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

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

CyberSecPro

D4.5
Reports and Training Material on Cybersecurity Offensive Practices Modules

Document Identification	
Due date	2026-02-28
Submission date	2026-02-28
Version	1.0

Related WP	WP4	Dissemination Level	PU
Lead Participant	TalTech	Lead Author	Ricardo Lugo
Contributing Participants	UNSPMF, ACEEU, SINTEF, UMA	Related Deliverables	D2.2, D.2.3, D3.1, D3.3, D3.4, D3.5, D4.1, D4.2, D4.3 D4. 4, D5.1, D5.2, D5.3

Abstract: This deliverable presents the outcomes of T4.6 up to the conclusion of CyberSecPro in Month 39 (February 2026). Hence, it comprehensively records all CSP modules corresponding to the capability category Cybersecurity Offensive Practices 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 an initial 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 T4.6 “Operating the Training Modules on Cybersecurity Offensive Modules” up to Month 39 (February 2026). It documents all CSP Modules corresponding to the capability category “Cybersecurity Offensive Practices” implemented by the end of February 2026.

The document reports on the delivery of CSP010 Penetration Testing, CSP011 Cyber Ranges and Operations, and CSP012 Digital Forensics is related (partially by T4.6 and this deliverable) 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 D4.5, 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 D4.5, i.e. the documentation of implemented CSP modules, KPI 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 report. We then documented the CSP modules covering the Cybersecurity Offensive Practices capability, and implemented by M39.For this documentation we used the online tool[2] developed by ACEEU.

A total of 52 training modules were implemented across multiple sectors, including energy, health, maritime, and general cybersecurity, and delivered at both Basic and Advanced levels. The modules were offered through different formats, such as seminars, workshops, courses, and cybersecurity exercise, and involved a wide range of academic, research, and industrial providers. Enrolment data indicate strong engagement across all module categories, with particularly high enrolment in cross-sectoral and seminar-based trainings.

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

[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
Ricardo G. Lugo	TalTech
Danijela Boberic Krsticev	UNSPMF
Thorsten Kliewe, Jeldo Meppen	ACEEU
Nektaria Kaloudi	SINTEF
Cristina Alcaraz	UMA

Reviewers

Name	Beneficiary
Danijela Boberic Krsticev	UNSMPF
Nektaria Kaloudi	SINTEF
Jeldo Meppen	ACEEU (as QM)

History

Version	Date	Contributor(s)	Comment(s)
0.01	2023-11-13	Ricardo. G. Lugo	1st Draft of ToC
0.02	2025-11-01	Ricardo G. Lugo	Improved ToC
0.03	2025-11-17	Ricardo G. Lugo	Updated ToC
0.04	2025-11-17	Atiyeh Sadeghi	Upload SVN
0.05	2025-11-27	Atiyeh Sadeghi	Feedback on ToC
0.06	2025-12-01	Ricardo.G. Lugo	Update on content
0.07	2026-02-01	Ricardo G. Lugo	Sent for High level Review
0.08	2026-02-10	Danijela Boberic Krsticev	Review #1
0.09	2026-02-12	Nektaria Kaloudi	Review #1
0.10	2026-02-15	Ricardo .G.Lugo	Improvements based on feedback
0.11	2026-02-18	Jeldo Meppen	High level Review #2
0.12	2026-02-19	Danijela Boberic Krsticev	Review #2
0.13	2026-02-20	Ricardo G. Lugo	Improvements based on feedback
0.14	2026-02-21	Ricardo G. Lugo	Improvements based on meetings
0.15	2026-02-23	Ricardo G. Lugo	Updated tables and figures
0.16	2026-02-23	Ricardo G. Lugo	Sent for High-level review
0.17	2026-02-23	Nektaria Kaloudi	Review High-level review
0.18	2026-02-23	Ricardo G. Lugo	Final document for submission
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**A**	Advanced
	ACEEU	ACEEU GmbH
	AIT	AIT Austrian Institute of Technology GmbH
	APIRO	ApiroPlus Solutions Ltd
B	**B**	Basic
C	**C**	Course
	C2B	C2B Consulting
	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 , whereas workshops aim to build competence and application of skills.
	WP	Work Package
Z	**ZELUS**	Zelus IKE

Glossary of Terms

C **Course**

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

Cybersecurity Exercise

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

H **Hackathon**

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

S **Seminar**

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

SS **Summer Schools**

an educational course that happens during the summer

W **Workshop**

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

Terminology points

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

1. Introduction

Cybersecurity is expected to remain a critical concern for organisations across all sectors in the foreseeable future. Ongoing digitalisation of business processes and services, combined with a persistent shortage of suitably skilled professionals, is likely to exacerbate capability gaps in roles requiring specialised cybersecurity knowledge and practice. Addressing these challenges requires sustained investment in comprehensive education and training to prepare the next generation of practitioners for a threat landscape that is both dynamic and expanding. By strengthening links between academia and industry, CyberSecPro seeks to enhance cybersecurity education and professional training, thereby contributing to improved organisational resilience and broader societal security.

Accordingly, the CyberSecPro project aims to establish a distinctive professional training programme centred on state-of-the-art, hands-on modules. The programme is designed to accommodate heterogeneous training needs and varying levels of proficiency, offering both general modules and sector-specific content tailored to domains including the maritime, health, and energy sectors.

The rapid evolution of offensive security techniques, tooling, and adversary tools, tactics, techniques and procedures (TTPs) is continuously reshaping the cybersecurity landscape, increasing both the demand for practical defensive readiness and the need for controlled, responsible exposure to offensive practices. Within the CyberSecPro project, dedicated training offers have been developed and delivered to strengthen professionals' capabilities in offensive-practices-related domains, ensuring that learners can understand, apply, and critically evaluate offensive methods in ways that support detection, prevention, and resilient system design. This deliverable reports on the implementation and documentation of the training offers associated with offensive practices developed within the CyberSecPro project under Task 4.6. It provides a consolidated overview of each delivered training offer, including the hosting training site, the number of learners enrolled, the background of participating learners, and the evaluation instruments completed by both trainees and trainers. In addition, it documents relevant financial information for each offer (including income and any scholarships or sponsorships provided) and captures the outcomes of the training modules covering the offensive-practices-related capabilities delivered in T4.6. The report aims to provide transparent evidence of training deployment, uptake, and outcomes, thereby supporting assessment of the project's progress toward its capacity-building and skills development objectives in offensive-practices-related competencies.

1.1 Purpose and Scope

This deliverable has been produced within the context of CyberSecPro Work Package 4 (WP4), "Operating the CyberSecPro Professional Training Programme". Its objective is to provide comprehensive documentation for each CyberSecPro (CSP) training offer delivered under Task 4.6 (T4.6), with particular emphasis on the training modules addressing offensive-practices-related capabilities. Accordingly, the deliverable consolidates evidence for each implemented training offer, including the hosting training site, the number of learners enrolled, the background of participating learners, trainee and trainer evaluation instruments, and relevant financial information (income and any scholarships or sponsorships provided). In addition, it captures the learning outcomes associated with the offensive-practices modules delivered within T4.6, thereby enabling transparent reporting of deployment, uptake, and results.

Through systematic reporting on the implemented CSP training offers under T4.6, this deliverable directly supports several WP4 objectives, including:

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

To support the objectives of this deliverable, an administrative portal was established to enable CSP training providers to record, update, and manage documentation for each implemented training offer. The scope of this report is limited to the reporting and descriptive analysis of delivered training activities. It provides a structured overview of all implemented modules, including quantitative data on module delivery and enrolments, and a summary of deployment by module code, training level, module type, and sector.

The deliverable does not provide a detailed assessment of learning outcomes or training impact; rather, it supports systematic monitoring of training execution and progress toward WP4 capacity-building and skills development objectives. The reported results contribute to the project's evaluation framework and inform subsequent activities and deliverables.

1.2 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 templates and final CSP module design), D3.3, D3.4, D3.5 (on CSP module syllabi in three sector areas), D4.1 (including originally planned supply of modules in the CSP knowledge areas), D4.2, D4.3, D4.4(on synchronization structure of deliverables and template for Implemented CSP modules) D5.1, D5.2 (on evaluation forms), D5.3 (on certification schemes).

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 collected feedback from training providers as well as provided a follow-up questionnaire for WP5 and in return, it received the analysis of the evaluation forms filled by learners and trainers, as well as a compilation of best practices from the im-plemented 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 templates and final CSP module design), D3.3, D3.4, D3.5 (on CSP module syllabi in three sector areas), D4.1 (including originally planned supply of modules in the CSP knowledge areas), D4.2, D43, D4.4 (on synchronization structure of deliverables and template for Implemented CSP modules) D5.1, D5.2 (on evaluation forms), D5.3 (on certification schemes).

1.4 Structure of the Deliverable

Section 1 situates the deliverable within CyberSecPro WP4 and T4.6, clarifies its purpose and scope (documentation of training offers), and outlines linkages to related work packages and deliverables.

Section 2 describes the methodological approach and reporting framework. It also provides an overview of the CSP modules relevant to T4.6 (offensive-practices-related capabilities) and summarises the training offers implemented by the reporting cut-off, including module codes and titles, implementation periods, training levels, providers, sectoral focus, and learner enrolment.

Section 3 presents the structure, implementation, and reported outcomes of the T4.6 training offers. It includes descriptive statistics (and visualisations where applicable) on delivery and enrolment by module code, training

level, module type, and sector, alongside a dedicated discussion of operational, management, and logistical aspects of implementation.

Section 4 documents the MOOC syllabi associated with the T4.6 training offers.

Section 5 concludes by summarising key findings and their relevance to CyberSecPro capacity-building and skills development objectives.

The **Annexes** provide supporting materials: **Annex A** presents the documentation template used for implemented training offers; **Annex B** references the CSP module offering template reported in D3.1; **Annex C** justifies the use of the administrative portal as an interim documentation mechanism prior to full availability of the Dynamic Curriculum Management (DCM) system; and **Annex D** compiles the complete set of training-offer documentation collected via the administrative portal for all T4.6 implementations. **Annex E** offers other analyses of CSP modules in relation to modules and participants that may be of interest.

2. Methodology

In this chapter, we describe the approach adopted to document the implemented CSP modules and outline the specific information documented, as well as the reporting methods applied.

2.1 Data Collection Procedure

The template for documenting the implemented CSP modules was developed through an iterative process to ensure methodological consistency and alignment with WP/task requirements, European Commission reporting expectations, and feedback received after the first periodic report. Building on the module description template in D4.1, it was extended to capture implementation-specific information (delivery content, management and logistics, outcomes, financials, and best practices) not covered in the original format. The template was harmonised with the training module specifications in D3.1 to ensure coherence across work packages and to support comparability between planned and implemented activities. It was operationalised through the project's administrative portal to enable standardised data entry, centralised record-keeping, and efficient retrieval. In response to the call's KPIs and the SO4 indicator, additional data fields and a complementary learner questionnaire were incorporated (see Annex D). Reviewer and European Commission feedback was subsequently integrated, and the portal-based template was updated periodically to reflect evolving requirements. CSP providers are required to complete the documentation in the portal upon completion of each implementation and to update entries when amendments or additional reporting elements are introduced. This process is summarized in the below in Figure 1.

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

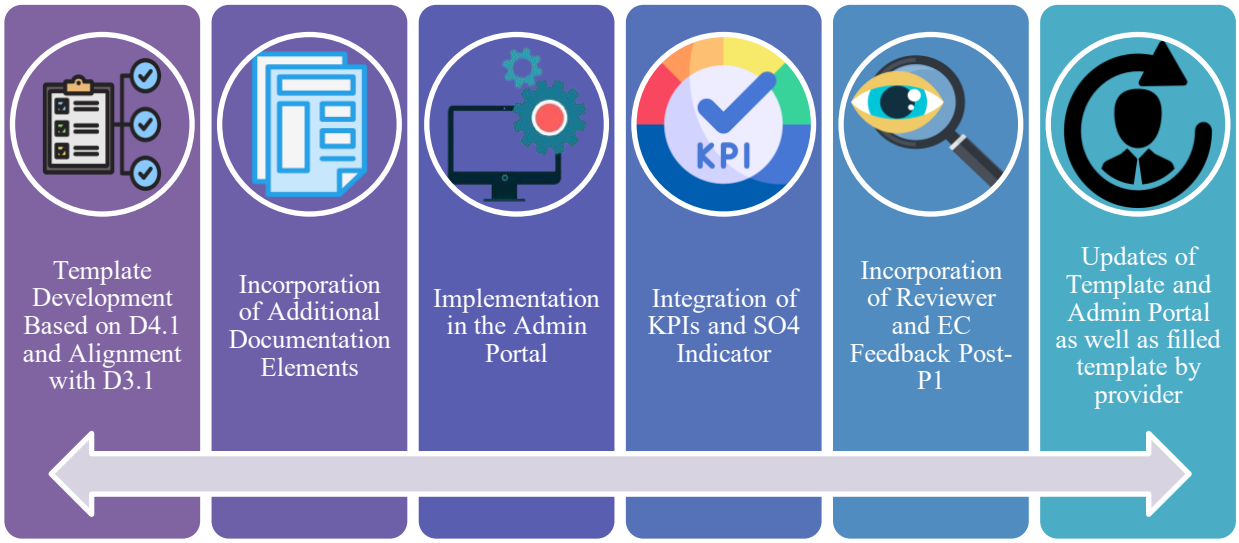

Figure 1: Process of Data collection Method

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

By extending the capabilities of the CyberSecPro internal admin portal (https://admin.cybersecpro-project.eu) and implementing the template described in Annex B for documenting implemented CSP modules, an administrative platform has been established that allows module providers to complete the documentation template for the implemented modules (see Figure 2).

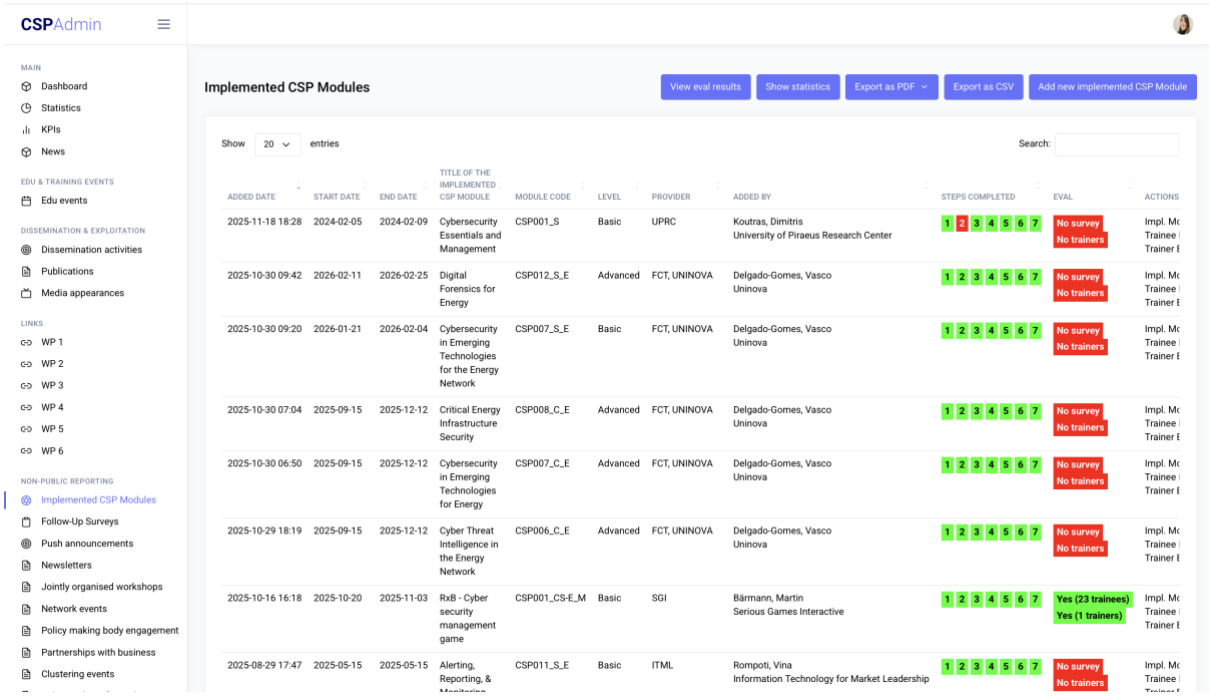

Figure 2 - CyberSecPro Admin Portal

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

As illustrated in Figure 1, the final template consists of five tabs—content, management and logistics, outcomes, financials, best practices, and employment—with all fields detailed in Annex A.

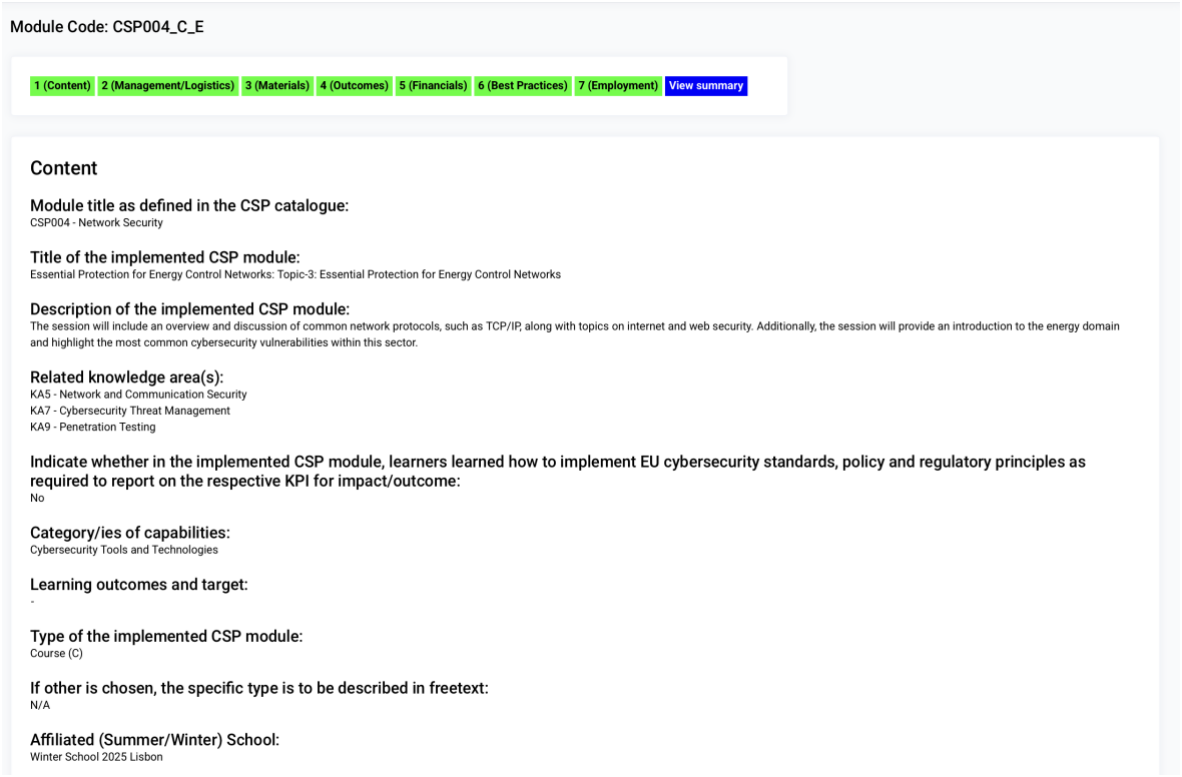

Figure 3 - Screenshot of Template for the Documentation of Implemented CSP Modules

Full documentation of implemented CSP modules was initially envisaged within the Dynamic Curriculum Management (DCM) system. However, because DCM is primarily designed to orchestrate teaching actions, a

separate documentation platform was adopted (see Annex C) to provide greater flexibility for trainers to report implementation outcomes. This approach also accommodated successive changes in KPIs and reporting requirements introduced by the European Commission and reviewers, and the associated need to update documentation fields rapidly and repeatedly.

3. Implemented CSP Modules Under T4.6

The T4.6 Offensive Cybersecurity Practices modules (CSP010–CSP012) addresses a core capability gap in the cybersecurity workforce: organisations cannot materially improve resilience against real adversaries without developing a practical understanding of attacker tools, tactics, and procedures (TTPs) in controlled, ethical, and legally compliant environments. Penetration testing, cyber range operations, and digital forensics align closely with the lifecycle of contemporary incidents, enabling learners to move beyond conceptual knowledge toward applied competence in identifying attack paths, validating security controls, prioritising mitigation, and collecting and interpreting evidence during investigations. This is particularly consequential for critical infrastructure sectors, where operational disruption, safety risks, and compliance obligations increase the need for demonstrable readiness. Moreover, implementation helps create the evidence base required for accountable project reporting: it demonstrates deployability across contexts, generates trainee and trainer feedback that supports continuous improvement, and establishes a scalable, standardised training portfolio that contributes directly to WP4 capacity-building and skills development objectives.

3.1 CSP Modules on Offensive Cybersecurity Practices

In this section, we briefly identify the CSP modules that align with Task 4.6 (T4.6) and are therefore within the scope of Deliverable D4.5, which documents training offers addressing offensive cybersecurity practices. Based on the mapping of CSP Knowledge Areas to capability categories (Table 1, derived from D4.1), T4.6 covers modules within Knowledge Area 9 (Penetration Testing) and Knowledge Area 10 (Cyber Incident Response), both of which correspond to the capability category Offensive Cybersecurity Practices. Accordingly, D4.5 reports the implementation and documentation of the following CSP modules: CSP010 Penetration Testing, CSP011 Cyber Ranges and Operations, and CSP012 Digital Forensics. As indicated in Table 1, CSP011 Cyber Ranges and Operations is relevant to both Knowledge Area 9 and Knowledge Area 10; the module is therefore reported once within D4.5, while its outcomes are interpreted across both capability domains (penetration testing and incident response).

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

CSP Knowledge Area	Capability Category	Module(s)
		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 T4.6 and in this deliverable, D4.5.

CSP010 "Penetration Testing"
This module is related to the CSP KA9: Penetration Testing, among others. This area is focused on simulating cyber-attacks to uncover and rectify security vulnerabilities. Additionally, this module can be related to the market analysis identified knowledge area: Ethical Hacking and Penetration Testing, among others.
CSP011 "Cyber Ranges and Operations"
This module is related to the CSP KA9: Penetration Testing and CSP KA10: Cyber Incident Response, among others. These areas focus on simulating cyber-attacks to uncover and rectify security vulnerabilities, as well as deal with the procedures for reacting to and recovering from cybersecurity incidents, respectively. Additionally, this general module can be related to the market analysis identified knowledge areas: Incident Response, Technical Skills, Analysis and Critical Thinking, Communication and Teamwork, among others.

CSP012 "Digital Forensics"
This general module is related to the CSP KA10: Cyber Incident Response, among others. This area deals with the procedures for reacting to and recovering from cybersecurity incidents. Additionally, this general module can be related to the market analysis identified knowledge area: Cybersecurity Forensics, among others.

3.2 Overview of Implemented CSP Modules Under T4.6

This section provides an overview of the most relevant information of all implemented CSP modules, organized according to T4.6. As shown in Table 2, it reports for each CSP module its corresponding code and title, the implementation period indicated by the start and end dates, the level, the provider, and the corresponding sector. In addition, the number of participating learners is documented. In total, 52 training modules related to Offensive Cybersecurity Practices have 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 T4.6

Module Code	Module Name	Start Date	End Date	Sector	Provider	Level	No. Of Learners
CSP010_H	Cybersecurity Hackathon: Introduction to CTF	2025-07-19	2025-07-19	General	PDMFC	A	41
CSP010_H	Hackathon	2026-01-24	2026-01-24	General	PDMFC	B	35
CSP010_S_E	Penetration Testing in Energy Sector	2024-05-10	2024-05-10	Energy	UPRC	A	7
CSP010_S_E	Penetration Testing in Energy Sector	2024-02-05	2024-02-09	Energy	UPRC	A	60
CSP010_W	Introduction to Penetration Testing and Nmap Tool Training	2023-10-10	2023-10-18	General	LAU, trustilio, Zelus	B	40
CSP010_W	B Network Vulnerability Assessment and Beyond: Nessus Hands on Training	2023-10-10	2023-10-19	General	LAU	B	40

Implemented CSP Modules Under T4.6

Module Code	Module Name	Start Date	End Date	Sector	Provider	Level	No. Of Learners
CSP010_W	Pentesting	2026-01-20	2026-01-20	General	COFAC	A	35
CSP010_W_H	Penetration Testing for Healthcare IT Infrastructures	2024-07-01	2024-07-02	Health	FP	A	25
CSP010_W_H	Penetration Testing in the Health Sector	2024-05-10	2024-05-10	Health	FP, Lau, TalTech, trustilio, UPRC	A	10
CSP010_W_H	Penetration Testing for Healthcare IT Infrastructures	2024-07-05	2024-07-05	Health	FP	A	30
CSP010_W_H	Penetration Testing-Active Directory- Healthcare	2024-07-01	2024-07-02	Health	FP	A	28
CSP010_W_M	Detection Engineering on a Cyber Range of a Maritime IT infrastructure-Active Directory	2024-07-01	2024-07-02	Maritime	FP	A	25
CSP010_W_M	Penetration Testing for Maritime IT Infrastructures	2024-07-01	2024-07-02	Maritime	FP	A	25
CSP010_W_M	Pentesting for Maritime	2024-09-01	2025-09-01	Maritime	C2B	B	6
CSP010_W_M	Detection Engineering on a Cyber Range of a Maritime IT infrastructure-Active Directory	2024-07-05	2024-07-05	Maritime	FP	A	25
CSP010_W_M	Penetration Testing for Maritime IT Infrastructures	2024-07-05	2024-07-05	Maritime	FP	A	35
CSP010_W_M	Penetration Testing-Active Directory- Maritime	2024-07-01	2024-07-02	Maritime	FP	A	28
CSP011_C_E	Leveraging Domain and Threat Intelligence in the Energy Domain	2024-07-01	2024-07-13	Energy	COFAC, LAU, SGI, PDMFC, UMA, FCT	B	35
CSP011_H	Cybersecurity hackathon	2024-06-21	2024-06-21	General	LAU, PDMFC	B	7
CSP011_H	Cybersecurity Hackathon: CyberSec Pro Cyber Range	2025-07-26	2025-07-26	General	PDMFC	A	41
CSP011_S_E	Cyber range and operations on SCADA	2024-09-01	2025-09-01	Energy	C2B	B	1
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2024-07-03	2024-07-03	Energy	ITML	B	35
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2024-09-10	2024-09-10	Energy	ITML	B	22
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2024-10-24	2024-10-24	Energy	ITML	B	50
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2024-11-26	2024-11-26	Energy	ITML	B	14
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-07-25	2025-07-25	Energy	ITML	B	29
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-03-24	2025-03-24	Energy	ITML	B	10
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-03-31	2025-03-31	Energy	ITML	B	10
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-04-25	2025-04-25	Energy	ITML	B	9
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-06-19	2025-06-19	Energy	ITML	B	6

Module Code	Module Name	Start Date	End Date	Sector	Provider	Level	No. Of Learners
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-05-15	2025-05-15	Energy	ITML	B	9
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-12-11	2025-12-11	Energy	ITML	B	11
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2025-12-17	2025-12-17	Energy	ITML	B	14
CSP011_S_E	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector	2026-02-17	2026-02-17	Energy	ITML	B	11
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2024-06-22	2024-06-22	Health	ITML	B	17
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2024-07-04	2024-07-04	Health	ITML	B	35
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2025-07-25	2025-07-25	Health	ITML	B	29
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2025-12-11	2025-12-11	Health	ITML	B	11
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2025-12-17	2025-12-17	Health	ITML	B	14
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2026-02-09	2026-02-09	Health	ITML	B	6
CSP011_S_H	Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector	2026-02-17	2026-02-17	Health	ITML	B	11
CSP011_S_M	Cyber Ranges and Operations in Maritime	2024-02-05	2024-02-09	Maritime	UPRC	B	60
CSP011_W	Detection Engineering on a Cyber Range -Active Directory	2024-07-05	2024-12-31	General	FP	A	10
CSP011_W_H	Detection Engineering on a Cyber Range of a Healthcare IT infrastructure-Active Directory	2024-07-05	2024-07-05	Health	FP	A	30
CSP011_W_M	Detection Engineering on a Cyber Range of a Maritime IT infrastructure-Active Directory	2024-07-05	2024-07-05	Maritime	FP	A	25
CSP012_C_M	Digital Forensic for Maritime	2024-09-01	2025-09-01	Maritime	C2B	B	1
CSP012_S_E	Digital Forensics for Energy	2025-07-14	2025-07-28	Energy	Uninova, FCT	A	15
CSP012_S_E	Digital Forensics for Energy	2026-02-11	2026-02-25	Energy	Uninova, FCT	A	15
CSP012_S_H	Digital Forensics for Health Sector	2024-06-22	2024-06-22	Health	ITML	B	17
CSP012_W	SOC Foundations and Digital Forensics: Incident Detection and Response	2025-07-25	2025-07-25	General		B	41
CSP012_W	Data Forensics	2026-01-00	2026-01-00	General	COFAC	B	35
CSP012_W_H	Digital Forensics in the Health Sector	2024-09-10	2024-09-10	Health	Zelus	B	27

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

This section summarises the implementation and documented outcomes of CSP training offers delivered under T4.6. Section 4.1 presents descriptive statistics for the implemented T4.6 modules, and—where relevant for completeness—includes reporting on overlapping implementations documented under T4.6. Section 4.2 synthesises key management and logistical aspects of delivery. Overall, the implementation profile reflects the CyberSecPro deployment strategy of ensuring baseline coverage across module areas where feasible, while scaling additional offerings in response to demonstrated demand.

4.1 Statistics of Implemented CSP Modules

This section presents descriptive statistics for CSP training offers implemented under T4.6, focusing on the offensive-practices modules CSP010 (Penetration Testing), CSP011 (Cyber Ranges and Operations), and CSP012 (Digital Forensics). These modules correspond to CSP Knowledge Area 9 (Penetration Testing) and CSP Knowledge Area 10 (Cyber Incident Response) within the Offensive Cybersecurity Practices capability category, with CSP011 spanning both knowledge areas.

- 4.1.1 Number of implemented CSP modules per module code
- 4.1.2 Number of Learners in 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 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.
The reported figures summarise key implementation characteristics, including the distribution of delivered offers across sectors, the sectoral composition of enrolments, and the balance of delivery across training levels. Collectively, the visualisations provide transparent reporting of deployment metrics for CSP010–CSP012 and establish a quantitative baseline for subsequent evaluation activities within the project.

4.1.1 Number of Implemented CSP Modules Per Module Code

Figure 4 presents the number of implemented CSP modules by module code within T4.6. CSP011 shows the highest level of implementation (28 modules), followed by CSP010 (17 modules). CSP012 has the lowest number of implemented modules (7). Overall, the distribution indicates a strong implementation emphasis on CSP010 and CSP011, reflecting their broad applicability across offensive-practices training contexts (i.e., penetration testing and cyber range/operations), while CSP012 contributes more selectively to the programme through targeted deliveries in digital forensics.

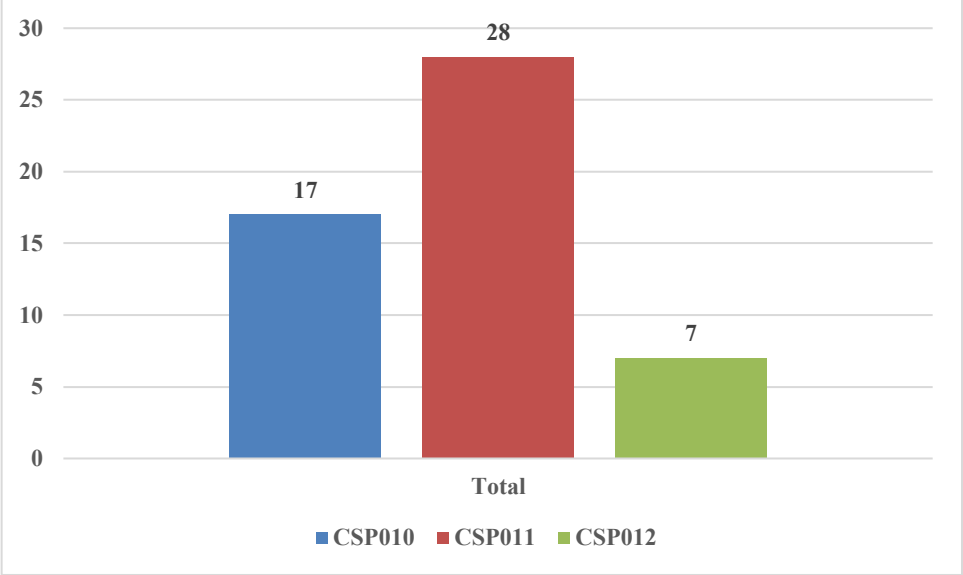

Figure 4 - Number of Implemented CSP Modules Per Module Code

4.1.2 Number of Learners in Implemented CSP Modules Per Module Code

Figure 5 illustrates total enrolments across implemented CSP modules, aggregated by module code. In line with observed demand, enrolments are concentrated in CSP011 (562), followed by CSP010 (495), while CSP012 accounts for 151 enrolments for a total of 1208 total enrolled learners. This distribution indicates particularly strong uptake of CSP010 and CSP011, plausibly reflecting the broad relevance of penetration testing and cyber range and operations-oriented content across sectors and roles. By contrast, CSP012 was delivered to comparatively smaller cohorts, which is consistent with the more specialised nature of digital forensics within the overall offensive-practices training portfolio.

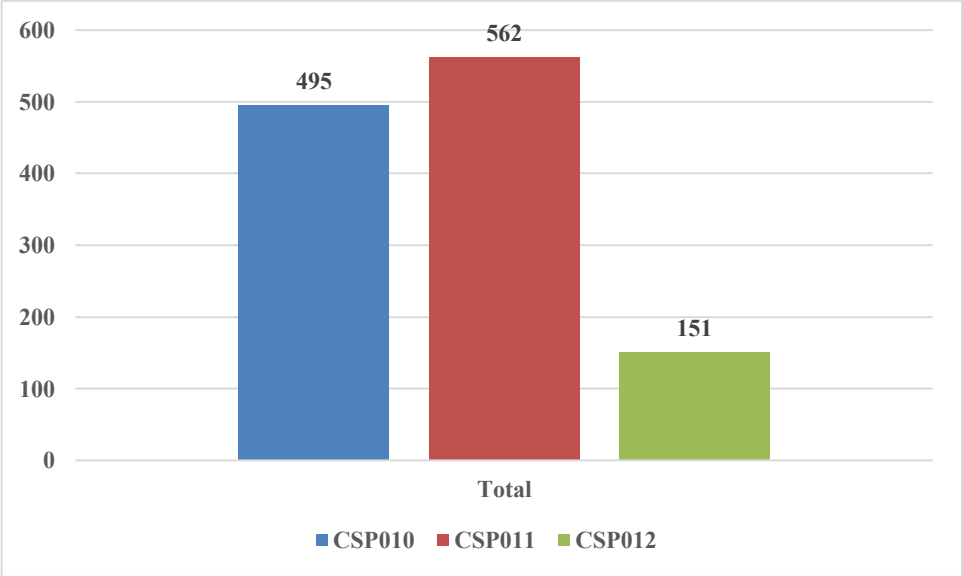

Figure 5 - Number of Learners in Implemented CSP Modules Per Module Code

4.1.3 Number of Implemented CSP Modules Per Module Level

Figure 6 - Number of Implemented CSP Modules Per Module Level
shows the distribution of implemented CSP modules by training level. Followed demand market, basic-level modules dominate the CSP implementation in T4.6, with 33 implementations compared to 19 implementations

of A-level modules. 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 Offensive Cybersecurity Practices.

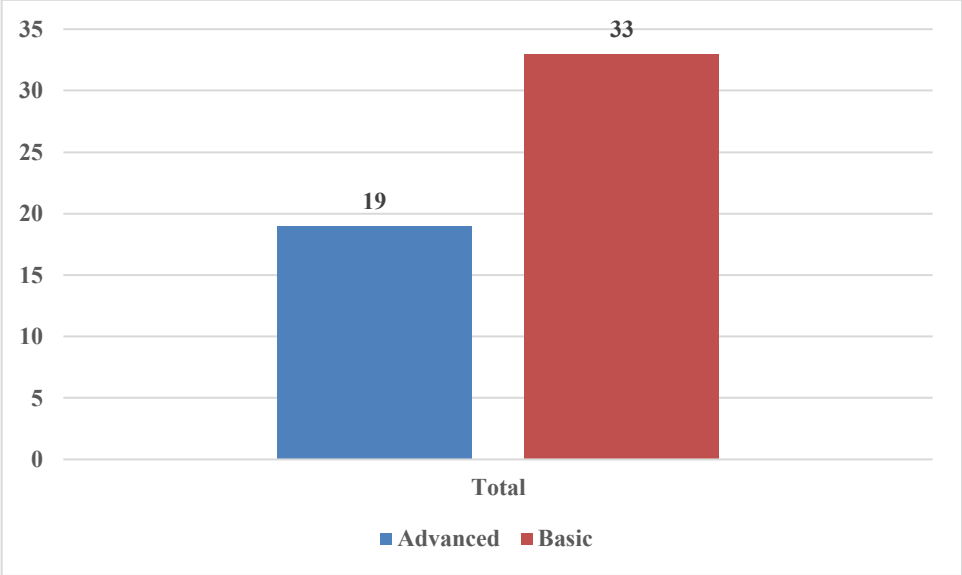

Figure 6 - Number of Implemented CSP Modules Per Module Level

4.1.4 Number of Implemented CSP Modules Per Module Level and Code Level

Figure 7 presents the distribution of implemented CSP modules by module code and training level for T4.6. In line with observed demand, CSP010 comprises 17 implementations, predominantly at the Advanced level (12), with 4 Basic implementations. CSP011 includes the highest number of implementations (28), delivered primarily at the Basic level (24), with 4 Advanced implementations. CSP012 comprises 7 implementations, mainly Basic (5) with 2 Advanced. Overall, the distribution indicates differentiated positioning across the T4.6 portfolio: CSP011 is implemented largely as foundational training, whereas CSP010 is delivered more frequently at an advanced level, with CSP012 providing more targeted coverage across both levels.

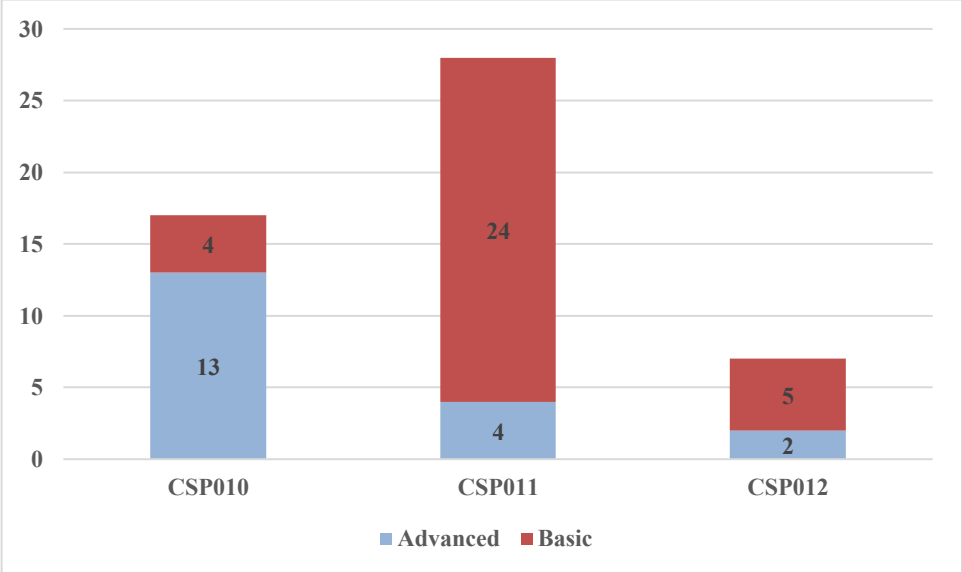

Figure 7 - Number of Implemented CSP Modules Per Module Level and Code

4.1.5 Number of Implemented CSP Modules Per Module Type

Figure 8 presents the distribution of implemented T4.6 CSP modules by delivery format. In line with observed demand, seminars (S) constitute the largest share of implementations (27), followed by workshops (19).

Hackathons (H) account for a smaller proportion (4), and courses (C) are least frequently implemented (2). Overall, the distribution indicates a clear emphasis on seminar-based delivery within the T4.6 portfolio, complemented by a substantial volume of workshop implementations that support practice-oriented learning. The smaller number of hackathons and courses suggests more selective use of these formats, potentially reflecting their higher organisational requirements and/or targeted application to specific learner cohorts.

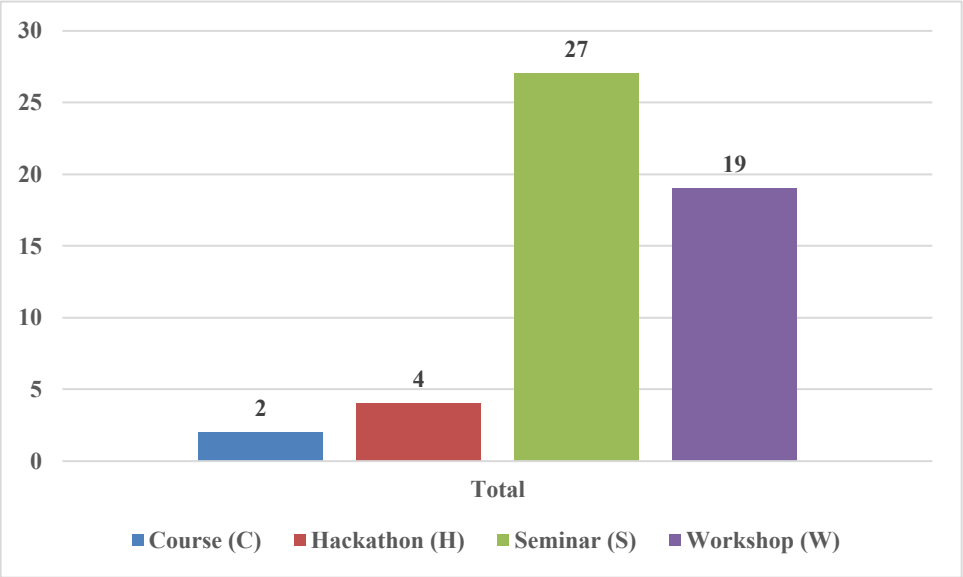

Figure 8 - Number of Implemented CSP Modules Per Module Type

4.1.6 Number of Implemented CSP Modules Per Module Type and Code

Figure 9 illustrates the distribution of implemented T4.6 CSP modules by delivery format and module code (CSP010–CSP012). Overall, implementation is concentrated in seminars and workshops, although the balance varies by module code. CSP010 is delivered primarily as workshops (13 implementations), supplemented by seminars (2) and hackathons (2), with no course-type implementations recorded. CSP011 is predominantly seminar-based (22 implementations), complemented by workshops (3) and hackathons (2), with one course implementation. CSP012 is implemented through a smaller number of offerings overall, delivered mainly as workshops (3) and seminars (3), with one course and no hackathons. This shows that the central role of seminar and workshop formats within the T4.6 portfolio, while also indicating differentiated delivery strategies across

CSP010–CSP012 (workshop-oriented for CSP010, seminar-oriented for CSP011, and a mixed but lower-volume profile for CSP012).

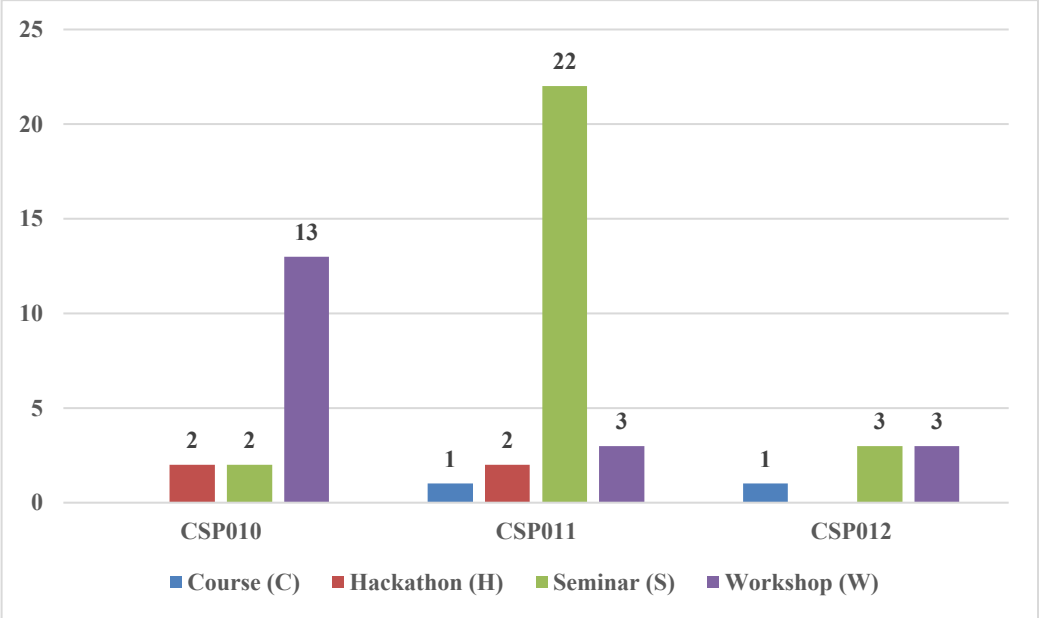

Figure 9 - Number of Implemented CSP Modules Per Module Type and Code

4.1.7 Number of Implemented CSP Modules Per Module Sector

Figure 10 presents the sectoral distribution of implemented T4.6 CSP modules by delivery format (course, hackathon, seminar, workshop). Implementation in the Energy sector is dominated by seminars (18), with a single course (1). In the General category, delivery is split between workshops (6) and hackathons (4). The Health sector shows a mixed profile, with workshops (6) and seminars (8). In Maritime, implementation is primarily workshop-based (7), supplemented by one seminar (1) and one ourse (1). Overall, the results indicate differentiated delivery strategies by sector: seminar-led provision in energy, workshop-led provision in maritime, and a more balanced mix of workshops and seminars in health, alongside hackathon activity concentrated in general (cross-sector) offerings.

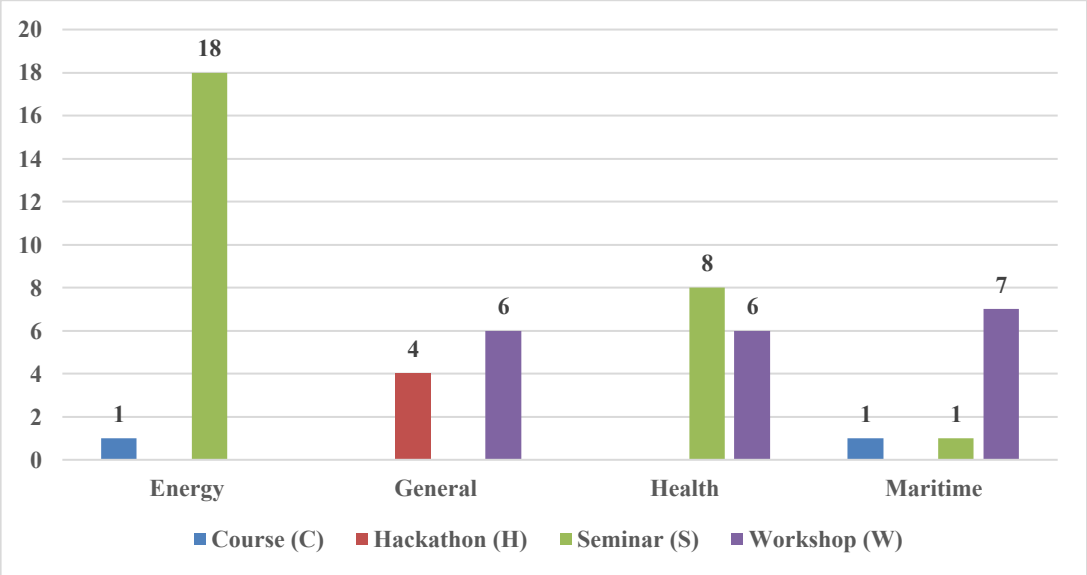

Figure 10 - Number of Implemented CSP Modules Per Module Sector

4.1.8 Number of Learners in Implemented CSP Modules Per Module Sector

Figure 11 presents the distribution of enrolments across implemented T4.6 CSP modules by sector. The Energy sector accounts for the highest number of learners (363 enrolments), followed by Health (290) and Maritime (230). The General category records 325 enrolments. Overall, the pattern indicates that learner participation is concentrated in sector-specific implementations—particularly energy, health, and maritime—while cross-sector ("general") offerings contribute a meaningful share of enrolments.

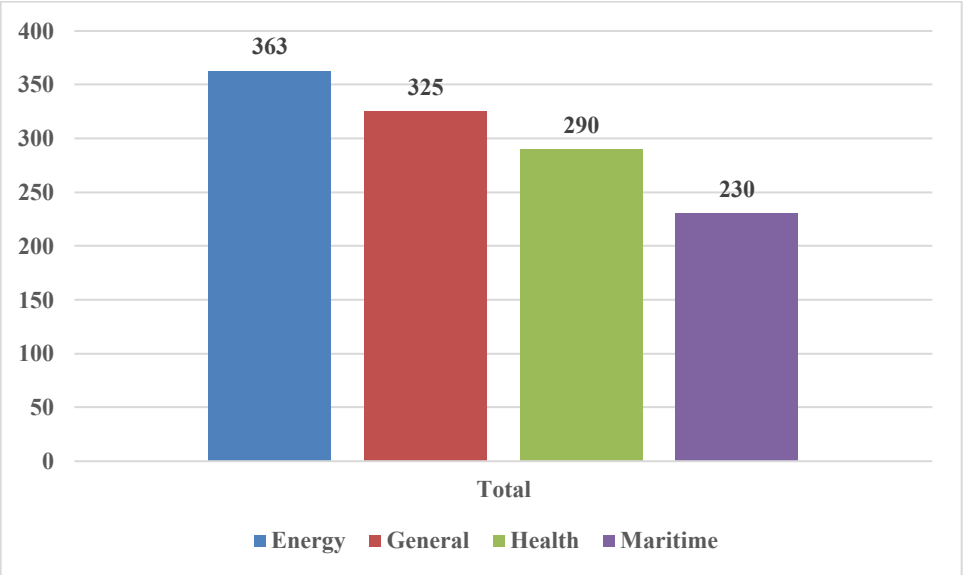

Figure 11- Number of Enrolments in Implemented CSP Modules Per Module Sector

4.1.9 Number of Implemented CSP Modules Per Module Sector and Code

Figure 12 presents the distribution of implemented T4.6 CSP modules across sectors, disaggregated by module code (CSP010–CSP012), and evidences distinct sectoral deployment profiles. CSP011 is strongly concentrated in the Energy sector (15 implementations), with additional delivery in Health (8), General (3), and Maritime (2). CSP010 shows a more dispersed implementation pattern, with the highest activity in Maritime (6) and General (5), followed by Health (4) and Energy (2). CSP012 is implemented at lower volume overall, distributed across Energy (2), General (2), Health (2), and Maritime (1). Overall, the results indicate that CSP011 primarily targets energy-sector needs, whereas CSP010 supports broader cross-sector delivery—particularly maritime and general contexts—and CSP012 provides more limited but multi-sector coverage.

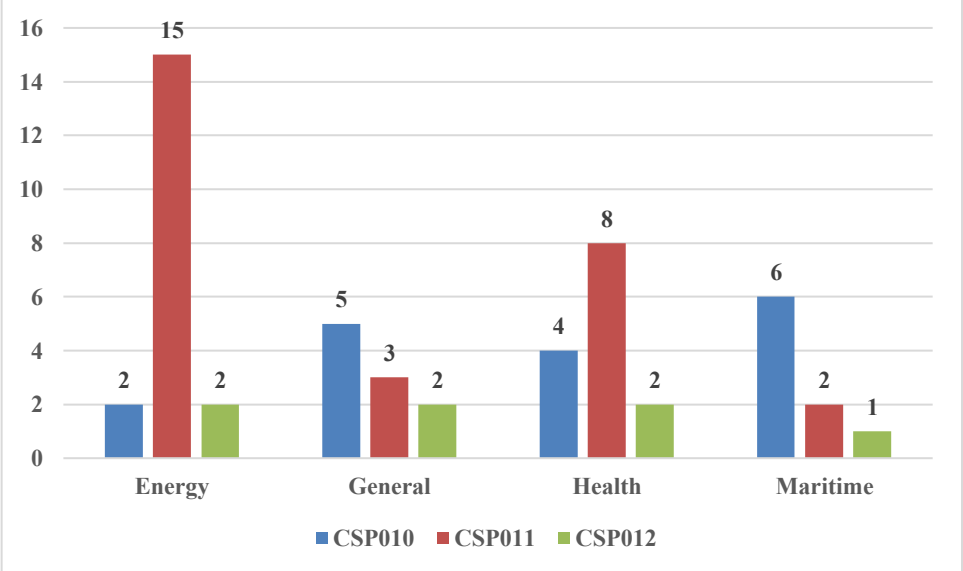

Figure 12: Number of implemented CSP modules per module sector and code

4.1.10 Number of Implemented CSP Modules Per Seasonal Schools

Figure 13 reports the distribution of implemented T4.6 CSP modules across seasonal-school programmes. Implementation is highly concentrated in Summer School 2025 Novi Sad – Week 1 (40 modules), followed by Summer School 2025 Novi Sad – Week 2 (4 modules). Summer School 2025 Novi Sad – Week 1 and Winter School 2025 Lisbon each account for one implemented module. Overall, the results indicate that the seasonal-school activity under T4.6 was delivered primarily through a single flagship event (Novi Sad Week 1), with limited additional implementation in subsequent seasonal-school sessions. No modules were delivered in the CYberHoT and CSP summer and Winterschools in 2024.

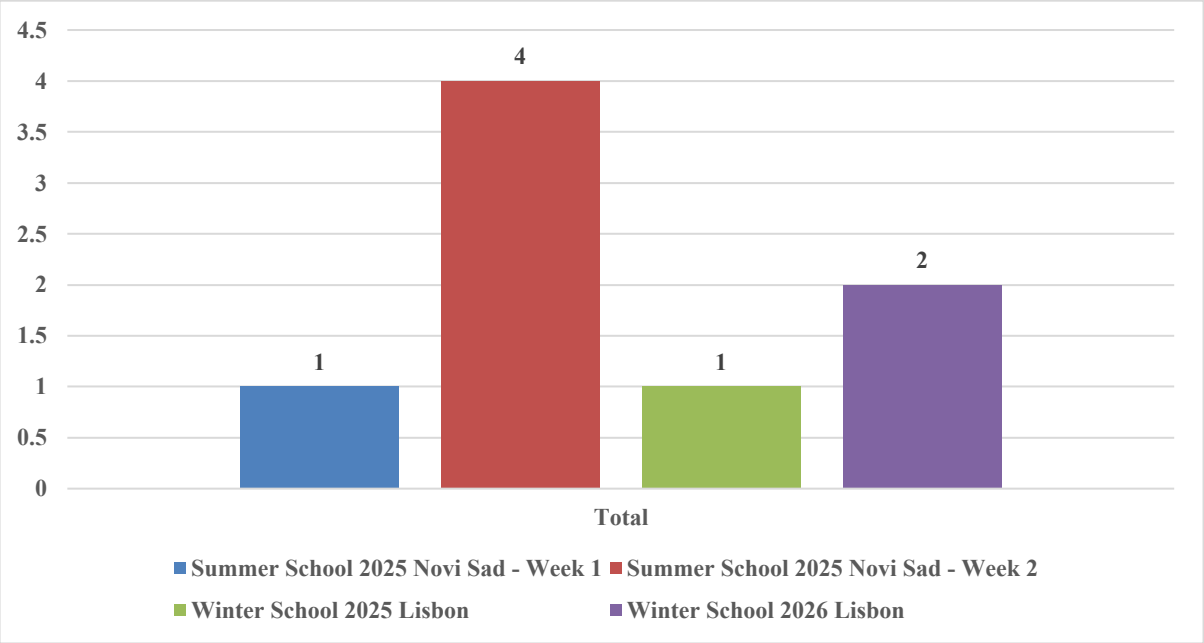

Figure 13 - Number of Implemented CSP Modules Per Seasonal Schools

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
- 4.2.7 Number of job-placements/internships carried out by the students
- 4.2.8 Background of learners
- 4.2.9 Hosting sites
- 4.2.10 Evaluation forms of learners and trainers

4.2.1 Actions to attract learners

The actions we have used to attract learners are as follows:
The strategies 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 especially 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 - Post Messages in the Dissemination Channel (CyberSecPro Project LinkedIn and Twitter /X)
-) 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 Twitter /X)

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

Income

There was no income generated from the implemented CSP module and seasonal schools for T4.6/D4.5.
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
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.
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.

Seasonal schools	Sponsorship	Scholarship
Winter School January 2026 Lisbon	Students from Serbia were financially supported by company JetBrains and OSCE office in Serbia. Total number of Serbian students which were supported is 8. 10 students from the University of Piraeus and 6 students-cadets from the Hellenic Airforce Academy were supported through Erasmus fellowships (HAF cooperates with UPRC in the project through Prof. Antonios Andreatos).	CyberSecPro organizers (PDMFC, COFAC) enabled 38 scholarships covering the admission-fee.

4.2.3 Registration process

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

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

Table 4 - Registration Process of CSP Seasonal Schools

Seasonal schools	Registration process of CSP seasonal schools
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/
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/

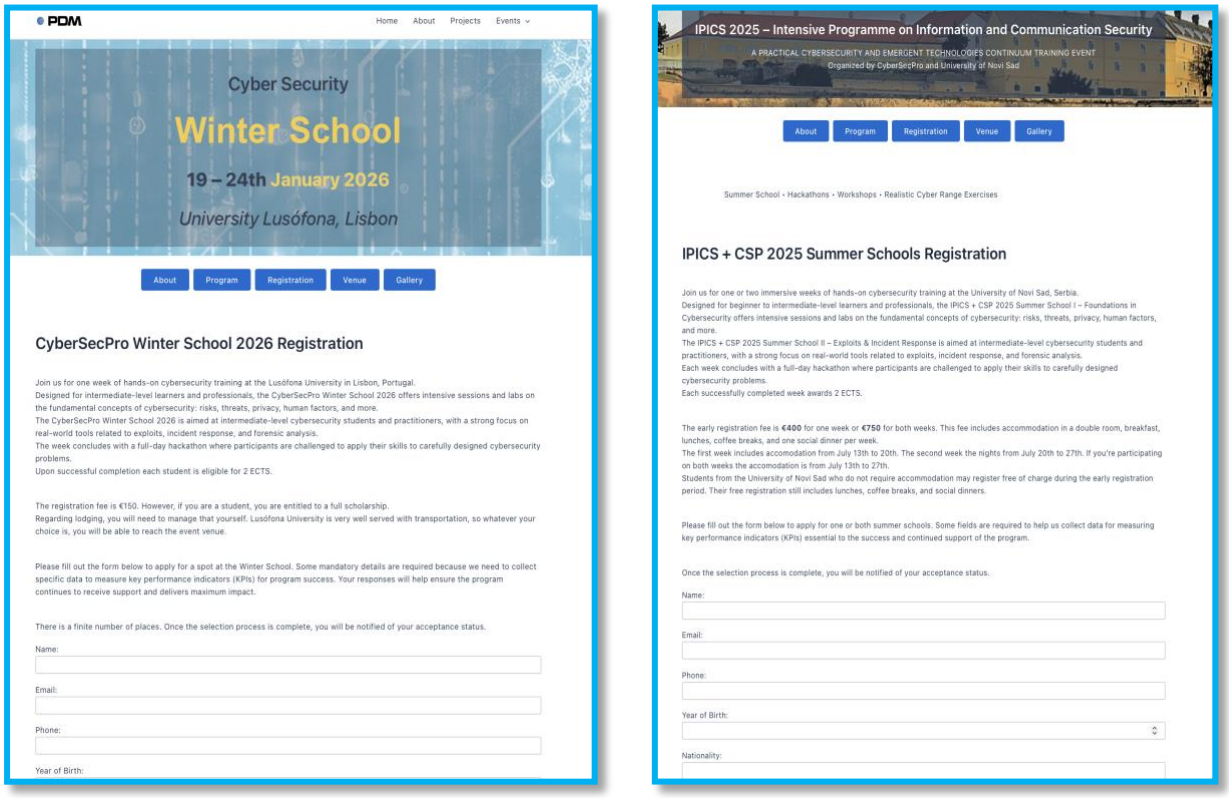

Figure 15 - Screenshot of CyberSecPro Seasonal Registration Page

4.2.4 Pre-requisites and Admission Criteria

For the seasonal schools, we usually requested a CV from applicants. The host of seasonal schools 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.

In addition, in one of the seasonal events 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.

Table 5 - Prerequisites and Admission Criteria Description

Seasonal schools	Admission Criteria
Winter School 2025 Caparica	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.
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 reward to learners

Certificates are the one the tangible reward across the implemented CSP modules. As illustrated in Figure 16, the majority of modules award certificates upon full attendance, while a smaller number also link with passing exam, or other defined criteria. Certificates are awarded by several partner organizations, including COFAC, PDMFC, LAU and UNINOVA, highlighting the institution involvement in organizing seasonal schools. Also, ECTS credits as additional tangible rewards for learners were and are being awarded by some events.

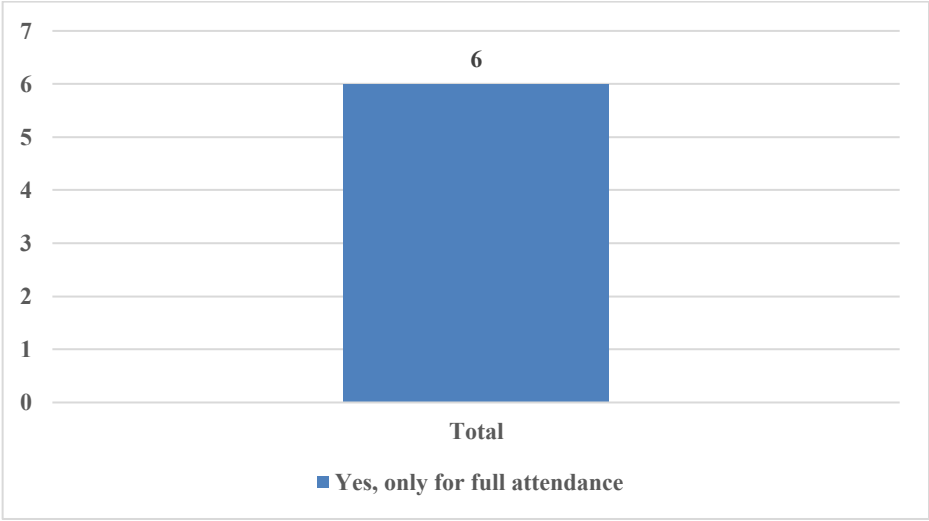

Figure 16 - Number of Implemented CSP Modules Award Certificate

As most of the tangible rewards are related to seasonal schools, all such rewards are listed in Table 6.

Table 6 - Tangible Reward to Learners from Seasonal Schools

Seasonal schools	ECTS rewarded	Certification and awarding organization
Winter School 2025 Caparica	2 ECTS upon successful completion of the program	Learners got certificate of attendance signed by UNINOVA and FCT.
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	2 ECTS upon successful completion of the program	Learners got certificate of attendance signed by PDMFC.and UNSPMF.
Winter School January 2026 Lisbon	2 ECTS upon successful completion	Learners got certificate of attendance signed by COFAC.

4.2.6 Learning Outcomes

The learning outcomes of all implemented CSP modules related to Offensive Cybersecurity Practices are largely consistent with those designed in D3.1, with no significant deviations observed. It is copied here for ease of reference (Table 7).

Table 7 - Learning Outcomes for T4.5 CSP Modules

Related CSP to T4.6	Learning Outcomes
CSP010 – Penetration Testing	By the end of the training, learners gained the following: Knowledge: • In-depth understanding of penetration testing methodologies and frameworks. • Comprehensive knowledge of legal and ethical considerations for penetration testing engagements. • Advanced understanding of network protocols, vulnerabilities, and exploitation techniques. • Solid grasp of operating system vulnerabilities, web application security testing methodologies, and mobile application security principles. • Awareness of cloud security concepts and penetration testing techniques. • Knowledge of advanced penetration testing tools and scripting for automation. • Understanding of social engineering techniques and their application in penetration testing. • Knowledge of professional ethics and legal requirements for penetration testers. **Skills:** • Conduct thorough information gathering and reconnaissance using advanced tools and techniques. • Perform advanced network scanning and vulnerability assessments to identify and exploit vulnerabilities. • Penetrate and exploit operating systems, web applications, and mobile applications using advanced tools and techniques. • Develop and execute post-exploitation strategies for maintaining access and escalating privileges. • Write comprehensive and informative penetration testing reports, documenting findings and recommendations. • Effectively communicate test results and vulnerabilities to both technical and nontechnical audiences. • Apply ethical hacking techniques and social engineering in controlled, simulated environments. • Utilise scripting for automation and custom exploit development. Competencies: • Critical thinking and problem-solving in complex penetration testing scenarios. • Ability to analyse information, identify vulnerabilities, and develop effective exploitation strategies. • Strong analytical and technical skills to utilise advanced penetration testing tools and methodologies. • Effective communication and collaboration skills to work with clients and stakeholders. • Adaptability and continuous learning to stay updated with evolving threats and technologies. • Ability to prioritize risks, make ethical decisions, and act responsibly in penetration testing engagements. • Leadership potential in planning, conducting, and reporting on penetration testing projects.

Related CSP to T4.6	Learning Outcomes
CSP011 – Cyber Ranges and Operations	By the end of the training, learners gained the following: Knowledge: • In-depth understanding of various types of cyber ranges and their applications (virtual, cloud-based, hardware-based). • Solid grasp of industry best practices and standards for cyber range operations. • Gain interdisciplinary knowledge from Computer networks, databases, and Web programming. • Comprehensive knowledge of ethical considerations and responsible use of cyber ranges. • Understanding of cybersecurity frameworks and methodologies utilised in cyber range exercises (incident response, vulnerability assessment). • Awareness of emerging trends and future directions in cyber range technology. • Knowledge of security best practices for managing and maintaining cyber range environments. • Understanding of data backup, recovery, and disaster planning in cyber range contexts.. Skills: • Navigate and utilise simulated cyber environments with proficiency. • Deploy and configure security controls, firewalls, and intrusion detection/prevention systems. • Analyse network traffic to identify indicators of compromise (IOCs) and respond to simulated cyberattacks. • Develop and execute incident response playbooks and containment strategies within controlled environments. • Design and configure basic cyber range exercises using industry-standard frameworks (e.g., MITRE ATT&CK). • Evaluate and utilise various cyber range platforms for different use cases (training, vulnerability testing, research). • Build and utilise basic custom cyber range tools and scripts for automation and enhanced analysis. • Effectively communicate findings and lessons learned from cyber range exercises Competencies: • Critical thinking and problem-solving in complex cyber range scenarios. • Ability to analyse network traffic, identify malicious activity, and make informed decisions during simulated incidents. • Adaptation and continuous learning to stay updated with evolving cyber threats and best practices. • Effective communication and collaboration skills to work with instructors, peers, and other stakeholders. • Leadership potential in designing, managing, and facilitating cyber range exercises. • Ability to prioritise risks, make ethical decisions, and act responsibly in cyber range operations. • Competence in utilising cyber ranges for effective cybersecurity training, testing, and research purposes.

Related CSP to T4.6	Learning Outcomes
CSP012 – Digital Forensics	By the end of the training, learners gained the following: Knowledge: • Knowledge of digital forensics methods, best practices and tools. • Knowledge of digital forensics analysis techniques. • Knowledge of digital forensics testing techniques. • Knowledge of criminal investigation methodologies and procedures. • Knowledge of malware analysis tools. • Knowledge of cyber threats and vulnerabilities. • Advanced knowledge of cybersecurity attack tactics and techniques. • Knowledge of legal framework related to cybersecurity and data protection. • Knowledge of operating systems security • Computer network security. Skills: • Work ethically and independently without bias. • Retrieve information while preserving its integrity. • Identifying, analysing, and correlating cybersecurity events. • Maintain chain-of-custody procedures to ensure the admissibility of digital evidence. • Conduct network forensics investigations and analyse network traffic logs for malicious activity. • Extract and analyse digital evidence from mobile devices (Android, iOS). • Visualize complex digital forensic data for clear communication in various settings. • Report and present digital evidence in an understandable way. • Produce a detailed and objective investigative report. Competencies: • Critical thinking and problem-solving in complex digital forensic scenarios. • Ability to analyse digital evidence, identify relevant indicators, and draw sound conclusions. • Attention to detail and meticulousness in handling and processing digital evidence. • Effective communication and presentation skills to articulate technical findings to technical and non-technical audiences. • Adaptability and continuous learning to stay updated with evolving technologies and cyber threats. • Ethical decision-making and adherence to legal regulations in digital forensic investigations. • Independent ability to conduct and manage digital forensic investigations from start to finish.

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

Table 8 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 8 - Number of Job-placements/internships Carried Out by the Students

	Related to T4.6
in the organization member of the consortium	33
in an external organization	10

4.2.8 Background of Learner

This section 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 17 shows the number of learners enrolled in CSP modules by gender. The results indicate that male learners make up by far the largest group. There are 840 (69.5%) male enrolments, 358 (29.6%) female learners, and 10 (.8%) non-binary learners, for a total of 1208 learners.

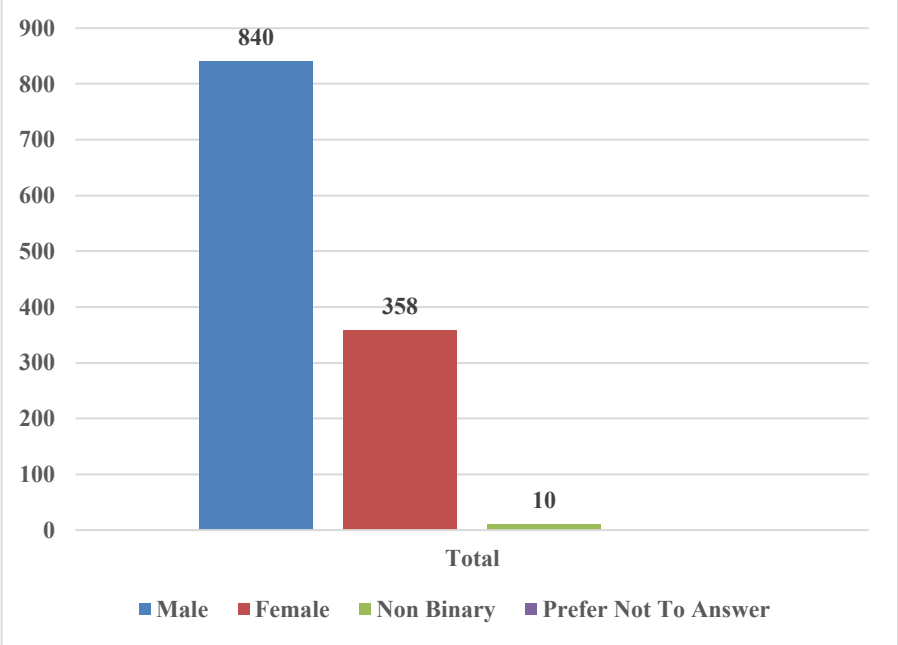

Figure 17 - Number of Learners in CSP Modules Per Gender

4.2.8.2 Number of Learners in CSP Modules Per Age

Figure 18 shows the number of learners enrolled in CSP modules across different age groups. Surprisingly most learners are concentrated in the 18-24 (389) age group, which has by far the highest participation. The second largest group is learners aged 25-34 (352). Also, learners 35 and over (221 total)[3] shows that professionals also were interested on learning offensive cybersecurity practices. Very few learners (11) are in the 55–65 age group, and there are no learners under 18 or over 65. Overall, the data indicates that CSP modules mainly attract young adults, particularly those between 18 and 44 years. old. Overall, the age profile indicates that T4.6 training primarily attracts early-career learners (18–34), with progressively lower participation in older age groups.

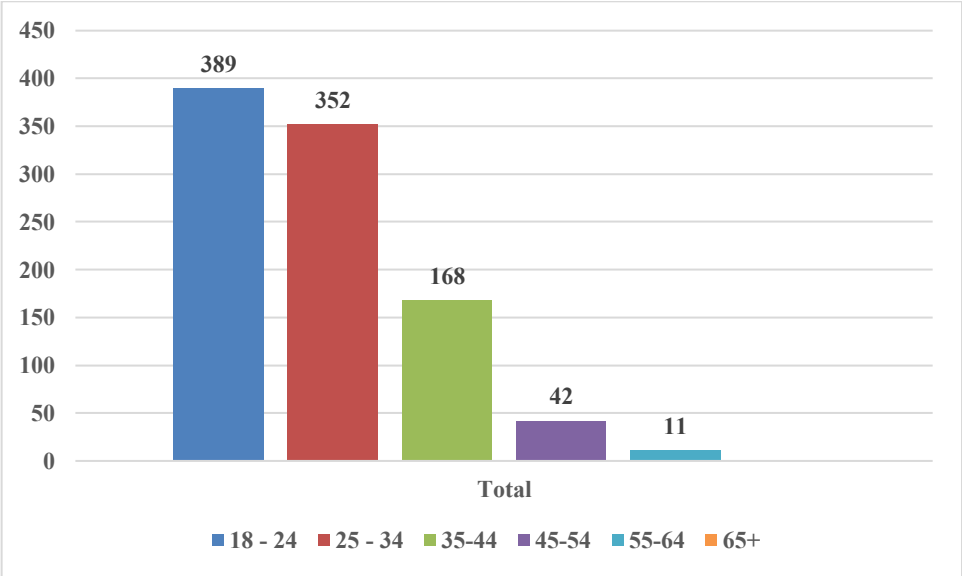

Figure 18 - Number of Learners in CSP Modules Per Age

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

4.2.8.3 Number of Learners in CSP Modules Per Educational Background

Figure 19 summarises learners' educational backgrounds across the implemented T4.6 CSP training offers. Participation is concentrated among learners with tertiary education, with undergraduate degrees (BSc/BA) representing the largest group (426 learners), followed by master's degrees (287) and PhD holders (104). Smaller numbers are reported for some college/no degree (23) and high school diploma (18), while no learners are recorded in the remaining categories (e.g., less than high school or other). Overall, the educational profile indicates that T4.6 training primarily attracts learners with established academic qualifications, which is consistent with the technical and specialised character of the offensive cybersecurity practices portfolio.

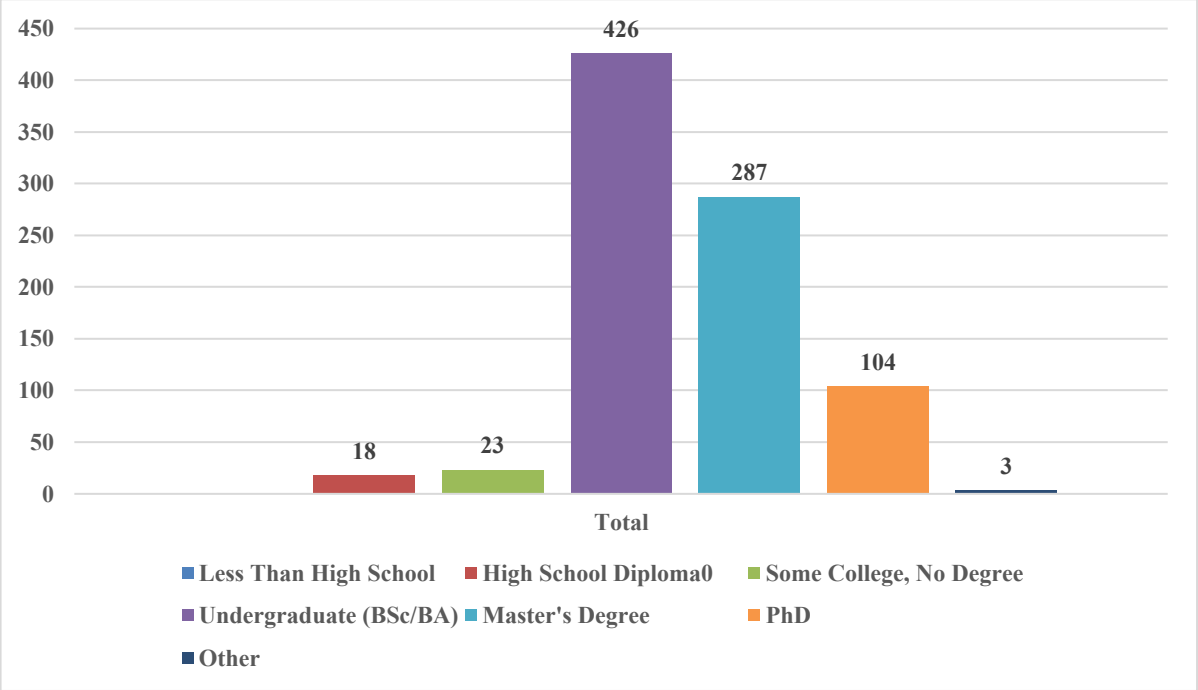

Figure 19 - Number of Learners in Implemented CSP modules Per Educational Background

4.2.8.4 Professional Experience and Affiliation

Figure 20 summarises learners' backgrounds across the implemented T4.6 training offers. Students constitute the largest cohort (671), indicating strong uptake among learners in formal education pathways. The next largest group comprises employees (233), followed by developers (148) and academic personnel (118). Employers account for 99 learners, while practitioners (85) and officers (65) represent smaller but still substantive segments. Overall, the distribution indicates that the T4.6 portfolio attracted a heterogeneous audience spanning early-career learners and active professionals, supporting both foundational skills development and continuing professional upskilling.

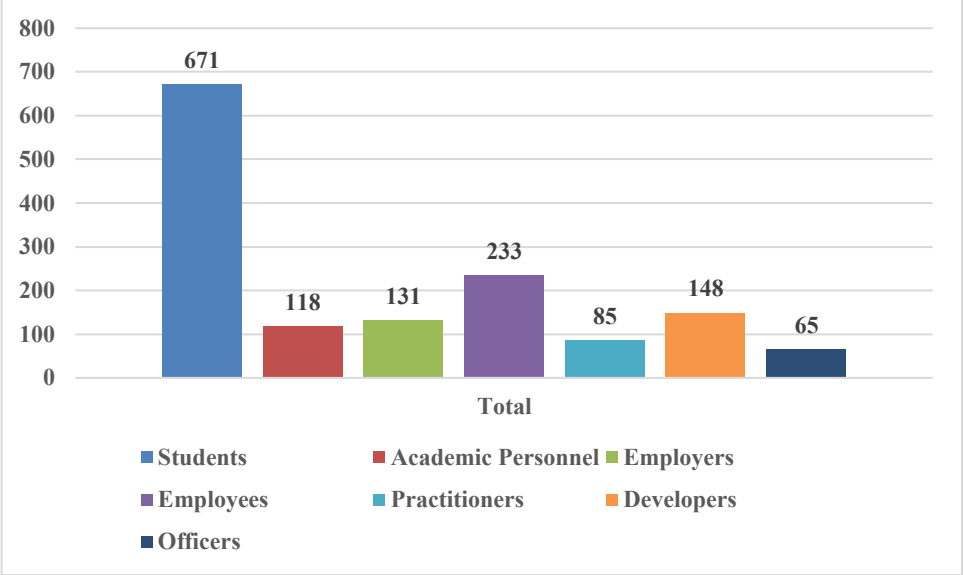

Figure 20 - Learners Professional Experience and Affiliation

Table 9 presents some project KPIs related to background characteristics of learners. Regarding age distribution, higher number of learners over 45 years old (136 learners). In terms of educational background, it has involved 122 non-ICT graduates and 230 reported self-trained learners.

Table 9 - Project KPIs Related to Learner's Background

Learners Background	Related to T4.6
Number of learners more than 45 years old	136
Number of learners, who are non-ICT graduates	122
Number of learners, who are cybersecurity self-trained	230

4.2.9 Hosting site

Figure 21 presents the distribution of implemented T4.6 CSP modules by host type. The results indicate that companies constitute the largest group of hosts (20 implementations), while EU higher education institutions (EU HEIs) accounted for 17 implementations, and other (public organisations) host types each account for 12 implementations. Overall, the distribution suggests a broadly diversified hosting landscape with a modest predominance of industry-hosted delivery, complemented by substantial participation from higher education and other organisations in deploying offensive-practices training offers.

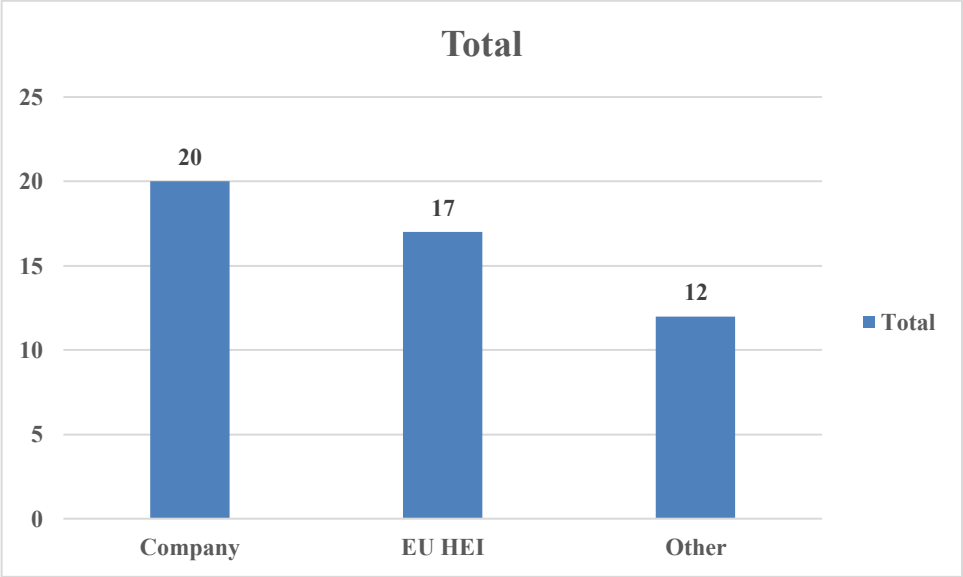

Figure 21 - Number of Implemented CSP Modules Per Module Host

4.2.10 Evaluation forms of learners 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 CyberSecPro training modules. The templates were developed within a DCM system, and feedback was collected online (see D3.1 for further details). Accordingly, the CyberSecPro 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 trainers was developed based on a review of existing evaluation frameworks as well as CyberSecPro context (refer to D5.1 for further details). So, this comprehensive evaluation had used afterward. 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.
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 introduce the evaluation forms developed within WP5 and implemented in the admin portal to collect data online.

CyberSecPro Learners Evaluation Form

The evaluation is conducted from the learner's perspective through a digital "Evaluation Survey" integrated into the CSP Admin Portal, where trainers can independently design and customise surveys for each module by selecting relevant pre-defined questions covering areas such as content, structure, instruction, platform, interaction, impact, and overall insights; once finalised, the system automatically generates a unique URL and QR code to enable easy distribution of the survey to learners via multiple digital channels. Figure 22 shows a Screen shot of CyberSecPro learner Evaluation Form in the Admin Portal.

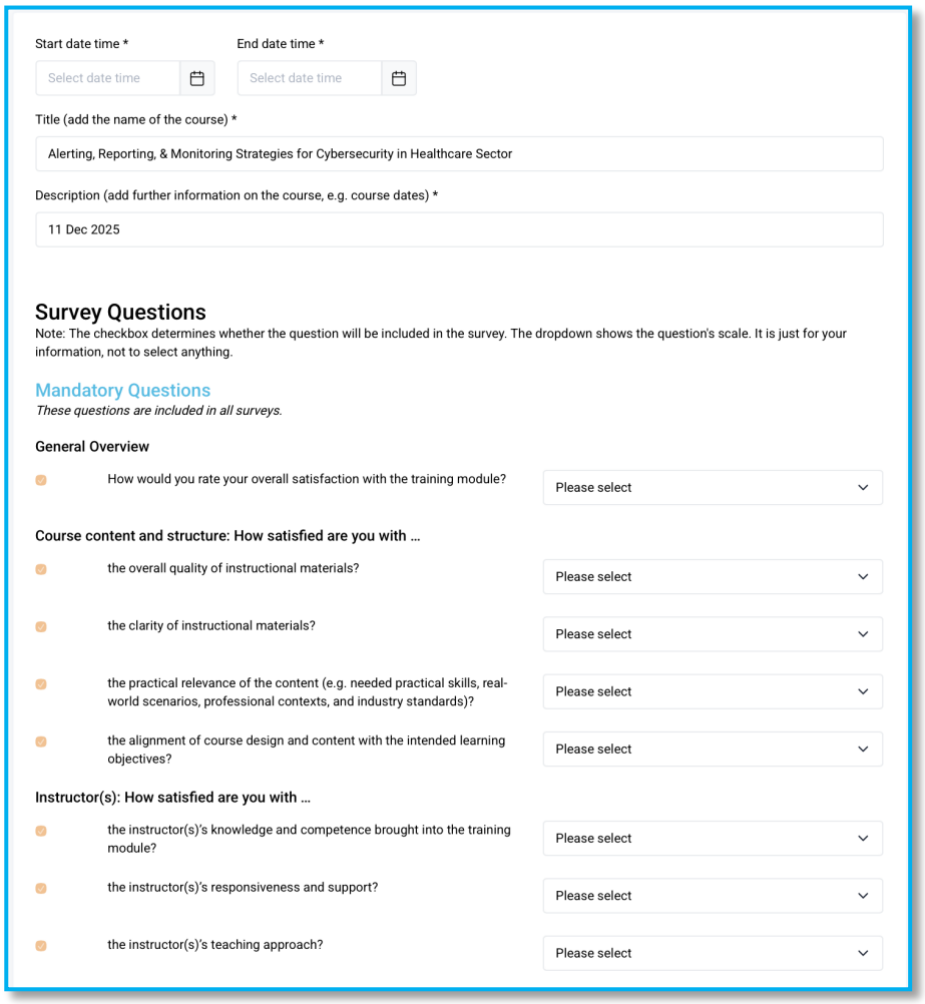

Figure 22 - Screenshot of CyberSecPro Learners Evaluation Form in the Admin Portal

CyberSecPro Trainer Evaluation Form

The evaluation of the training implementation from the trainers' perspective is also conducted using the "Evaluation Survey" feature integrated into the CSP Admin Portal. This feature allows trainers to reflect on and assess their own experience in delivering the module, focusing on aspects such as ease of use of the training materials, interaction with learners, and overall satisfaction with the training implementation process. The trainer survey is automatically generated within the portal for each module implementation. As the survey is standardised, trainers do not need to create the survey from scratch as in the case for learners. The survey can be found under each respective module, allowing trainers to select and complete the survey relevant to their implementation. More information on the survey is described in D5.1. Figure 23 shows a screen shot of CyberSecPro Trainer Evaluation Form in the Admin Portal.

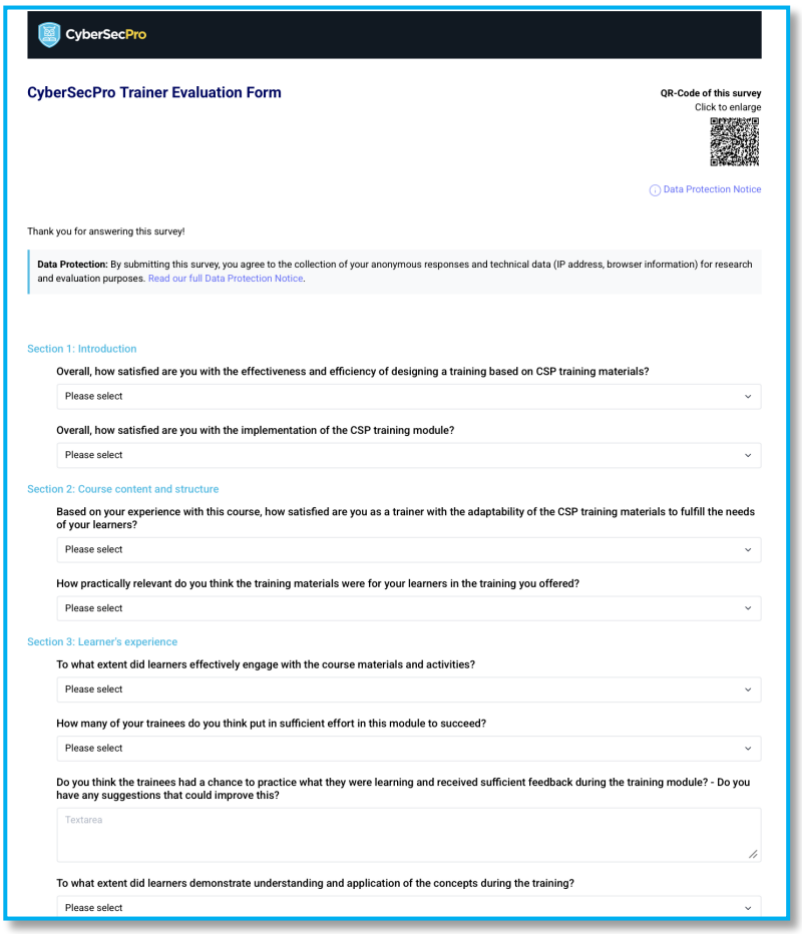

Figure 23 - Screenshot of CyberSecPro Trainer Evaluation Form in the Admin Portal

Follow-up survey

As mentioned in chapter 3.1, in order to in response to European Commission requirements regarding KPIs specified in the call, as well as the SO4 indicator 3, an additional questionnaire was developed for CSP providers to collect the relevant data from learners (see Annex D: CyberSecPro Evaluation Forms for further details). We followed two approaches to ensure that we collected the required data as accurately as possible. In the first approach, individual module providers gathered required data from their learners and completed the required information themselves by filling in the seventh tab of the admin portal, labelled “Employment.” A screenshot of this section of the admin portal is shown in Figure 24.

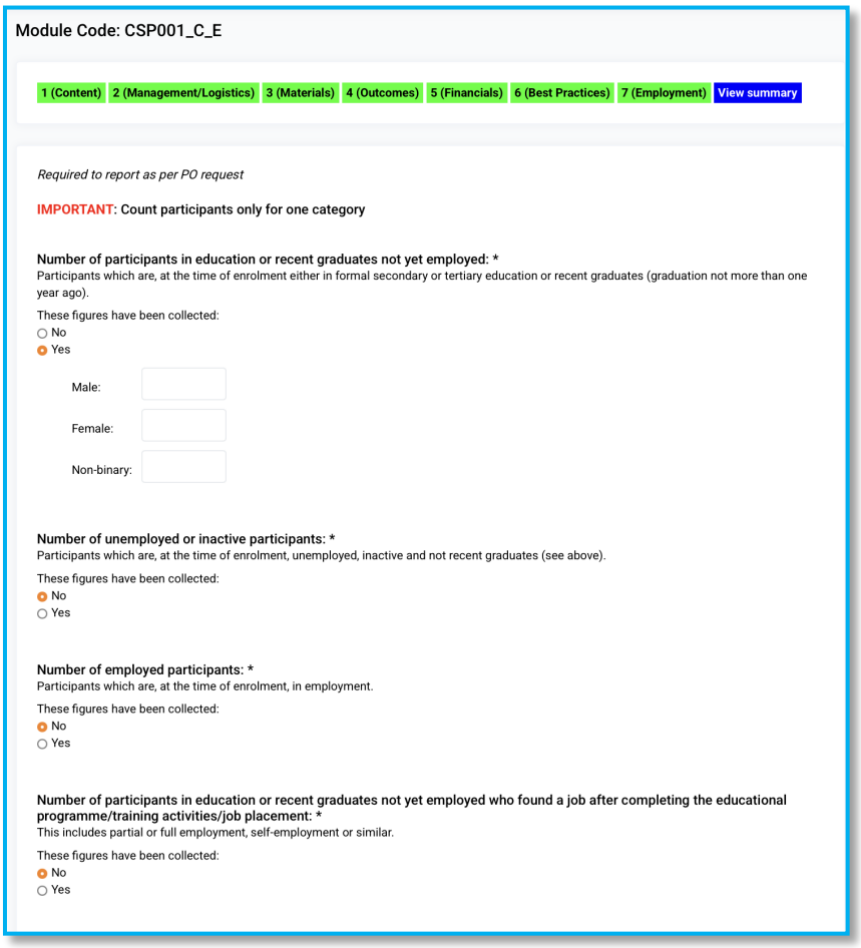

Figure 24 - Screenshot of Follow-up Survey in the Admin Portal

In the second approach, as described in D5.2, WP5 followed up with 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 25.

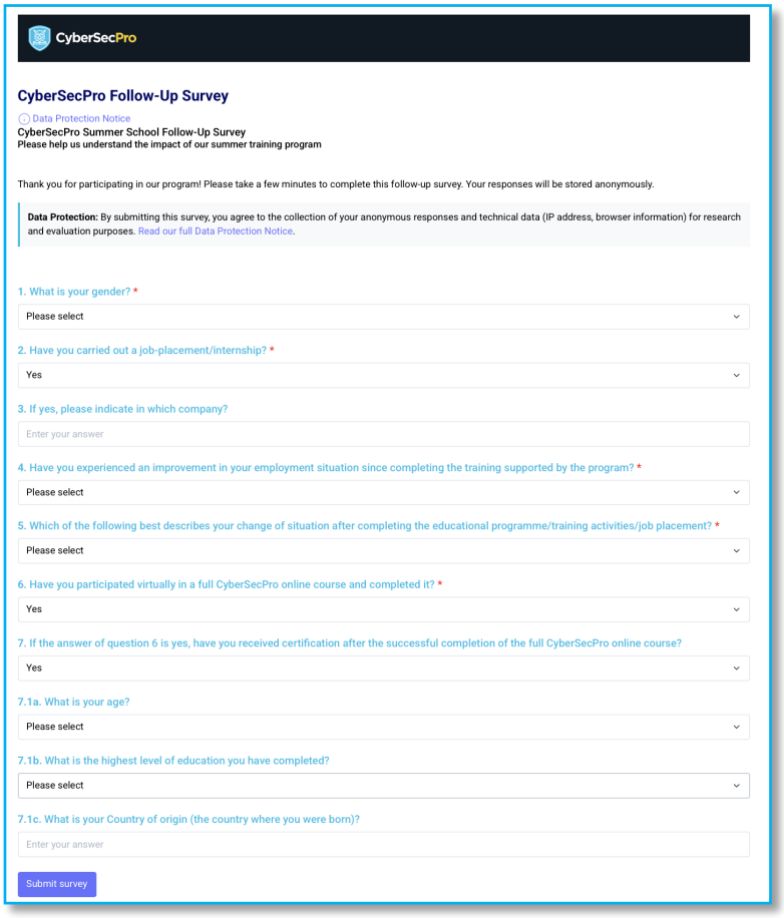

Figure 25 - Follow-up Survey in the Admin Portal

5. MOOC

MOOC can be classified under Offensive Cybersecurity Practices (T4.6/D4.5) when its curriculum explicitly develops competencies aligned with Knowledge Area 9 (Penetration **Testing)** and/or Knowledge Area 10 (Cyber Incident Response)**,** and when learners engage—ethically and in controlled environments—in activities that mirror attacker tools, tactics, and procedures (TTPs) for the purpose of improving detection, response, and resilience. In practice, this includes structured instruction and practice on topics such as reconnaissance and enumeration, vulnerability assessment, controlled exploitation, and post-exploitation analysis, as well as incident-response-oriented artefact collection and forensic reasoning. For example, the *From Zero to Hero – A complete CyberSecurity Toolkit* MOOC includes substantial content mapped primarily to KA9 and KA10, alongside hands-on components (e.g., network scanning, vulnerability assessment, Metasploit and Burp Suite exercises, and incident-response/SIEM workflows) that operationalise offensive-practice capabilities within a training context, thereby meeting the T4.6 categorisation criteria.

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

The following section presents the MOOC description using the format and structure defined in Deliverable D3.1 for documenting individual modules. Table 10 provides the general information about the "From Zero to Hero – A complete CyberSecurity Toolkit" MOOC, while Table 11 presents detailed information on its syllabus, including the topics and learning content.

Table 10 - Description of MOOC: From Zero to Hero – A complete CyberSecurity Toolkit

MOOC Title *The title of the training module*	**From Zero to Hero – A complete CyberSecurity Toolkit**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	The Practical Cybersecurity Toolkilt: Learn, Practice, Defend Hands-On Cybersecurity: Tools, Techniques, and Tactics Cybersecurity in Practice Cybersecurity Toolkits: Hands-On Experience with Practical Tools
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*	This MOOC provides a practical introduction to essential cybersecurity concepts, tools, and practices. Designed for beginners, it walks learners step by step through building a foundational security toolkit—covering topics such as threat awareness, secure communication, password management, system hardening, and incident response basics. By the end, participants will be equipped with the knowledge and skills to confidently navigate the cybersecurity landscape and apply protective measures in real-world scenarios.
MOOC description *Indicates the main purpose and description of the MOOC.*	This MOOC is designed to guide beginners through the essentials of cybersecurity, covering foundational concepts, practical skills and advanced techniques to protect against cyber threats. As part of the CyberSecPro project, this MOOC attempts to empower learners with the knowledge and tools needed to build upon a career in cybersecurity, focusing on areas like network security, ethical hacking, and incident response.

MOOC Title *The title of the training module*	**From Zero to Hero – A complete CyberSecurity Toolkit**
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: • **Remember & Understand** ○ Define fundamental cybersecurity concepts, including threats, vulnerabilities, attack vectors, and security controls. ○ Describe the purpose and functionality of common cybersecurity tool categories, such as network security, endpoint protection, vulnerability assessment, penetration testing, and digital forensics. • **Apply** ○ ○ Use industry-standard cybersecurity tools to perform basic security tasks, including network scanning, traffic capture, vulnerability identification, and controlled exploitation in safe environments. ○ Apply defensive security mechanisms to protect networks and systems, including firewalls, intrusion detection/prevention systems, and endpoint security solutions. • **Analyze** ○ ○ Analyse network traffic, scan results, and system artefacts to identify suspicious behaviour, misconfigurations, and potential security weaknesses. ○ Differentiate between attacker techniques and defensive controls by examining real-world attack and mitigation scenarios. • **Evaluate** ○ ○ Assess the security posture of systems and networks based on vulnerability scan outputs and monitoring data. ○ Evaluate risks and prioritize remediation actions based on impact, likelihood, and best practices. • **Create** ○ ○ Create clear and structured security reports summarising findings from scans, traffic analysis, and exploitation exercises. ○ Propose appropriate mitigation and prevention measures to improve the overall security of IT systems and applications.
Main topics and content list *A list of main topics and key content*	• Knowledge on red-teaming and ethical hacking • Network scanning and enumeration • Vulnerability scanning and assessment • Intrusion detection and prevention system • Packet analysis and network forensics • Malware analysis and reverse engineering • Incident response
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.
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=154

MOOC Title *The title of the training module*	**From Zero to Hero – A complete CyberSecurity Toolkit**
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*	Mainly • KA8 – Cybersecurity Tools and Technologies • KA9 – Penetration Testing • KA10 – Cyber Incident Response
Pre-requisites	Cybersecurity Fundamentals
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: Digital Forensics Investigator • ECSF Profile: Penetration Tester
Tools to be used *A list of tools that will be used for the operation of this MOOC.*	Several tools may be applied such as: Burp Suite, Chain-of-custody templates, ClamAV, DNS (basic networking support), DVWA (Damn Vulnerable Web Application), Elasticsearch, EICAR test file, File integrity monitoring (FIM), Firewall logs, GnuPG / GPG, hping3, HTTP/HTTPS web browser, Hydra, Incident response templates, IOC tracking tables, Java (required by Burp Suite / Splunk), jq, Kali Linux, Kibana, Linux (Ubuntu recommended), Logstash, Metasploit Framework, Metasploitable 2, Modern web browser (Chrome, Firefox, Edge, or Safari), Nmap, OpenVAS, OpenVPN (conceptual / optional), PAM (Pluggable Authentication Modules), ParrotOS, pfSense, Ping / ICMP utilities, Presentation software (PowerPoint or Google Slides), Risk register template, RDP (Remote Desktop Protocol), SHA-256 hashing tool (sha256sum), SIEM-style log datasets, Snort, Splunk Enterprise, Spreadsheet software (Excel, Google Sheets, or LibreOffice Calc), SQLmap, SSH client/server, Suricata, Terminal / command line interface, Text editor, VirtualBox, VPN client software, Wazuh Agent, Wazuh Server (All-in-One OVA), Wireshark, Windows 10 or 11, Word processor (Word, Google Docs, or LibreOffice Writer).
Language *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 11 - Syllabus of MOOC: From Zero to Hero – A complete CyberSecurity Toolkit

Main topics	Suggested Content
Topic-1: Introduction to Cybersecurity	Common offensive cybersecurity tools Network security tools Endpoint security tools Vulnerability assessment tools Forensics & incident response tools Penetration testing tools
Topic-2: Introduction to Red Teaming and Ethical Hacking	Setting up the environment with Kali Linux Steps on ethical hacking Exploiting vulnerabilities with Metasploit Intercepting traffic with Burp Suite Brute forcing logins with Hydra
Topic-3: Network Scanning and Enumeration	What is network scanning? Phases of network scanning Essential network scanning tools
Topic-4: Vulnerability Scanning and Assessment	What is vulnerability scanning? Types of vulnerability scans
Topic-5: Introduction to Software Security for Health	Introduction to software security for health Static application security testing (SAST) workflow
Topic-6: Intrusion Detection System	What is an intrusion detection and prevention system? Intrusion detection systems Intrusion prevention systems Network-based intrusion detection and prevention system Host-based intrusion detection and prevention system Snort and Suricata Triggering and analyzing alerts
Topic-7: Packet Analysis and Network Forensics	Key components of a packet How packet analysis works? Key uses of packet analysis Security and ethical considerations Wireshark – for analyzing suspicious traffic Packet capture and analysis using tcpdump Packet analysis lab
Topic-8: Malware Analysis and Reverse Engineering	What is malware analysis? Types of malware Essential tools for malware analysis Inspecting malware without execution
Topic-9: Incident Response: SIEM – Splunk & Elk	Introduction to SIEM Log collection and normalization Real-time monitoring and reporting Early threat detection
Topic-10: Cybersecurity Essentials and Management (Energy Sector) Foundations	Cyberattacks on energy Case study: colonial pipeline cyber attack Smart grids and cybersecurity challenges
Topic-11: Cybersecurity Essentials and Management (Energy Sector) – Common vulnerabilities	Vulnerability assessment Assets in energy domain and their cybersecurity challenges
Topic-12: AI and Cybersecurity: Research in Maritime	AI for maritime cybersecurity Adversarial AI Defensive AI Model inversion and perturbation attacks Dataset poisoning for AIS

6. Summary and Conclusion

This deliverable presents the outcomes of Task T4.6 up to the conclusion of CyberSecPro in Month 39 (February 2026). Hence, it comprehensively records all CSP modules corresponding to the capability category Offensive Cybersecurity Practices by Task 4.6 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.

Followed market demand, the analysis demonstrates that a total of 52 training modules were successfully implemented across multiple industry sectors, including energy, health, maritime, and general cybersecurity. The results show balanced coverage across training levels, a strong emphasis on seminar-based delivery formats, and substantial participant engagement in both sector-specific and cross-sectoral modules. The sectoral distribution of modules and enrolments confirms alignment with the project's focus on critical domains while maintaining broad applicability.

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

References

[1] “Apache Subversion,” [Online]. Available: https://subversion.apache.org/. [Accessed 20 February 2024].
[2] OwnCloud GmbH," OwnCloud," [Online]. Available: https://owncloud.com. [Accessed 26 January 2024].
[3] NextCloud GmbH," NextCloud," [Online]. Available: https://nextcloud.com. [Accessed 26 January 2024].
[4] GitLab Inc., “GitLab,” [Online]. Available: https://about.gitlab.com . [Accessed 04 March 2024].

Annex A: Template for the Documentation of Implemented CSP Modules

In this section, we have used the template for describing CSP modules from D4.1. We have added additional elements needed for the documentation of implemented CSP modules as shown in Table 12. We have also synchronized this template with the descriptions for training modules D3.1.

Table 12: 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 the CSP Grant Agreement.*	
	Learning outcomes and targets (mandatory)	

CSP Module Elements	CSP Module fields legend	CSP Module information
	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 (A)*	
	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" as well as number of "Not from members of the consortium"*	

CSP Module Elements	CSP Module fields legend		CSP Module information
	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 (mandatory)	*Duration of the implemented CSP module (in hours)*	
		Duration of prefabricated teaching video(s) from the CSP	

CSP Module Elements	CSP Module fields legend		CSP Module information
		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*		
	Number of job-placements/internships carried out by the students * *Required to report these KPIs in relation to the call.*		

CSP Module Elements	CSP Module fields legend	CSP Module information
	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 is no evaluation and verification of learning outcomes, please write, "None"*	
	The number of people reporting an improved employment situation after the end of the training supported by the programme	
Financial information (possibly confidential depending on the decision of the provider)	**Income** (mandatory)	
	Scholarships/sponsorships (mandatory) *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 education institutions ***	
	Number of female participants benefitting from	

CSP Module Elements	CSP Module fields legend	CSP Module information
	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 *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 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	

CSP Module Elements	CSP Module fields legend	CSP Module information
	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 13: 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.*	

CSP Module Elements	CSP Module [Fields legend]	CSP Module Information
	Information on the sector *Mandatory field. Indicates General, Maritime, Health, or Energy*	
	Pre-requisites *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 (A)*	
	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)*	

CSP Module Elements	CSP Module [Fields legend]		CSP Module Information
	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*		
	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.

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

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

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

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

For this reason, and while the DCM platform was being finalised and tested, we chose Strategy 4 by extending the capacities of the CSP internal web (https://admin.cybersecpro-project.eu) and implementing the template described in Section 0 via a (semi-)interactive tool for module providers.

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

Annex D: CyberSecPro Evaluation Forms

CyberSecPro 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 Learners

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 Learners 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 implemented CSP modules per module level
- Number of implemented CSP modules per module sector and level

Number of learners in implemented CSP modules per module level

Figure 26 illustrates the distribution of enrolments across T4.6 CSP modules by training level. Overall participation is higher in Basic offerings (698 enrolments) than in Advanced offerings (510 enrolments). The pattern indicates substantial demand at both competency levels, with the stronger uptake at Basic level consistent with the role of introductory and foundational content in broadening access and establishing baseline offensive-practices capabilities. At the same time, the sizeable Advanced cohort suggests sustained interest in more specialised, practice-oriented training. Collectively, these results indicate that the T4.6 training portfolio engages learners at multiple stages of competency development.

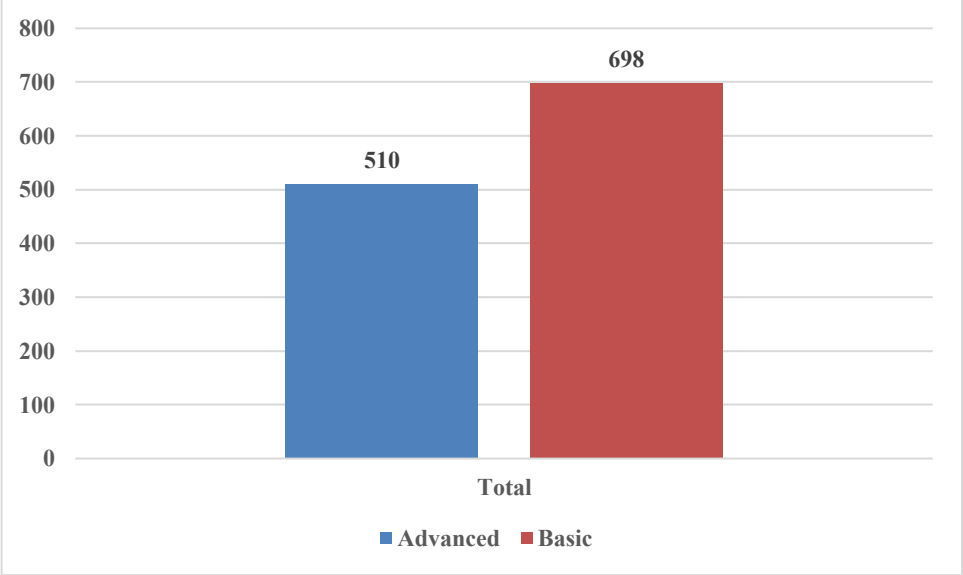

Figure 26 - Number of Learners in CSP Modules Per Module Level

Number of implemented CSP modules per module sector and level

Figure 27 presents the distribution of implemented T4.6 CSP modules by sector and training level. Basic implementations are most prevalent in the Energy sector (15), followed by Health (9) and Maritime (3), with General recording 6 basic implementations. Advanced implementations are comparatively fewer and are concentrated in Maritime (6) and Health (5), with Energy (4) and General (4) showing smaller numbers; no implementations are recorded for Hackathon (H) in this figure. Overall, the results indicate that basic-level

delivery dominates in energy-sector offerings, whereas maritime and health show a stronger relative emphasis on advanced implementations within the T4.6 portfolio.

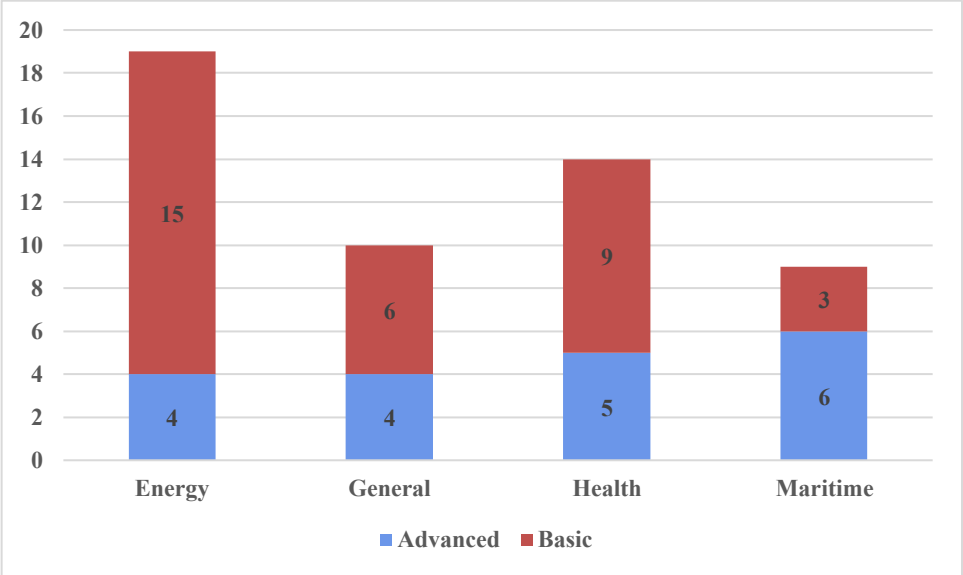

Figure 27 - Number of Implemented CSP Modules per Module Sector and Level