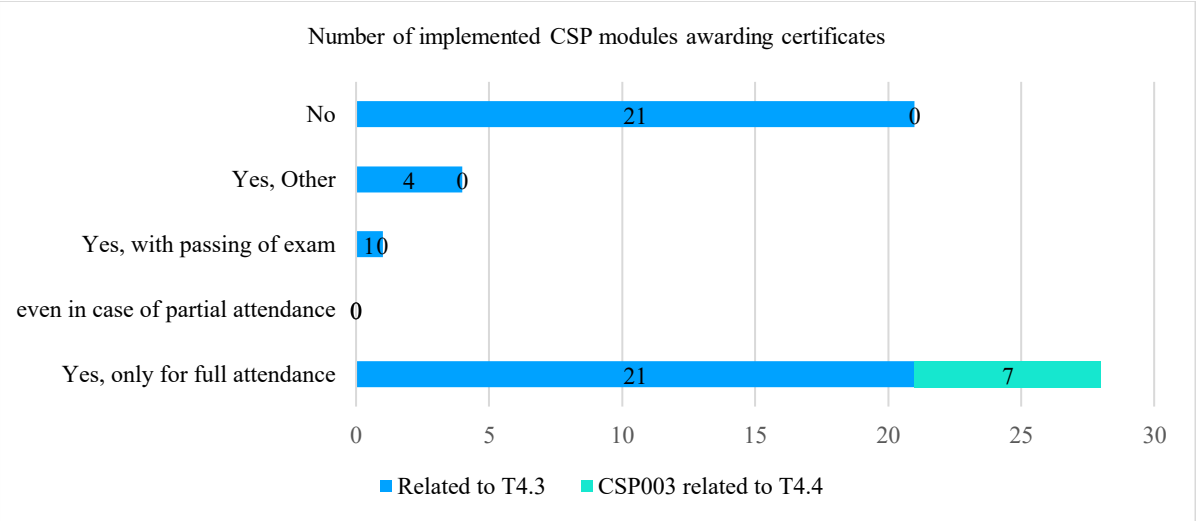


Figure 16: Number of implemented CSP modules awarding certificates

Certificates are awarded by several partner organizations, including UPRC, UNINOVA and FCT, PDMFC, the University of Western Attica, LAU, TalTech, UNSPMF, APIRO, the Digital Security Authority of Cyprus,

and Nova, highlighting the institution involvement in organizing seasonal schools. As most of the tangible rewards are related to the seasonal schools, all such rewards are listed in Table 6. Also, ECTS credits as additional tangible rewards for learners were and are being awarded by some events.

Table 6: Tangible reward to the learners from seasonal schools

Seasonal schools	ECTS reward	Certification and awarding organization
Summer School 2024 Madeira	No ECTS were awarded.	Learners got certificate of attendance signed by UNINOVA.
Summer School 2024 Porto (IPICS 2024)	4 ECTS upon successful completion of the program (including the two-day long Hackathons) by COFAC.	Learners got certificate of attendance signed by COFAC.
CyberHOT 2024 Piraeus	No ECTS were awarded.	Learners got certificate of attendance signed by the organizers (UPRC, TUC, trustilio, FP, Dienekes).
Winter School 2025 Caparica	2 ECTS upon successful completion of the program by COFAC.	Learners got certificate of attendance signed by UNINOVA and FCT.
CyberHOT 2025 Crete	No ECTS were awarded.	Learners got certificate of attendance signed by the organizers (UPRC, TUC, trustilio, FP, Dienekes).
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	2 ECTS 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 upon successful completion by COFAC.	Learners got certificate of attendance signed by COFAC.

4.2.6 Learning Outcomes

The learning outcomes of implemented CSP modules are largely consistent with modules designed in D3.1, with no significant deviations observed. They are copied here in Table 7 for ease of reference.

Table 7: Learning outcomes

CSPs related to T4.3	Learning Outcomes
CSP001 - Cybersecurity Essentials and Management	By the end of the training, learners gained the following: Knowledge: • Ethical principles and guidelines for cybersecurity professionals. • Basic cybersecurity terminology and concepts • The CIA triad (confidentiality, integrity, and availability). • Types of cybersecurity threats and vulnerabilities. • Cybersecurity frameworks and models (ISO/IEC 27001, ECSF, NIST Cybersecurity Framework, CyBoK). • Human psychology in cybersecurity. • Secure architecture design and implementation principles. • Data security and privacy principles. • Cybersecurity governance practices and frameworks. • Cybersecurity laws, regulations, and legislation. • Information security risk management (ISRM) methodologies. Skills: • Identify and classify cybersecurity threats and vulnerabilities. • Conduct vulnerability assessments and penetration tests. • Implement vulnerability management strategies. • Develop and implement cybersecurity policies and procedures. • Select and implement security controls. • Design secure network architectures and systems.

CSPs related to T4.3	Learning Outcomes
	• Implement data security measures. • Manage user access and privileges. • Communicate cybersecurity risks effectively. • Document cybersecurity incidents and procedures. • Conduct self-assessments and stay updated on cybersecurity trends. Competencies: • Apply ethical decision-making in cybersecurity situations. • Analyse the impact of cybersecurity threats and vulnerabilities. • Design and implement secure solutions. • Manage and mitigate cybersecurity risks. • Educate and empower users on cybersecurity best practices. • Collaborate effectively with stakeholders on cybersecurity initiatives. • Adapt to changing cybersecurity threats and technologies. • Embrace continuous learning and professional development.
CSP002 - Human Factors and Cybersecurity	By the end of the training, learners gained the following: Knowledge: • Understanding of the human element's role in cybersecurity. • Knowledge of common human errors and vulnerabilities exploited in cyberattacks. • Awareness of psychological and social factors influencing security decisions. • Understanding of organisational culture's impact on cybersecurity posture. • Knowledge of effective communication strategies for cybersecurity collaboration. • Insights into decision-making at different levels in cybersecurity. • Awareness of best practices for designing and implementing cybersecurity training programmes. • Understanding of emerging trends and challenges in cybersecurity related to human factors. Skills: • Identifying and analysing human factors contributing to cybersecurity risks. • Assessing and mitigating risks associated with human vulnerabilities. • Developing and implementing effective communication strategies for security awareness and collaboration. • Making informed security decisions considering human factors and data. • Designing and evaluating cybersecurity training programmes for different audiences. • Staying up to date on emerging trends and best practices in human factors and cybersecurity. Competencies: • Critical thinking about the human element in cybersecurity. • Problem-solving to address human-related security risks. • Effective communication with diverse stakeholders about cybersecurity. • Collaboration across domains to build a robust security culture. • Decision-making based on data, analysis, and understanding of human factors. • Adaptability to evolving threats and challenges in the cybersecurity landscape.
CSP003 - Cybersecurity Risk Management and Governance	By the end of the training, learners gained the following: Knowledge: • Basic definitions related to Information Security Management Systems and Information Security Governance • Risk Management: Basic phases and principles for an effective risk management methodology. • Standards and Methodologies of Risk Management

CSPs related to T4.3	Learning Outcomes
	• Legal and Policies related to Risk Management • Measurements, Scales and Metrics of Risks • Technical and non-Technical Mitigation Actions Skills: • Applying a suitable methodology for Information Security Risk Management and Risk Assessment. • Analysing Information Security Risk utilising different methodologies. • Creating policies, procedures and processes compliant with the requirements of the current version of the ISO/IEC 27000x series of standards. • Selecting and implementing appropriate mitigation actions and controls. • Developing security policies and procedures • Developing Business Continuity Plans and Disaster Recovery Plans. • Implementing cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards. • Analysing and consolidating the organisation's quality and risk management practices. • Enabling business asset owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks. • Enabling employees to understand, embrace and follow the controls. • Building a cybersecurity risk-aware environment. • Communicating, presenting and reporting to relevant stakeholders. • Proposing and managing risk-sharing options Competencies: • Lead and participate in strategic, operational, and tactical cybersecurity discussions. • Lead the design, development, operation and improvement of an Information Security Management System. • Support the organisation in the audits of an Information Security Management Systems. • Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories • Knowledge of risk-sharing options and best practices • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks.

CSPs related to T4.3	Learning Outcomes
CSP005 - Data Protection and Privacy Technologies	By the end of the training, learners gained the following: Knowledge**:** • Regulations and Standards: Understand key data privacy regulations (e.g., GDPR and others) and their implications for organisations and individuals. • Privacy-Enhancing Technologies (PETs): Identify and explain the purpose, benefits, and limitations of various PETs (e.g., anonymization, encryption, differential privacy). • Data Protection Best Practices: Gain knowledge of effective data security measures, data retention and deletion practices, and data breach response plans. • Emerging Trends: Recognise the impact of new technologies (e.g., AI, big data) on data privacy and ethical considerations. Skills: • Data Mapping and Inventory: Identify and map data flows within an organisation. • Data Protection Impact Assessments (DPIAs): Conduct risk assessments for data processing activities and implement mitigation strategies. • Security Policy and Procedure Development: Define and implement data security policies and procedures, including access control and MFA. • Data Anonymisation and Sharing Techniques: Apply PETs to anonymize data and enable secure data sharing. • Incident Response: Develop and implement a plan for responding to data breaches and security incidents. Competencies: • Critical Thinking: Analyse complex data privacy scenarios and recommend appropriate solutions. • Problem-solving: Identify and address data protection challenges within organisations. • Communication and Collaboration: Effectively communicate data privacy risks and best practices to stakeholders. • Adaptability: Stay informed about evolving data privacy regulations and technologies, and adapt practices accordingly. • Ethical Decision-Making: Balance the need for data security with individual privacy rights and ethical considerations.

In addition to the learning outcomes outlined in D3.1, the following supplementary learning outcomes shown in Table 8 identified from the implemented CSP modules, as recorded in the Admin Portal.

Table 8: Supplementary learning outcomes from implemented CSP modules

CSPs related to T4.3	Learning Outcomes
CSP001 - Cybersecurity Essentials and Management	Knowledge: • Define cybersecurity and its significance in the energy sector. • Identify and assess energy cybersecurity threats. • Understand the principles of cybersecurity risk management. • Understand the principles of network segmentation, firewall configuration, and access control. • Understand the importance of password security, multi-factor authentication (MFA), data encryption, and patch management. • Understand the importance of incident response planning and procedures. • Understand energy cybersecurity regulations and guidelines. • Analyse real-world energy cybersecurity cases. • Be aware of the Network Code on Cybersecurity for the Electricity Sector. • Understand the impact of emerging technologies on energy sector security. • Know strategies for building a strong cybersecurity culture. • Understand the critical role of cybersecurity in protecting European critical infrastructure. • Develop a comprehensive understanding of the EU cybersecurity regulatory and policy framework. • Acquire knowledge of various cybersecurity technologies and their applications in critical infrastructure.

	Skills: • Develop and execute cybersecurity risk management plans. • Design and implement secure network architectures. • Deploy and manage security controls for energy systems. • Develop and execute incident response plans. • Comply with energy cybersecurity regulations and guidelines. • Apply cybersecurity concepts and techniques through practical exercises. • Communicate cybersecurity risks, policies, and procedures effectively. • Develop and maintain cybersecurity documentation. • Demonstrate a willingness to stay up-to-date with the latest cybersecurity threats and trends. • Identify cybersecurity risks in the energy sector. • Analyze compliance requirements for the energy sector. • Assess the impact of new technologies on security. • Develop cybersecurity policies and procedures. • Implement cybersecurity best practices. • Conduct thorough vulnerability assessments and risk management for critical infrastructure. • Develop and implement effective incident response and business continuity plans. • Design and implement robust access control and identity management measures. • Protect critical infrastructure systems, including industrial control systems, SCADA, and IoT. • Mitigate insider threats and manage cybersecurity risks in remote work environments. • Collaborate effectively with public and private sector stakeholders on cybersecurity initiatives. • Measure and evaluate cybersecurity performance using appropriate metrics. Competencies: • Demonstrate understanding of the energy sector's cybersecurity challenges. • Apply regulatory knowledge to ensure compliance. • Evaluate cybersecurity risks and develop mitigation strategies. • Lead cybersecurity initiatives within an organization. • Foster a strong cybersecurity culture.
CSP002 - Human Factors and Cybersecurity	Knowledge: • Gain an understanding of the psychological, social, and organisational elements that shape cybersecurity actions within the energy domain. • Understand the critical role of communication and teamwork in bolstering energy cybersecurity across different sectors. • How decision-making frameworks are used at strategic, operational, and tactical levels within energy cybersecurity. • Recognise the profiles and strategies of adversaries targeting energy operations. • Evaluate human-related threats and vulnerabilities in energy contexts. Competencies: • Understand the discussions pertinent to energy cybersecurity at various levels of decision-making. • Cultivate an environment of transparent communication and teamwork focused on energy cybersecurity. • Reflect on cybersecurity decision-making with the understanding of how human factors are related in the energy arena. • Identify human-centric threats and vulnerabilities in energy operations.
CSP003 - Cybersecurity Risk Management and Governance	Knowledge: • Demonstrate an in-depth understanding of cyber security risk management framework in energy sector • Recognize the significant cybersecurity governance structures and processes in the energy sector • Demonstrate knowledge and understanding of risk management as a process • Gain knowledge of the different stages of risk management • Gain knowledge on the governance structures and processes for cybersecurity • Become acquainted of the controls applied and the specific directions provided by standard ISO 27799, Health informatics – Information security management in health using ISO/IEC 27002. Skill: • Critically assess and report security risk and suggest suitable mitigation strategies in professional manner • Critically develop and evaluate security policy and select controls by following ISO 27019 for security governance.Skills: • Identify and know to apply an appropriate methodology for Information Security Risk Management and Risk Assessment according to the specific characteristics of the energy scenarios. • Analyse the results of a cybersecurity risk assessment. • Ability to perform a risk assessment methodology and produce the relevant risk assessment results.

	• Select suitable controls (as adapted and customized by ISO 27799) to treat relevant un acceptable risks. Competencies: • Lead and participate in strategic, operational, and tactical cybersecurity discussions, with a particular focus on the energy sector. • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories; all of them specific to the energy sector and its operational systems. • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks in the energy sector and its operational systems.
CSP005 - Data Protection and Privacy Technologies	Knowledge: • Methos, rules and policies applied in the computer network and network connected SCADA networks between energy sector business and organisations. Skill and Competence: • Learning to administer and setup security devices. • Knowledge of Linux OS and use of terminal focusing to administer networks and servers. • Setup servers and networks to avoid leaks and breaches.

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

Table 9 describes the number of job-placements/internships carried out by the students. In both cases, the number of organizations of members of the consortium three times higher than that the number of external organizations.

Table 9: Number of job-placements/internships carried out by the students

	Related to T4.3	Related to T4.4
In the organizations of members of the consortium	34	10
In an external organization	95	32

4.2.8 Background of the learners

This subsection describes the background of the learners. It provides an overview of learners' age, gender, educational background, and professional experience and affiliation.

4.2.8.1. Number of learners in CSP modules per gender

Figure 16 shows the number of learners enrolled in the implemented CSP modules by gender. There are 1129 male learners in T4.3 modules and a further 184 in CSP003 realted to T4.4. Female learners are with 418 learners in T4.3 and 64 in CSP003 realted to T4.4, for a total of 482 which is 27.02% of the total learners under T4.3. Overall, the figure shows that female learners account for 27.02% percent of the total, positioning this share at the upper margin of the industry distribution standard.

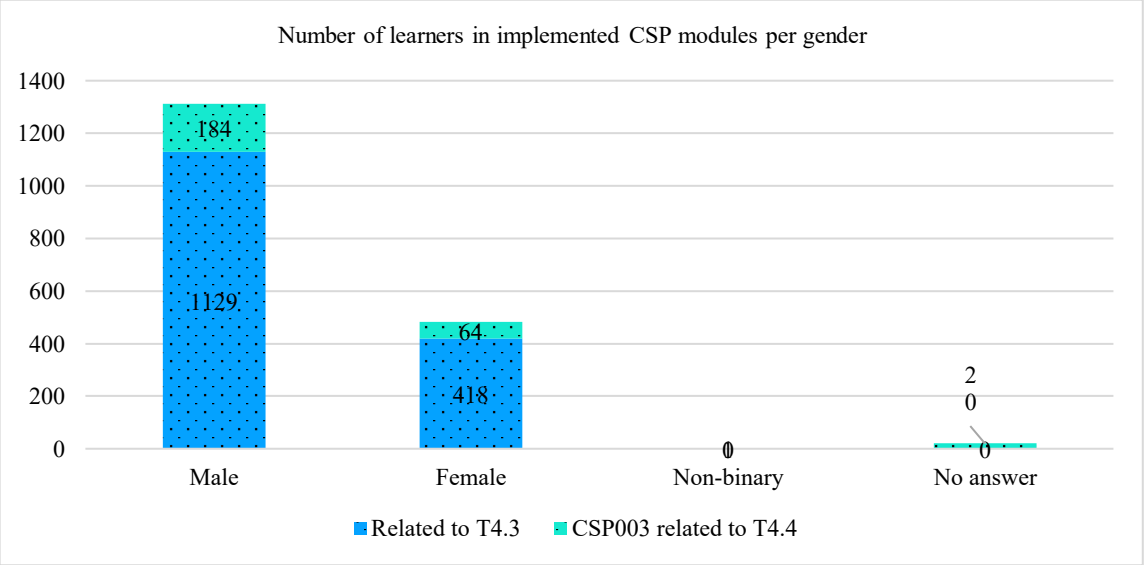


Figure 16: Number of learners in implemented CSP modules per gender

4.2.8.2. Number of learners in implemented CSP modules per Age

Figure 17 shows the number of learners enrolled in implemnted CSP modules across different age groups. Not surprisingly most learners are concentrated in the 18–25 age group, which has by far the highest participation. The second largest group is learners aged 26–34. At the same time, we have also some learners aged 35–45 and 45+–54[7] which means second careers also able to attend. Very few learners are under 18, 55–65 and more than 65 age group. Overall, the data indicates that implemented CSP modules mainly attracted young adults, particularly those between 18 and 34 years old.

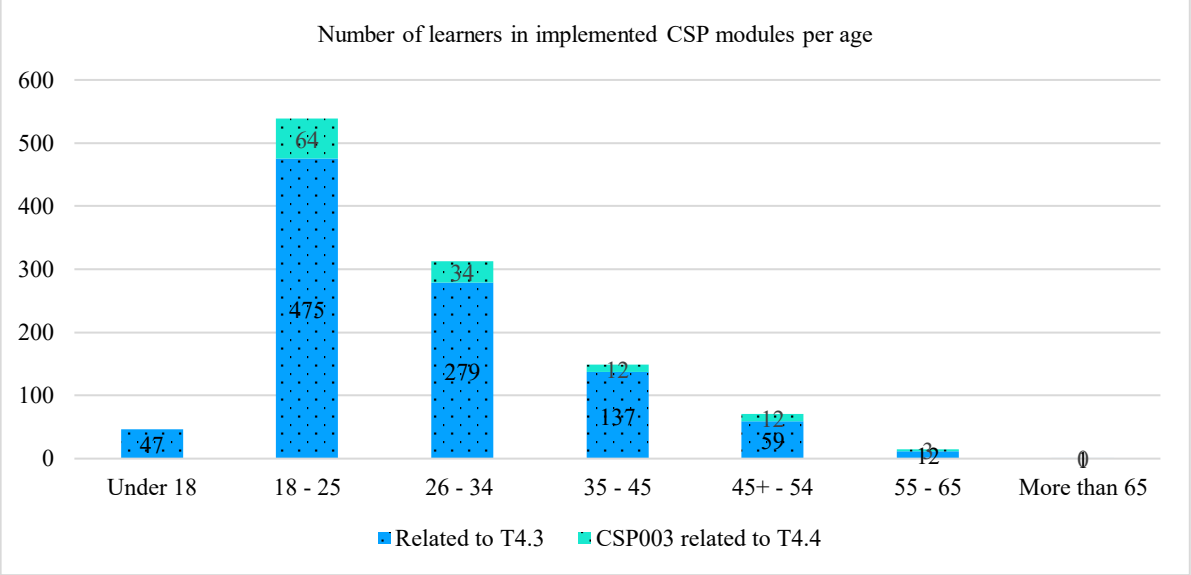


Figure 17: Number of learners in implemented CSP modules per age

4.2.8.3. Number of learners in implemnted CSP modules per educational Background

Figure 18 shows the number of learners in implemented CSP modules by educational background. Learners with less than a high school education and high school diploma or equivalent are few in both categories. For with some college but no degree, there are 132 in T4.3 and none in T4.4. Not surprisingly, the largest group learners are undergraduate (Bachelor's) degree holders as T4.3 focus on introductorily and fundamental CSP modules. Master's degree learners show 208 in T4.3 and the 46 for T4.4. Doctoral (PhD) learners have 104 in T4.3 and 13 in T4.4. Overall, implemented CSP modules under T4.3, are mostly taken by learners with undergraduate (Bachelor's) degree holders which means that we drove cybersecurity knowledge into the earlier level of education, which is good as the awareness needs to raise in the earlier level.

[7] 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."

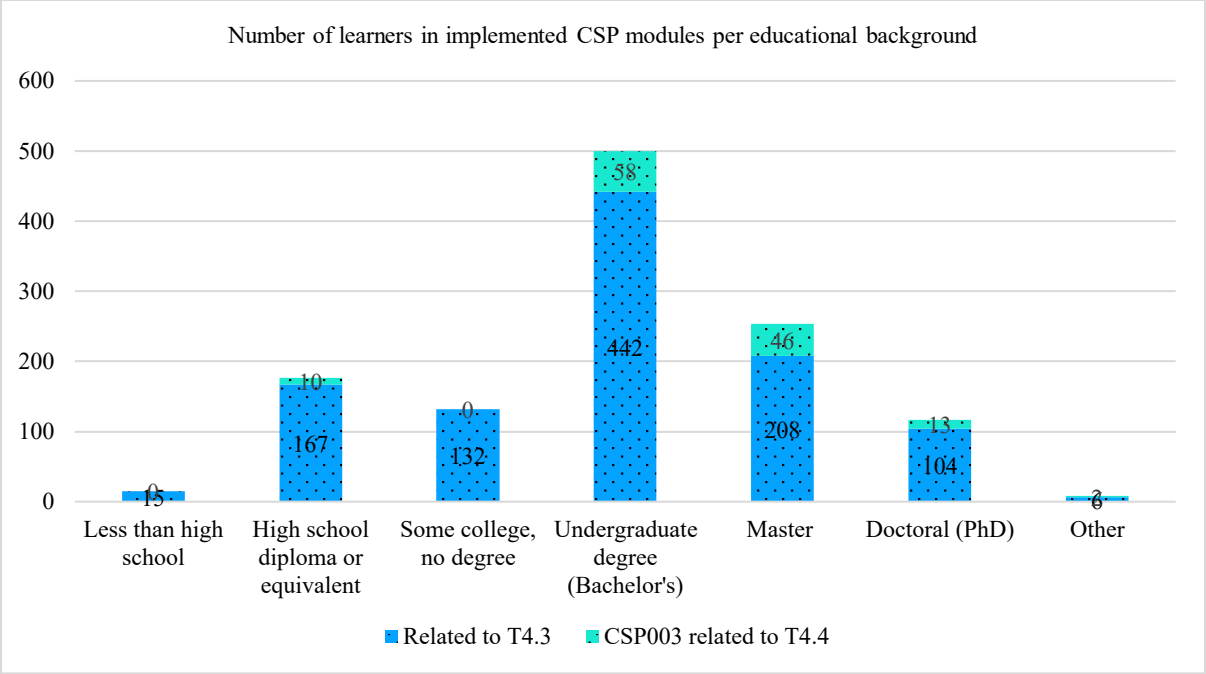


Figure 18: Number of learners in implemented CSP modules per educational background

4.2.8.4. Professional experience and affiliation

Figure 19 indicate that the CSP modules primarily attracted students, while also engaging a diverse range of professionals from industry and organizational environments. One learner can belong to more than one category.

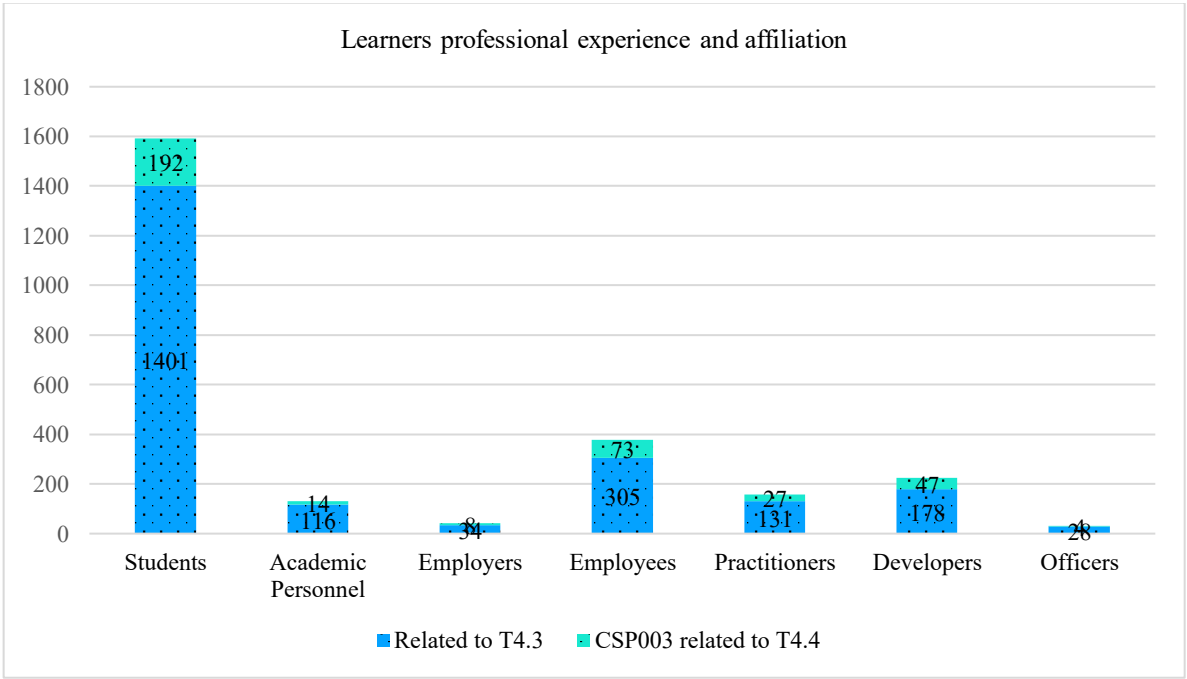


Figure 19: Learners professional experience and affiliation

Table 10 presents some project KPIs related to the background characteristics of learners. Regarding age distribution, there are 134 learners over 45 years old. In terms of educational background, it has involved

considerable number of non-ICT graduates (138 learners). Also, concerning prior cybersecurity knowledge, T4.3 includes 336 self-trained learners.

Table 10: Project KPIs related to learner's background

Learners Background	Related to T4.3	Related to T4.4
Number of learners more than 45 years old	134	19
Number of learners, who are non-ICT graduates	138	7
Number of learners, who are cybersecurity self-trained	340	112

4.2.9 Hosting sites

Figure 20 shows the number of implemented CSP modules by type of host. EU HEIs host the largest number of implemented CSP modules, with 30 implemented modules, followed closely by companies with 15 modules. In addition to companies and HEIs, few modules (2) were held in the public sector organizations, such as Digital Security Authority of Cyprus - Cyprus Standardization body, Nicosia, Cyprus.

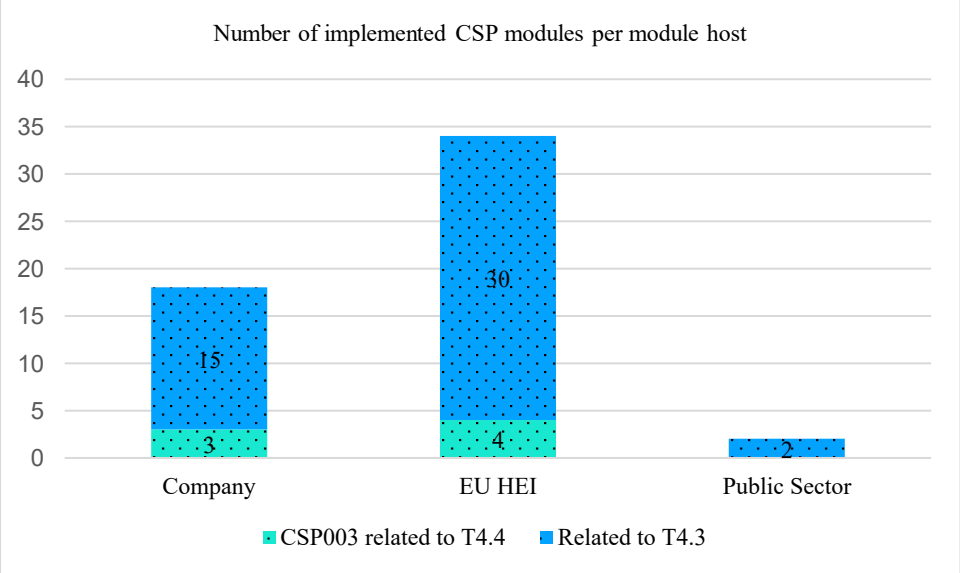


Figure 20: Number of implemented CSP modules per module host

4.2.10 Evaluation forms of learners[8] and trainers

At the initial stage, D3.1 provided evaluation templates based on the combined development work of WP2, WP3, and D4.1. These templates were intended for use by both learners and trainers to collect feedback on the implemented CSP modules. The templates were developed within a DCM system, and feedback was collected online (see D3.1 for further details). Accordingly, the CSP modules implemented in the early phase of the project made use of these templates.

Subsequently, following the start of WP5 activities, a new set of evaluation forms for learners and trainer was developed based on the review of existing evaluation frameworks as well as CyberSecPro context (refer to D5.1 for further details). This evaluation is centred on two key aspects: assessing learner satisfaction with the training activities and examining the trainer's experience in developing and delivering the module using the provided training materials. The responses from these evaluation forms were analysed in WP5.

[8] "Trainees" is the original terminology used in the Grant Agreement, but it turned out that the rest adopted the term "learners".

In addition to these two evaluation forms developed within the project, some participating organisations were required to use their own internal evaluation forms in order to comply with institutional or organisational requirements. Also, it worth to mention that in some cases, data collection from the learners was also conducted during the face-to-face training sessions. Below, we breifly introduce the evaluation forms developed within WP5 and implemented in the Admin Portal to collect data online.

CyberSecPro learner 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 designed and customised 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 generated a unique URL and QR code to enable easy distribution of the survey to learners via multiple digital channels. Figure 21 shows a screen shot of CyberSecPro learner evaluation form in the Admin Portal.

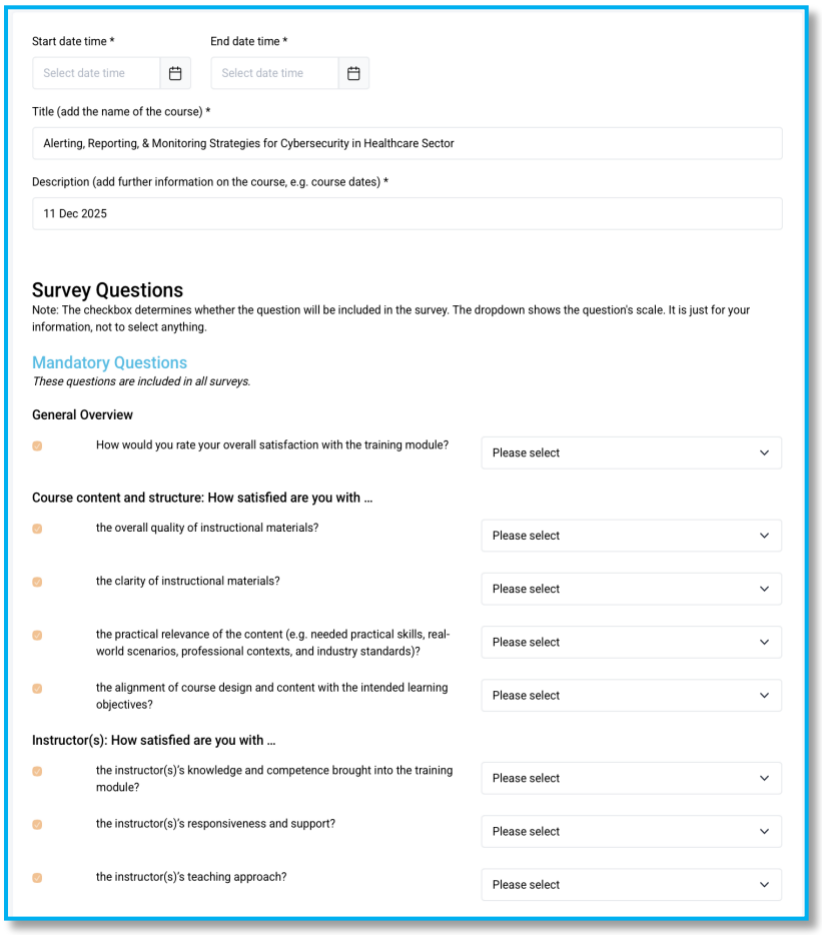


Figure 21: Screen shot of CyberSecPro learner evaluation form in the Admin Portal

CyberSecPro trainer evaluation form

The evaluation of the training implementation from the trainers' perspective 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 was automatically generated within the portal for each module implementation. As the survey is standardised, trainers did 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 described in D5.1 and D5.2 with results reported in D5.2. Figure 22 shows a screen shot of CyberSecPro trainer evaluation form in the Admin Portal.

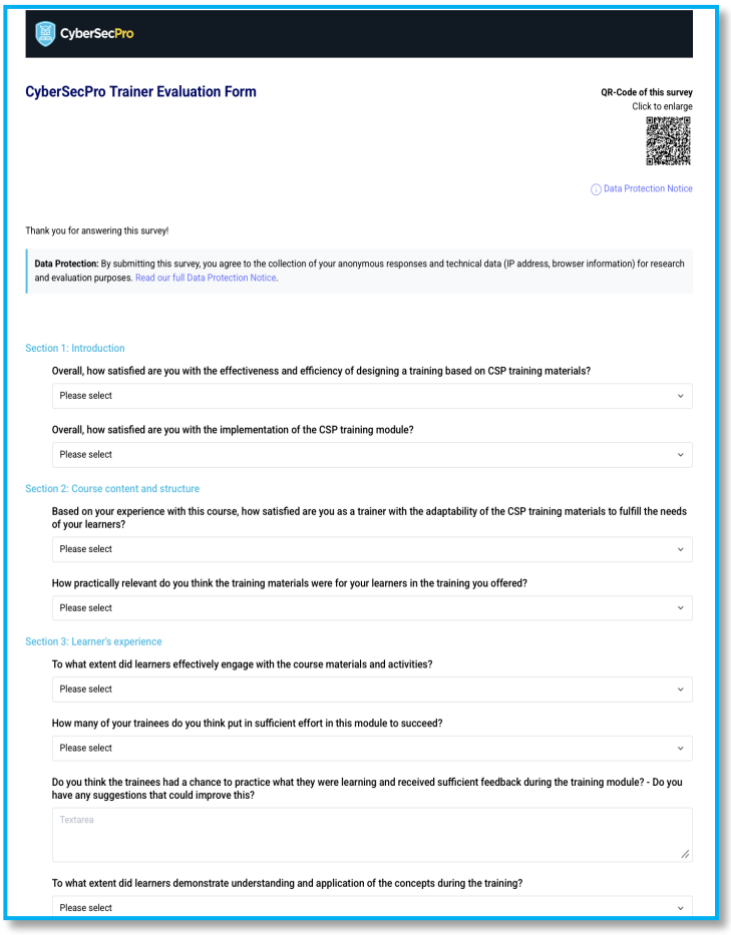


Figure 22: Screen shot of CyberSecPro trainer evaluation form in the Admin Portal

Follow-up survey

As mentioned in 2.1 in order to response to EC requirements regarding KPIs specified in the call, as well as the SO4 indicator 3, an additional questionnaires was developed for CSP module implementation providers to collect the relevant data from the learners (see Annex D: CyberSecPro Evaluation Forms for further details).

For the follow-up survey, we followed two approaches to ensure that we collected the required data as accurately as possible. In the first approach, individual module implementation 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 survey of the Admin Portal is shown in Figure 23.

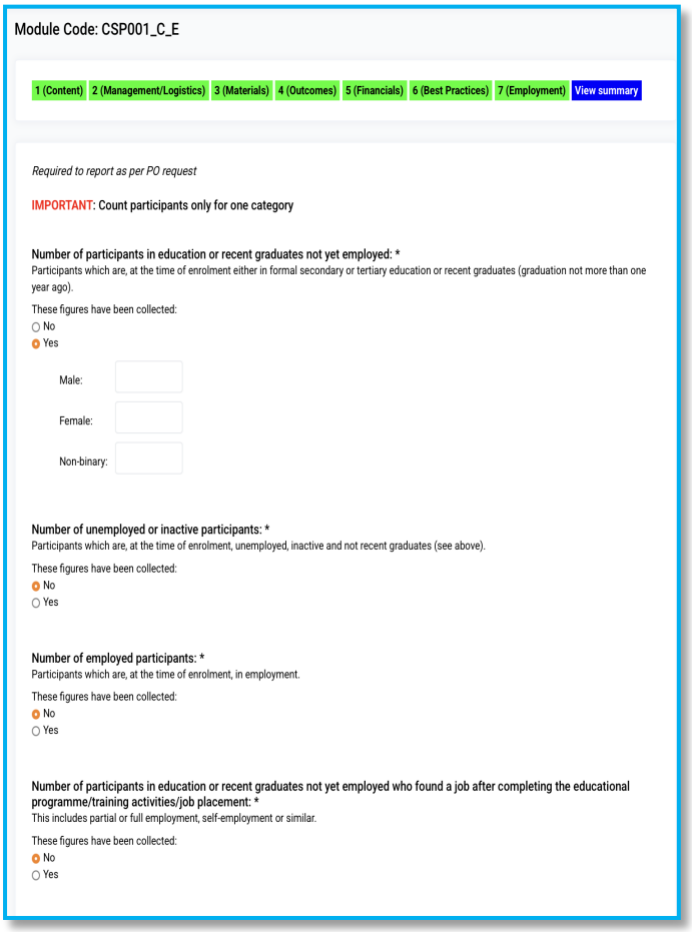


Figure 23: Screen shot of employment tab in the Admin Portal

In the second approach, as described in D5.2, WP5 followed up with the learners from 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 24. All results reported in the in the KPI section in the EC SYGMA portal.

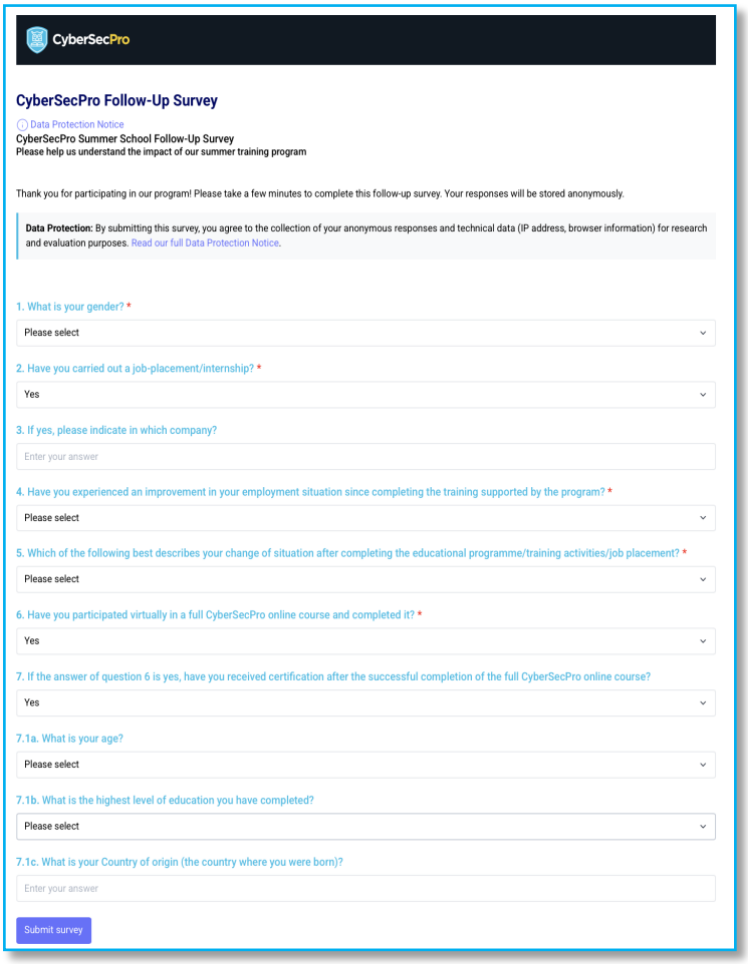


Figure 24: Follow-up survey in the Admin Portal

5. MOOCs

Within the CyberSecPro project, three MOOCs were developed to support cybersecurity capacity building. However, two of these MOOCs is directly aligned with the knowledge areas addressed in this deliverable. Therefore, Subsection 5.1 presents the essential information for the selected "CyberSecPro: Cybersecurity Fundamentals", including its structure, objectives, and syllabus and Subsection 5.2 presents the corresponding tables for the "Human Factors of Cybersecurity" MOOC.

5.1 MOOC – "CyberSecPro: Cybersecurity Fundamentals"

The following section presents the MOOC description using the format and structure defined in D3.1 for documenting individual modules. Two tables are included: Table 11 provides the general information about the "CyberSecPro: Cybersecurity Fundamentals" MOOC, while Table 12 presents detailed information on its syllabus, including the topics and learning content.

Table 11: Description of MOOC: CyberSecPro: Cybersecurity Fundamentals

MOOC Title *The title of the training module*	**CyberSecPro: Cybersecurity Fundamentals**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Cybersecurity Foundations: Concepts, Tools, and Best Practices Essential Cybersecurity: Concepts, Tools, and Best Practices CyberSecPro: Essential Cybersecurity Concepts CyberSecPro: Introduction to Cybersecurity – Start your journey in digital defense
Training offering type *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 *Training level: B (Basic), A (Advanced)*	Basic (B)
MOOC overview *High-level MOOC overview*	**Cybersecurity Fundamentals** is an introductory MOOC designed to provide learners with a solid foundation in cybersecurity concepts, threats, and defensive practices. The course targets a broad audience, including students, professionals from non-technical backgrounds, and early-career IT practitioners who want to understand how cybersecurity affects modern digital systems, organizations, and society.

MOOC Title *The title of the training module*	**CyberSecPro: Cybersecurity Fundamentals**
MOOC description *Indicates the main purpose and description of the MOOC.*	The course introduces the core principles of cybersecurity, such as confidentiality, integrity, and availability, and explains how these principles apply across personal, corporate, and critical infrastructure contexts. Learners will explore common cyber threats and attack vectors, including malware, phishing, social engineering, network attacks, and data breaches, gaining insight into how and why these attacks occur. The MOOC is concept-driven rather than tool-specific, focusing on building cybersecurity awareness, vocabulary, and critical thinking. Real-world examples and scenarios are used to illustrate how cybersecurity challenges arise and how they can be mitigated in practice.
Learning outcomes and targets *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: • Understand essential cybersecurity concepts, threats, and defense principles. • Secure operating systems, networks, and data by using best practices. • Apply basic cryptography to protect information and communication. • Detect, analyse, and respond to cybersecurity incidents. • Document incidents and clearly communicate security risks. • Show practical, job-ready skills through hands-on labs and a capstone project.
Main topics and content list *A list of main topics and key content*	• Core security principles • Operating system security • Network security and secure network protocols • Encryptions methods • Hashing and data integrity • Digital signatures and certificates • Risk management • Security monitoring • Incident response fundamentals • Cybersecurity career paths and roles
Evaluation and verification of learning outcomes *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. Automated feedback is provided to guide learners, highlight knowledge gaps, and support improvement. Successful completion of the assessment activities demonstrates that participants have achieved the intended learning outcomes by showing

MOOC Title *The title of the training module*	**CyberSecPro: Cybersecurity Fundamentals**
	both conceptual understanding and the ability to apply fundamental cybersecurity practices in context.
Training Provider *Name(s) of training providers.*	PDMFC
Contact *Name(s) of the main contact person and their email address.*	Nuno Pedrosa (nuno.pedrosa@pdmfc.com)
Dates offered *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 *Duration of the training.*	Estimated at 130 hours, including exercises.
Training method and provision *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) https://moodle.cybersecpro.grisenergia.pt/course/view.php?id=155
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management*	Mainly • KA1 – Cybersecurity Management • KA3 – Cybersecurity Risk Management

MOOC Title *The title of the training module*	**CyberSecPro: Cybersecurity Fundamentals**
KA8 – Cybersecurity Tools and Technologies *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	
Pre-requisites	None
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this MOOC training with ECSF. It also indicates which ECSF profiles needs this MOOC.*	Mainly: • ECSF Profile: Chief Information Security Officer (CISO) • ECSF Profile: Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this MOOC.*	• ClamAV • DNS leak test service (e.g., dnsleaktest.com) • GnuPG / GPG • Gpg4win • IP check service (e.g., whatismyipaddress.com) • Linux (Ubuntu 22.04+ recommended) • Linux syslog / auth.log • Local Users & Groups Manager (lusrmgr.msc) • login.defs • Microsoft Defender Antivirus • Modern web browser (Chrome, Edge, Firefox, or Safari) • Network activity logs • Network interface access (Wi-Fi / Ethernet / Loopback) • Nmap • Npcap • OpenSSH client/server • PAM (Pluggable Authentication Modules) • Ping / ICMP utilities • SHA-256 hashing tool (sha256sum) • Spreadsheet software (Excel, Google Sheets, or LibreOffice Calc) • sudo / visudo

MOOC Title *The title of the training module*	**CyberSecPro: Cybersecurity Fundamentals**
	• Terminal / command line interface • Text editor • Ubuntu Desktop or Server ISO • UFW (Uncomplicated Firewall) • VirtualBox, VMware Workstation Player, or Hyper-V • VPN client software • VPN protocols (OpenVPN or WireGuard) • Windows 10 or 11 • Windows Defender Firewall (Advanced Security) • Windows Event Viewer • Wireshark • Word processor
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	5 ECTS
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No (if attending as guest)
MOOC enrolment dates *Indicates the enrolment dates for the operation of this MOOC.*	Self-paced
Other important dates *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 12: Syllabus of MOOC: CyberSecPro: Cybersecurity Fundamentals

Main topics	Suggested Content (with bullet list)
Topic-1: Module 1 – Introduction to Cybersecurity	What is cybersecurity? Types of cyberattacks Core security principles Firewalls and antivirus tools
Topic-2: Module 2 – Operating System and Network Security	Introduction to operating system security OS hardening techniques Memory corruption and mitigation Introduction to network security Secure network protocols Wireless network security
Topic-3: Module 3 – Cryptography and Security Protocols	Introduction to cryptography Encryption methods: symmetric and asymmetric Hashing and data integrity Digital signatures and certificates
Topic-4: Module 4 – Risk Management and Security Policies	What is risk in cybersecurity? Identifying and assessing risk Risk mitigation and controls Security policies and governance Security awareness and training programs
Topic-5: Module 5 – Threat Detection and Incident Response	Introduction to threat detection Indicators of compromise (IoCs) Security monitoring and SIEMs Incident response fundamentals Incident reporting and documentation Cybersecurity forensics and evidence handling
Topic-6: Module 6 – Final Project and Capstone	Capstone project: Cybersecurity incident simulation
Topic-7: Module 7 – Launching Your Cybersecurity Journey	From student to practitioner – what's next? Cybersecurity career paths and roles Building a personal lab and portfolio Certification guide and study strategies

Main topics	Suggested Content (with bullet list)
	Community, ethics, and the industry you're entering Final reflection and course wrap-up

5.2 MOOC – "Human Factors of Cybersecurity"

Table 12 provides the general information about the "Human Factors of Cybersecurity" MOOC, while Table 14 presents detailed information on its syllabus, including the topics and learning content.

Table 13: Description of MOOC: Human Factors of Cybersecurity

MOOC Title *The title of the training module*	**Human Factors of Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Human Factors in Cybersecurity Human Aspects of Cybersecurity
Training offering type *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 *Training level: B (Basic), A (Advanced)*	Advanced
MOOC overview *High-level MOOC overview*	The course introduces threats and challenges/concerns arising from the human behaviour and decision making regarding technology use. In lectures we are focusing on raising the ability to assess and cope with cyber scams/threats (eg. social manipulation), on research skills to conduct studies in the field and to create and implement study materials, training programs and tools based on them in order to increase level of cyber hygiene in users and companies.
MOOC description *Indicates the main purpose and description of the MOOC.*	The course introduces threats and challenges/concerns arising from the human behaviour and decision-making regarding technology use. In lectures we are focusing on raising the ability to assess and cope with cyber scams/threats (eg. social manipulation), on research skills to conduct studies in the field and to create and implement study materials, training programs and tools based on them in order to increase level of cyber hygiene in users and companies.

MOOC Title *The title of the training module*	**Human Factors of Cybersecurity**
Learning outcomes and targets *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: After completing this course, the student: • understands the current state of research in this area; • can critically evaluate original research articles; • is able to analyze cyber competencies and find gaps and solutions to reduce human-related cyber risks; • is able to plan cyber-attacks which include elements of social engineering and propose defense mechanisms against them, • is able to assess and evaluate IT security interventions with employees; • is able to understand the behavioral science underpinnings of security-critical decision-making; • Understand how cognitive biases and human failure compromise practitioners' cybersecurity performance.
Main topics and content list *A list of main topics and key content*	1. Introduction to Human Factors and Cybersecurity 2. Human Factors Research Methodologies 3. Personality and Social Engineering (2 lessons) 4. Insider Threats 5. Mental Health of IT Security 6. Human-AI Interactions in Cybersecurity 7. Organisational Culture, Leadership, and Cybersecurity 8. Designing Education and Training for Cybersecurity (2 lessons) 9. Communication and Cybersecurity 10. Information and Deception 11. Human Aspects of Cybersecurity Risk Assessment 12. Situational Awareness and Shared Mental Modelling 13. Neuroergonomic Design and Cybersecurity
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	The final grade will be based on a written essay (3000 words) towards the end of the semester.
Training Provider *Name(s) of training providers.*	Tallinn University of Technology
Contact *Name(s) of the main contact person and their email address.*	Ricardo Lugo Ricardo.Lugo@taltech.ee

MOOC Title *The title of the training module*	**Human Factors of Cybersecurity**
Dates offered *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).*	August – December (yearly Autumn semester) January – May (yearly Spring semester)
Duration *Duration of the training.*	16 weeks
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual participation Students can enroll via TalTech admissions (https://taltech.ee/en/apply) or Euroteq (https://eduxchange.eu/euroteq/for-students-taltech/explore)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA7 – Cybersecurity Threat Management* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*
Pre-requisites	Bachelor's of Science in related fields (i.e.IT, cybersecurity, Management, Psychology)
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this MOOC training with ECSF. It also indicates which ECSF profiles needs this MOOC.*	Chief Information Security Officer (CISO) Cyber Legal, Policy & Compliance Officer Cybersecurity Educator Cybersecurity Implementer Cybersecurity Researcher Cybersecurity Risk Manager

MOOC Title *The title of the training module*	**Human Factors of Cybersecurity**
Tools to be used *A list of tools that will be used for the operation of this MOOC.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	6
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No
MOOC enrolment dates *Indicates the enrolment dates for the operation of this MOOC.*	May (Autumn semester) November (Spring semester)
Other important dates *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.*	Exams: December (Autumn semesters) May (spring semesters)

Table 14: Syllabus of MOOC: Human Factors of Cybersecurity

Main topics	**Suggested Content (with bullet list)**
Topics – 1,2,3,4,10	▪ van Steen, T. (2025). Developing a behavioural cybersecurity strategy: A five-step approach for organisations. *Computer Standards & Interfaces*, *92*, 103939. ▪ Wolbers, J., van Steen, T., Del-Real, C., & van den Berg, B. (2025, May). Cyber crisis averted: using safety science principles to learn from success. In *Proceedings of the International ISCRAM Conference*. ▪ Joinson, A., & van Steen, T. (2018). Human aspects of cyber security: behaviour or culture change? *Cyber Security: A Peer-Reviewed Journal*, *1*(4), 351-360.

Main topics	Suggested Content (with bullet list)
	▪ Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE. ▪ Sütterlin, S., Ask, T. F., Mägerle, S., Glöckler, S., Wolf, L., Schray, J., ... & Lugo, R. G. (2023, July). Individual deep fake recognition skills are affected by viewer's political orientation, agreement with content and device used. In *International Conference on Human-Computer Interaction* (pp. 269-284). Cham: Springer Nature Switzerland.
Topic 6,8	▪ •Maennel, K., & Maennel, O. M. (2024, December). Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges. In 2024 17th International Conference on Security of Information and Networks (SIN) (pp. 01-08). IEEE. • Wang, J., & Fan, W. (2025). The effect of ChatGPT on students' learning performance, learning perception, and higher-order thinking: insights from a meta-analysis. *Humanities and Social Sciences Communications*, *12*(1), 1-21. • Kestin, G., Miller, K., Klales, A., Milbourne, T., & Ponti, G. (2025). AI tutoring outperforms in-class active learning: an RCT introducing a novel research-based design in an authentic educational setting. *Scientific Reports*, *15*(1), 17458.
Topics 7,8,9,11,12	• Sütterlin, S., Lugo, R. G., Ask, T. F., Veng, K., Eck, J., Fritschi, J., ... & Knox, B. J. (2022, June). The role of IT background for metacognitive accuracy, confidence and overestimation of deep fake recognition skills. In *International Conference on Human-Computer Interaction* (pp. 103-119). Cham: Springer International Publishing. • Ofte, H. J., & Katsikas, S. (2023). Understanding situation awareness in SOCs, a systematic literature review. *Computers & Security*, *126*, 103069. • Endsley, M. R., & Garland, D. J. (2000). Theoretical underpinnings of situation awareness: A critical review. *Situation awareness analysis and measurement*, *1*(1), 3-21. • Mathieu, J. E., Heffner, T. S., Goodwin, G. F., Salas, E., & Cannon-Bowers, J. A. (2000). The influence of shared mental models on team process and performance. *Journal of applied psychology*, *85*(2), 273. • van Steen, T. (2025). Developing a behavioural cybersecurity strategy: A five-step approach for

Main topics	Suggested Content (with bullet list)
	organisations. *Computer Standards & Interfaces*, *92*, 103939. • Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: a meta-analysis. *Computers & Security*, *150*, 104206.
Common Readings for all Topics	• Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The digital competence framework for citizens: With new examples of knowledge, skills and attitudes. Publications Office of the European Union. https://doi.org/10.2760/115376 • European Union Agency for Cybersecurity. (2024). Best practices for cyber crisis management. ENISA. https://doi.org/10.2824/767828 • European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024: July 2023 to June 2024. ENISA. https://doi.org/10.2824/0710888 • European Union Agency for Cybersecurity. (2022). European cybersecurity skills framework (ECSF). ENISA. https://doi.org/10.2824/859537 • European Union Agency for Cybersecurity. (2022). European cybersecurity skills framework (ECSF): User manual. ENISA. https://doi.org/10.2824/95989

6. Summary and Conclusion

This deliverable presents the outcomes of T4.3 up to the conclusion of CyberSecPro in Month 39 (February 2026. Hence, it comprehensively records all CSP modules corresponding to the capability category "Cybersecurity Principle and Management" implemented by T4.3 by the end of February 2026 (M39). Moreover, it describes the context of the documentation task and the documentation methodology, including the definition of a record comprising the relevant information per module. ACEEU has established a system to document all implemented CSP modules.

The analysis demonstrates that a total of 47 implemented CSP 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 learners' engagement in both sector-specific and cross-sectoral modules. The sectoral distribution of modules and learners 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 here: "Cybersecurity Principles and Management". 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 used the template for describing CSP modules from D4.1 and added additional elements needed for the documentation of implemented CSP modules as shown in Table 15. We had also synchronized this template with the descriptions for training modules D3.1.

Table 15: Template for the documentation of implemented CSP modules

CSP Module Elements	CSP Module fields legend	CSP Module information
Code	**Code** (mandatory) *Code format:* *For general modules: CSP[n]_x:* • *[n] is the CSP module number (currently between 001 and 012)* • *x is the module offering type (see below)* *For sector-specific modules: CSP[n]_x_y:* • *[n] is the CSP module number (currently between 001 and 012)* • *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) *The title of the module as defined in the CSP catalogue (currently in D4.1)*	
	Title of the implemented CSP module (mandatory) *The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned either 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.* *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) *Usually, the module description from the syllabus (as stated in D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module*	
	Related knowledge area(s) (mandatory) *Mapping to the 10 selected CSP knowledge areas 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) *Yes (also if a part of the module covered this topic) or No (otherwise)*	
	Category/ies of capabilities (mandatory) *Mapping to the 4 category/ies of capabilities defined in*	

CSP Module Elements	CSP Module fields legend	CSP Module information
	the CSP Grant Agreement.	
	Learning outcomes and targets (mandatory) *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) *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 *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 2026, Lisbon*	
	Information on the sector (mandatory) *Indicates General, Maritime, Health, or Energy*	
	Pre-requisites (mandatory) *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) *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) *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 *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	
	Level (mandatory) *B (Basic), A (Advanced)*	
	Language (mandatory) *Indicates the spoken and the languages for the material and the assessment/evaluation*	Spoken: Material: Assessment:
Management /Logistics	**Provider(s)** (mandatory) *Name(s) of the providing organisation(s), e.g., beneficiary/ies*	
	Hosted of the module *Select the type of organization that hosted this implemented module (EH HEI, Company, other)*	
	Host details *A freetext to provide additional details about the host organization (name, location, specific department, etc.)*	
	Number of seminars/lectures held by industry experts: * *Required to report these KPIs in relation to the call.* *Indicate number of "From members of the consortium"*	

CSP Module Elements	CSP Module fields legend		CSP Module information
	as well as number of "Not from members of the consortium"		
	Contact (mandatory) *Full name(s) of the main contact person(s) including their email address*		
	Trainer(s) *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) *A list of tools that have been used for the implemented CSP module* *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 *How (e.g., where and when registration of learner took place) did learner have to register* *If there is no registration procedure, please write, "None"*		
	Admission criteria *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).* *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) *If there are no actions, please write, "None"*		
	ECTS *The number of ECTS* *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) *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) *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) *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	*Duration of the implemented CSP module (in hours)*	

CSP Module Elements	CSP Module fields legend		CSP Module information
	(mandatory)	*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** *Link to DCM, otherwise other link*		
	Location of activity modules, such as forums, quizzes, and assignments *Link to DCM, otherwise other link*		
	Location of community support *Link to DCM, otherwise other link*		
	Location of administrator documentation and configuration guides of tools used *Link to DCM, otherwise other link*		
	Hours of hands-on training, making use of the equipment purchased/leased within the framework of this action *Type "0" if you didn't use equipment purchased/leased within the framework of this action* *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) *Number of learners*		
	Number of learners per gender (mandatory) *Indicate per female, male, non-binary, prefer not to answer*		
	Number of learners per category (mandatory) *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) *Provides characteristics of learners, especially the following details, as they relate to CSP's KPIs:* • *Number of learners more than 45 years old* • *Number of learners, who are non-ICT graduates* • *Number of learners, who are cybersecurity self-trained* *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 up the figures for the KPIs*		

CSP Module Elements	CSP Module fields legend	CSP Module information
	Number of job-placements/internships carried out by the students* *Required to report these KPIs in relation to the call.* *Number in the organization member of the consortium* *Number in an external organization*	
	Have you collected the *number of applications* to the education programme(s) per gender, age, educational background, country of origin? *Required to report these KPIs in relation to the call.* *In case yes, Indicate gender, age, educational background*	
	The *number of students enrolled* to the education programme(s) per Age *Required to report these KPIs in relation to the call*	
	The number of students enrolled to the education programme(s) per educational background *Required to report these KPIs in relation to the call*	
	The number of students enrolled to the education programme(s) per Country of origin *Required to report these KPIs in relation to the call*	
	Evaluation method(s) (mandatory) *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) *The form that learners used to evaluate the course offer (reference or link)*	
	Evaluation forms of trainers (mandatory) *The form that trainers used to evaluate the outcomes (reference or link)*	
	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes (text or reference).* *If there are 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) *free text to describe the scenario*	
	Waived registrations *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.* • **Number of waived (payable) registrations *** • **In addition to the number of waived (payable) registrations, number of students benefiting from the support (financial or other) from the**	

CSP Module Elements	CSP Module fields legend	CSP Module information
	education institutions *	
	Number of female participants benefitting from financial support	
	Cost-benefit analysis of the modules *The amount of money paid for the course and the amount of income earned from the course* *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 **Brief suggestions to enhance the effectiveness of CSP training (Lessons learnt)**	**Recommendations for improving the module** *Brief practical suggestions to elevate and improve the future CSP training module quality*	*For example:* • *Enhance the training module with more interactive exercises.* • *Continuously update the module with the latest cybersecurity trends.*
	Recommendations for expanding the reach of the module *Brief practical suggestions to expand the reach to a wider audience and diversifying delivery methods*	*For example:* • *Partner with industry.* • *Promote the module through targeted marketing.*
	Recommendations for future initiatives *Brief practical suggestions and future recommendation for proactive strategies to further strengthen cybersecurity training initiatives and address emerging challenges*	*For example:* • *Implement Standard Cybersecurity Framework in syllabi.* • *Foster collaboration with industry clusters for ongoing professional development opportunities for the participants of the training.* • *Foster EU member state collaboration on cybersecurity training offerings.*
Employment	**Number of participants in education or recent graduates not yet employed** *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).* *If the answer is yes, indicate the figure by gender.*	
	Number of unemployed or inactive participants[9] *Participants which are, at the time of enrolment, unemployed, inactive and not recent graduates (see above).* *If the answer is yes, indicate the figure by gender.*	
	Number of employed participants *Participants which are, at the time of enrolment, in*	

[9] Same here

CSP Module Elements	CSP Module fields legend	CSP Module information
	employment. *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 activities/job placement *This includes partial or full employment, self-employment or similar.* *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 *This includes partial or full employment, self-employment or similar.* *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 *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.* *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 16: Template for planning the CSP modules offering.

CSP Module Elements	CSP Module [Fields legend]	CSP Module Information
Overview	**Code** *Mandatory field. Code format:* *For general modules: CSP[n]_x* • *[n] is the CSP module number (currently between 001 and 012)* • *x is the module offering type (see below)* *For sector-specific modules: CSP[n]_x_y* • *[n] is the CSP module number (currently between 001 and 012)* • *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 field. The title of the module as defined in the CSP catalogue (currently in D4.1)*	
	Title of the implemented CSP module *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 *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) *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 *Mandatory field. Yes (also if a part of the module covered this topic) or No (otherwise)*	
	Category/ies of capabilities *Mandatory field. Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.*	
	Learning outcomes and targets *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 *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 *Mandatory field. Indicates General, Maritime, Health, or Energy*	
	Pre-requisites	

CSP Module Elements	CSP Module [Fields legend]	CSP Module Information
	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) *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 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 *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	
	Level *Mandatory field. B (Basic), A (Advanced)*	
	Language *Mandatory field. Indicates the spoken and the languages for the material and the assessment/evaluation*	Spoken: Material: Assessment:
Management/ Logistics	**Provider(s)** *Mandatory field. Name(s) of the providing organisation(s), e.g., beneficiary/ies*	
	Contact *Mandatory field. Full name(s) of the main contact person(s) including their email address*	
	Trainer(s) *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 *Mandatory field. A list of tools that are to be used for the implemented CSP module.* *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 *How (e.g., where and when registration of learner will take place) will learner have to register.*	
	Admission criteria *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 *The number of ECTS*	
	Certificate of Attendance (CoA) *Mandatory field. Indicates Yes or No (and the conditions for yes, e.g., partial or full attendance, passing of exam)*	
	Exact dates, when offered *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*	

CSP Module Elements	CSP Module [Fields legend]		CSP Module Information
	Schedule and duration *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** *Link to DCM once available, otherwise other link.*		
	Location of activity modules, such as forums, quizzes, and assignments *Link to DCM once available, otherwise other link.*		
	Location of community support *Link to DCM once available, otherwise other link.*		
	Location of administrator documentation and configuration guides of tools used *Link to DCM once available, otherwise other link.*		
Outcomes	**Evaluation method(s)** *Mandatory field. Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.).*		
	Evaluation and verification of learning outcomes *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 *Number of offered cost free registrations* *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 particular restrictions of each entity, must be protected in several aspects, taking care of the confidentiality, integrity and availability of such data.

In addition, D4.2 which needs to document reports and training material on the Cybersecurity Principles and Management training modules had originally been due by M15.

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 Annex A: Template for the Documentation of Implemented CSP Modules via a (semi-)interactive tool for module providers. The admin portal 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

In this section the below evaluation forms template introduce:

- CyberSecPro Learners Evaluation Form
- CyberSecPro Trainer Evaluation Form
- Additional CyberSecPro Evaluation Template

CyberSecPro Learners Evaluation Form

CyberSecPro learners 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 Relevance• 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)?
Extremely Unlikely• Unlikely• Slightly Unlikely• 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?

Extremely Unlikely☐ Unlikely☐ Slightly Unlikely☐ 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

1. What is your age?
   Under 18• 18- 25• 26-34• 35-45• 45+-54• 55-65• More than 65•

2. What is your gender?
   Male• Female• Non-Binary• Prefer not to answer•

3. 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•

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

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

6. 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•

7. Are you an ICT graduate? Yes • No •
8. Are you self-trained in cybersecurity without any formal training in Cybersecurity topic? Yes • No •
9. 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?
   a) 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) •
   b) 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) •
   c) 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) •
   d) 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 •

   7.1 If yes, please answer the following questions:

   a) What is your age?
   Under 18• 18- 25• 26-34• 35-45• 45+-54• 55-65• More than 65•

   b) 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•

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

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

1. What is your age?
   Under 18• 18- 25• 26-34• 35-45• 45+-54• 55-65• More than 65•
2. What is your gender?
   Male• Female• Non-Binary• Prefer not to answer•
3. 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•
4. What is your Country of origin (the country where you were born)? _____

Annex E: Additional statistics of Implemented CSP Modules

In this section, additional statistics on the implemented CSP modules are provided.

- Number of Learners in Implemnted CSP Modules per Module Level
- Number of Implemented CSP Modules per Module Sector and Level
- Number of Learners in Implemnetd CSP Modules per Module Type

Number of Learners in Implemnted CSP Modules per Module Level

Figure 25 illustrates the distribution of learners across implemented CSP modules by the training level. The data indicates higher number of learners in basic-level modules (1394) compared to Advance-level modules (174). When CSP003 (related to T4.4) is also considered, these numbers increase to 1636. This distribution shows strong interest among learners in both training levels, with higher number of learners in the basic modules.

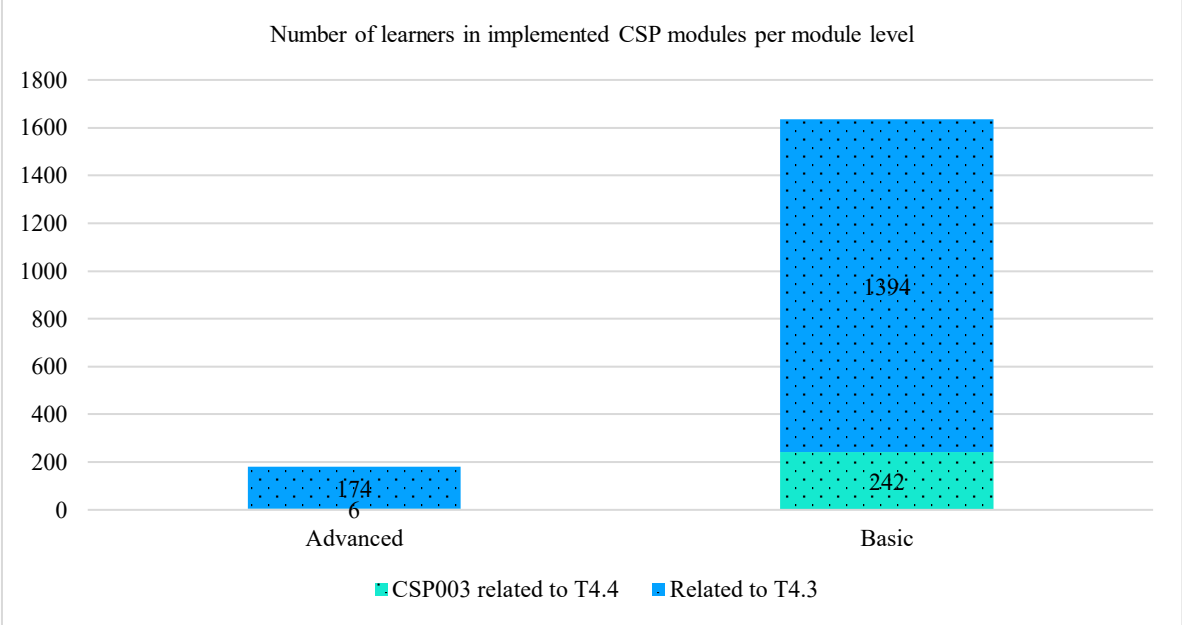


Figure 25: Number of learners in implemented CSP modules per module level

Number of Implemented CSP Modules per Module Sector and Level

Figure 26 presents the distribution of implemented CSP modules across industry sectors and training levels. In the basic modules related to T4.3, the energy sector leads with 13 modules, followed by general with 11 and maritime with 10 respectively. Health has the fewest with five implemnted modules in the basic level. Additionally, the number of advanced modules is lower across all sectors, ranging from 1 to 3. Energy has slightly more advanced modules (3).

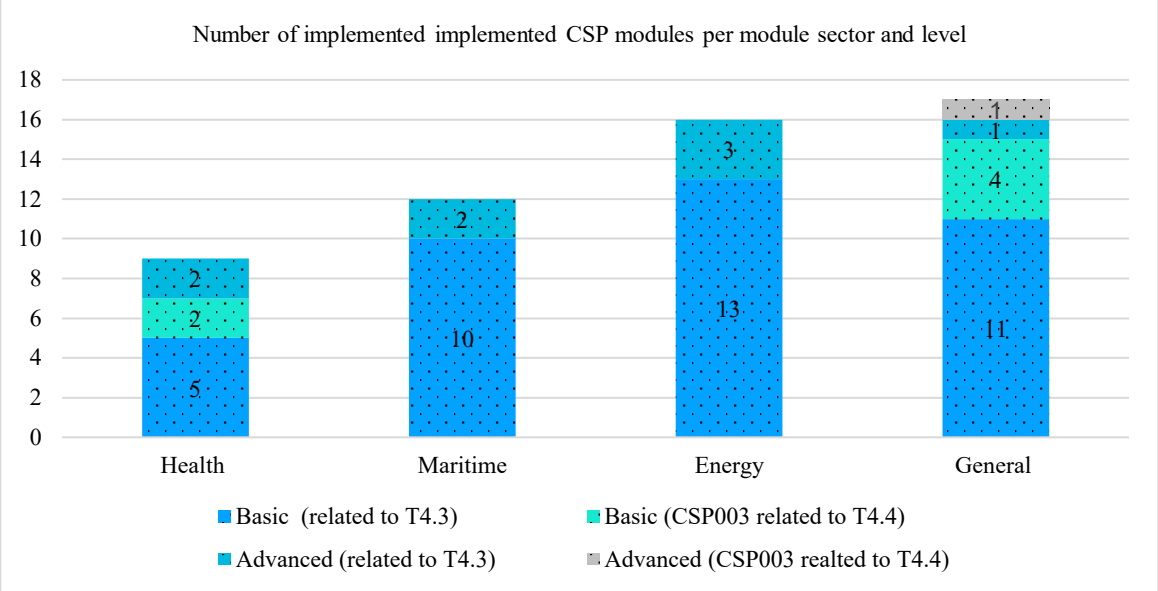


Figure 26: Number of implemented CSP modules per module sector and level

Number of Learners in Implemnetd CSP Modules per Module Type

Figure 27 presents the distribution of learners across CSP modules by module type. The results show that seminars account for the highest number of learners (647), followed by workshops (570), courses (197) and Cybersecurity exercise (154). When CSP003 (related to T4.4) is also taken into account, these numbers increase to seminars (688), workshops (722), and courses (252).

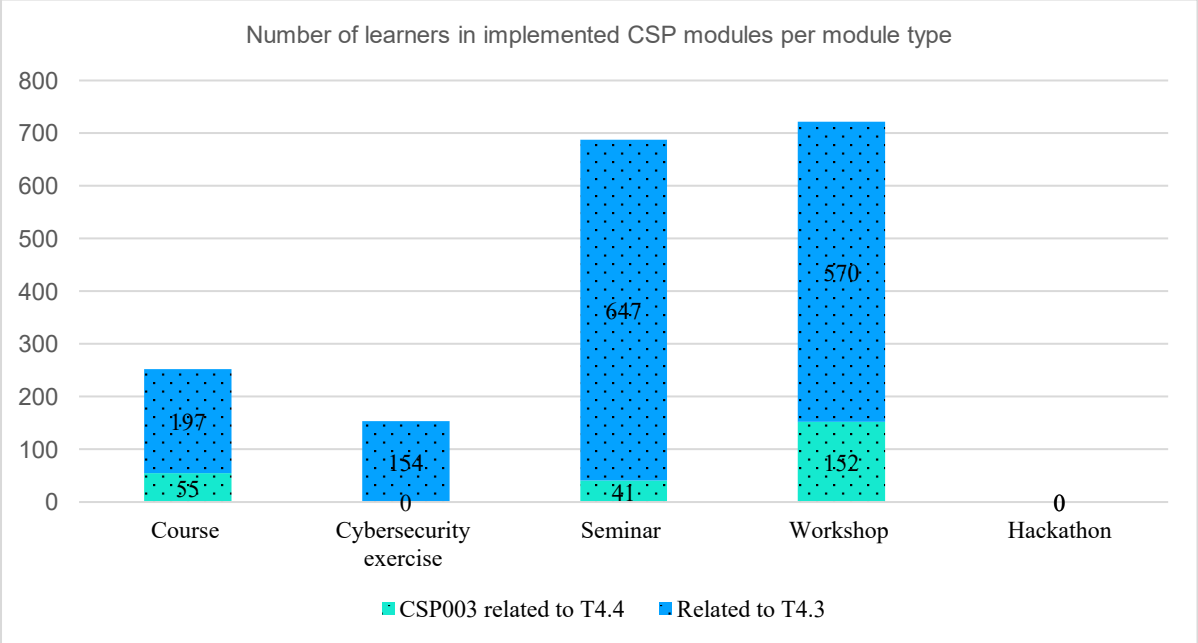


Figure 27: Number of learners in implemented CSP modules per module type