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

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

CyberSecPro

D4.3

Reports and Training Material on the Cybersecurity Tools Modules

Document Identification	
Due date	2026-02-28
Submission date	2026-02-28
Version	0.1

Related WP	WP4	Dissemination Level	PU
Lead Participant	PDMFC	Lead Author	Carlos Marques, Nuno Pedrosa (PDMFC)
Contributing Participants	ACEEU, UMA	Related Deliverables	D2.2, D.2.3, D3.1, D3.3, D3.4, D3.5, D.4.1, D4.2 D4.4, D4.5, D5.1, D5.2, D5.3

Abstract: This deliverable presents the outcomes of Task T4.4 up to the conclusion of CyberSecPro in Month 39 (February 2026). Accordingly, it comprehensively records all CSP modules corresponding to the capability category “Cybersecurity Tools and Technologies” implemented by the end of February 2026. The document provides quantitative information on the hosting site, learner enrolments, learner background, trainee evaluation forms, trainer evaluation forms, income, scholarships/sponsorships, training levels, delivery formats, and sectoral coverage across energy, health, maritime, and general cybersecurity domains. The deliverable includes descriptive analysis of training deployment, illustrating implementation patterns and participation across different module categories and sectors. Finally, 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 summarizes the results of Task T4.4, "Operating the training modules on Cybersecurity tools," covering progress up to the conclusion of CyberSecPro in Month 39 (February 2026). It provides a structured record of all CSP modules within the "Cybersecurity Tools and Technologies" capability category that were implemented by the end of February 2026.
The report covers the implementation of CSP003 "Cybersecurity Risk Management and Governance," CSP004 "Network Security," and CSP006 "Cyber Threat Intelligence," offering an evidence-based account of the training activities delivered during the reporting period. Since CSP003 spans more than one capability area, it is handled as an overlapping module; accordingly, this deliverable reports specifically on the tools/technologies-related component addressed under T4.4.
In addition, the document outlines the background and rationale of the documentation effort and explains the applied documentation methodology, including the definition of a "record" and the set of information captured for each module.

To prepare this deliverable, the following approach was applied:

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

The deliverable also includes quantitative overview of implementation, presenting distributions by module code, training level, module type, industry sector, module host, and associated enrolments.

[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
Carlos Marques, Nuno Pedrosa	PDMFC
Thorsten Kliewe, Jeldo Meppen	ACEEU
Cristina Alcaraz	UMA

Reviewers

Name	Beneficiary
Daniel Silveira	COFAC
Abdelkader Shaaban	AIT
Jeldo Meppen	ACEEU (as QM)

History

Version	Date	Contributor(s)	Comment(s)
0.01	2025-11-21	Carlos Marques	1st ToC
0.02	2026-01-21	Carlos Marques	1st draft
0.03		Atiyeh Sadeghi	High-level review
0.04	2026-02-13	Carlos Marques	Applied high-level review
0.05	2026-02-23	Abdelkader Shaaban, Daniel Silveira	First review
0.06	2026-02-24	Carlos Marques	Applied first review
0.07	2026-02-25	Abdelkader Shaaban, Daniel Silveira	Second review
0.08	2026-02-26	Carlos Marques	Applied second review
0.09	2026-02-27	Atiyeh Sadeghi, Jeldo Meppen, Christos Douligeris	High level review
0.10	2026-02-27	Carlos Marques	Applied High level review
0.11	2026-02-27	Atiyeh Sadeghi	Final check, preparation and submission process
0.12	2026-02-27	Nuno Pedrosa	Further improvement
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
	WP	Work Package
Z	**ZELUS**	Zelus IKE
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	**ECSF**	European Cybersecurity Skills Framework
F	**FCT**	Universidade NOVA de Lisboa (NOVA University of Lisbon)
	FTPS	File Transfer Protocol Secure
	FP	Focal Point
G	**GUF**	Johann Wolfgang Goethe-Universitaet Frankfurt am Main (Goethe University Frankfurt)
H	**H**	Hackathon
I	**ITML**	Information Technology for Market Leadership
	IMT	Institut Mines-Telecom
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 Formação e Consultadoria Lda
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 Tecnologias Associação (UNINOVA - Institute for the Development of New Technologies)
	UNSPMF	University of Novi Sad Faculty of Sciences
	UPRC	University of Piraeus Research Center
V	**VPN**	Virtual Private Network
W	**W**	Workshop
	WP	Work Package
Z	**ZELUS**	Zelus IKE

Glossary of Terms

C **Course**

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

Cybersecurity Exercise

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

H **Hackathon**

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

S **Seminar**

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

SS **Summer Schools**

A summer school is an educational course that happens during the summer.

W **Workshop**

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

Terminology points

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

1 Introduction

This section is structured as follows: Section 1.1 provides an overview of the background of the CyberSecPro project. In Section 1.2, the purpose and scope of WP4 and especially T4.4 are elaborated. Section 1.3 discusses the interrelation with other work packages and deliverables. Additionally, in Section 1.4, a brief outline of the subsequent sections' structure and organization is presented, offering readers a roadmap for navigating through this deliverable.

1.1 Background

Cybersecurity will remain a critical challenge for organisations and industries in every sector for the foreseeable future. As digitalisation continues to expand, the shortage of qualified professionals (especially those capable of effectively operating, configuring, and applying cybersecurity tools in real-world contexts) is expected to persist, raising serious concerns among stakeholders. Addressing the rapidly evolving and increasingly complex cybersecurity landscape requires comprehensive, hands-on training for the next generation of experts. By narrowing the gap between academia and industry, CyberSecPro seeks to enhance cybersecurity education and professional training, contributing to a safer and more secure digital future for everyone.
Therefore, the CyberSecPro project has the goal of establishing a distinctive professional training programme that delivers state-of-the-art, hands-on modules centred on the practical application of cybersecurity tools and technologies. The programme is designed to address a wide range of training needs and skill levels, offering both general modules and sector-specific modules tailored to areas such as maritime, healthcare, and energy.

1.2 Purpose and Scope

This deliverable has been developed within CyberSecPro Work Package 4 (WP4), Operating CyberSecPro Professional Training Program. Its overarching aim is to ensure consistent and traceable documentation for each CSP module offer. Specifically, the report covers the CSP modules implemented under Task 4.4 (T4.4), which align with the capability category Cybersecurity Tools and Technologies. Because certain topics cut across capability areas, some module content is shared with Cybersecurity Principles and Management; notably, CSP003 "Cybersecurity Risk Management and Governance" is addressed partly under T4.4 in this deliverable and partly under T4.3 in D4.2. The other CyberSecPro modules are covered in deliverables D4.2, D4.4 and D4.5.

By documenting implemented CSP modules, this deliverable contributes directly to several WP4 objectives, including:

- the execution of scalable CyberSecPro training offerings,
- enabling the engagement and training of external participants from diverse industries and sectors,
- ensuring the provision of training modules aligned with the CyberSecPro capability areas, particularly cybersecurity tools and technologies,
- the collection of qualitative feedback from training providers to enable continuous improvement.

The scope of this document is limited to reporting and analysing implemented training activities. It provides a structured overview of delivered modules, quantitative reporting on the number of implementations and enrolments, and an initial descriptive analysis of deployment patterns by module code, training level, module type, and industry sector.

This deliverable is not intended to provide an in-depth assessment of learning outcomes or long-term training impact. Instead, it supports monitoring of training execution and progress toward the project's capacity-building and skills development goals. The results reported here feed into the CyberSecPro evaluation framework and inform subsequent project activities and deliverables.

1.3 Relation to other Work Packages and Deliverables

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

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

1.4 Structure of the Deliverable

The deliverable is organized as follows:
Section 1 introduces the context of the CyberSecPro training activities on **cybersecurity tools and technologies**, outlines the purpose and scope of the deliverable, and describes its relation to other work packages and deliverables.
Section 2 explains the overall methodological approach.
In **Section 3**, we provide a brief overview of implemented modules on **cybersecurity tools and technologies** implemented by **M39**, including key information such as module codes and titles, implementation periods, training levels, providers, sectoral focus, and the number of learners.
Section 4 presents the structure, implementation patterns, and initial outcomes of all **CSP modules implemented under T4.4**. It is divided into two complementary parts. **Section 4.1** provides a quantitative overview of implementation through descriptive statistics and visualizations, reporting the number of delivered modules and learner enrolments across multiple dimensions: **module code** (including CSP003 as reported under T4.4), **training level**, **module type**, and **industry sector**. The section further explores combined distributions (e.g., **level by code**, **type by code**, **sector by code**, and **sector by level**) to highlight patterns in delivery choices and participation. It also includes a dedicated overview of implementations across **seasonal schools**, enabling comparison of delivery intensity across major project training events.
Section 4.2 complements the statistical analysis with a structured account of the **managerial and logistical aspects** of implementation. It summarizes how training offers were operationalized in practice, covering measures used to attract learners, income generation and the role of scholarships/sponsorships, the registration process, prerequisites and admission criteria, tangible rewards, and learning outcomes. In addition, it reports on job placements/internships where applicable, the background profile of learners, hosting sites, and the use of evaluation forms for trainees and trainers—providing context for interpreting the quantitative results and supporting continuous improvement of future module deliveries.
Section 5 concludes the document by summarizing the main findings and outlining their relevance to the objectives of the CyberSecPro project.

Annex A elaborates on the template utilized for documenting implemented CSP Modules. In **Annex B**, reference is made to the template for offering CSP modules as provided in **D3.1**. **Annex C** introduces the reason for using the admin portal as a provisional method for documenting implemented CSP Modules until the Dynamic Curriculum Management (DCM) became available. **Annex D** provides all CyberSecPro evaluation forms which had provided and analysed in WP5. And finallly **Annex E**, illustrates some additional statistics of the implemented CSP modules.

2 Methodology

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

2.1. Data Collection Procedure

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

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

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

Figure 1: provides an overview of the entire process:

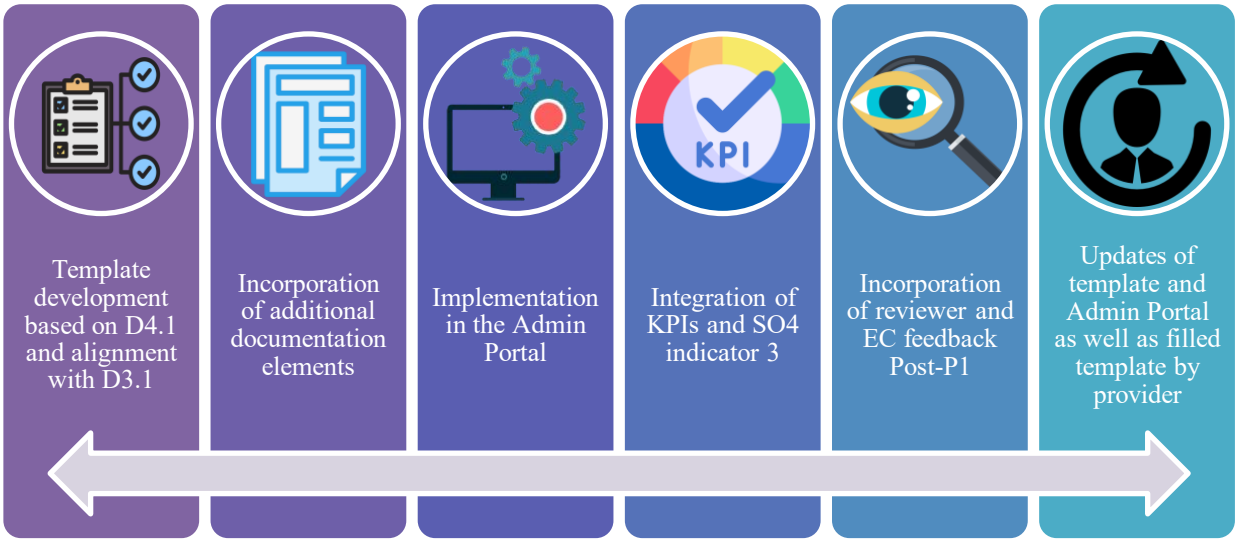

Figure 1: Data collection procedure

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

By extending the capabilities of the CyberSecPro internal web platform (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 (Figure 2).

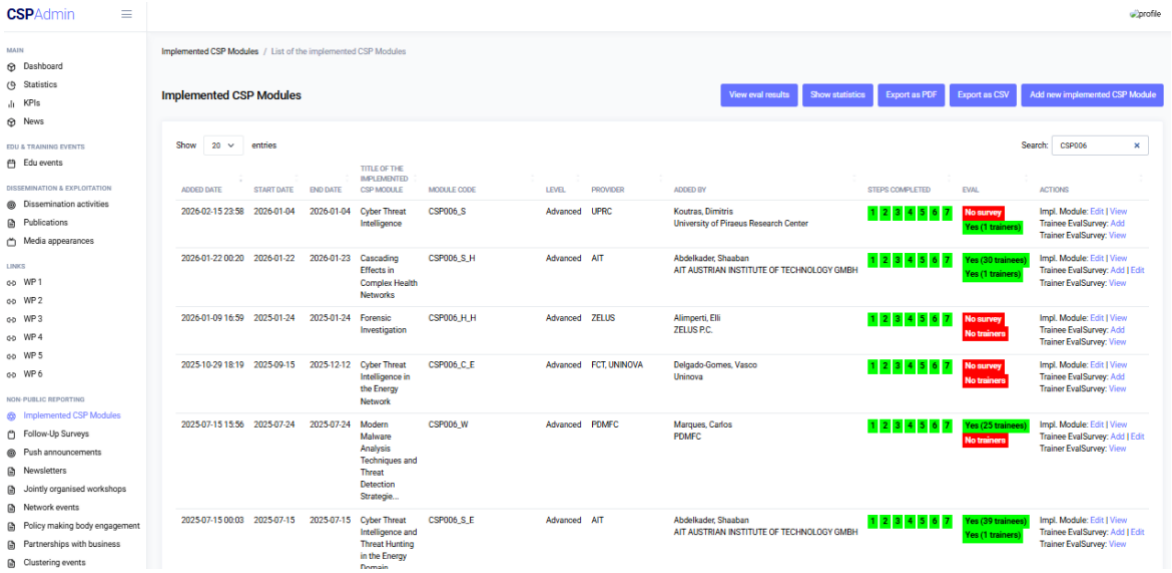

Figure 2: CyberSecPro Admin Portal

This semi-interactive platform, accessible via https://admin.cybersecpro-project.eu/implementedmodules/listimplementedmodules, enables module providers to enter, update, and manage information pertaining to each module.
Initially, we planned to have a full documentation of the implemented CSP modules in the DCM system; however, the DCM is designed to support teaching actions and that is why we decided to have another platform for documenting the implemented CSP modules (described in the Annex C: Reporting Method(s)), as it offers greater flexibility for trainers to report their outcomes than the DCM, which was needed for the flexibilty, as the KPIs and reporting duties changed several times mandated by the EC and the reviewer, and it was not clear whether and how often they would change again.

3 Overview of Implemented CSP Modules under T4.4

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

3.1 CSP Modules on Cybersecurity Principles and Management

In this section, we briefly describe which CSP Modules are related to cybersecurity tools and technologies and therefore to T4.4 titled Operating the training modules on Cybersecurity Tools. Based on Table 1, derived from D4.1, this task, T4.4, is responsible for the modules CSP004 "Network Security" and CSP006 "Cyber Threat Intelligence", as well as for the tools/technologies-related part of CSP003 "Cybersecurity Risk Management and Governance." As shown in Table 1, the module CSP003 "Cybersecurity Risk Management and Governance" is related to both Knowledge Area 3 (KA3) and Knowledge Area 4 (KA4), covering the capability categories cybersecurity tools and technologies and cybersecurity principles and management respectively. Therefore, CSP003 is covered partially by T4.4 and this deliverable, and partially by T4.3 and the corresponding deliverable addressing KA4 (see more details below). T4.3 is responsible for operating the training modules on Cybersecurity Principles and Management. Documentation of the implemented CSP modules related to Knowledge Area 3 is covered in this deliverable, and documentation of the implemented CSP modules related to Knowledge Area 4 is covered in the deliverable reporting on T4.3.

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

CSP Knowledge Area	Capabilities category	Module(s)
CSP Knowledge Area 1 – Cybersecurity Management	Cybersecurity Principles and Management	CSP001 "Cybersecurity Essentials and Management"
CSP Knowledge Area 2 – Human Aspects of Cybersecurity	Cybersecurity Principles and Management	CSP002 "Human Factors and Cybersecurity"
CSP Knowledge Area 3 – Cybersecurity Risk Management	Cybersecurity Tools and Technologies	CSP003 "Cybersecurity Risk Management and Governance"
CSP Knowledge Area 4 – Cybersecurity Policy, Process, and Compliance	Cybersecurity Principles and Management	
CSP Knowledge Area 5 – Network and Communication Security	Cybersecurity Tools and Technologies	CSP004 "Network Security"
CSP Knowledge Area 6 – Privacy and Data Protection	Cybersecurity Principles and Management	CSP005 "Data Protection and Privacy Technologies"
CSP Knowledge Area 7 – Cybersecurity Threat Management	Cybersecurity Tools and Technologies	CSP006 "Cyber Threat Intelligence"

CSP Knowledge Area 8 – Cybersecurity Tools and Technologies	Cybersecurity in Emerging Digital Technologies	CSP007 "Cybersecurity in Emerging Technologies" CSP008 "Critical Infrastructure Security" CSP009 "Software Security"
CSP Knowledge Area 9 – Penetration Testing	Offensive Cybersecurity Practices	CSP010 "Penetration Testing" CSP011 "Cyber Ranges and Operations"
CSP Knowledge Area 10 – Cyber Incident Response	Offensive Cybersecurity Practices	CSP011 "Cyber Ranges and Operations" CSP012 "Digital Forensics"

* Green colour indicates the KAs covered by T4.4 and in this deliverable, D4.3.

CSP003 Cybersecurity Risk Management and Governance
This module can be related to the CSP KA3: Cybersecurity Risk Management and the CSP KA4: Cybersecurity Policy, Process and Compliance. These areas involve recognising, evaluating, and mitigating cybersecurity risks, as well as the creation and implementation of cybersecurity policies and procedures and the management of cybersecurity compliance, respectively. Additionally, this module is related to the knowledge areas Cybersecurity Risk Assessment and Management, Cybersecurity Regulations and Compliance, Legal and Auditing Training, among others. This deliverable, D4.3, only covers the part related to CSP KA3 (see Table 1).

CSP004 Network Security
This module can be related to the CSP KA5: Network and Communication Security. This area addresses the principles and practices for protecting networks and communications, including secure network design and configuration, traffic control and monitoring, and safeguarding networked services and infrastructure. Additionally, this module can be related to knowledge areas such as network defence mechanisms, secure communications, and network monitoring and protection, among others.

CSP006 Cyber Threat Intelligence
This module can be related to the CSP KA7: Cybersecurity Threat Management. This area focuses on identifying, analysing, and managing cyber threats, including the collection and interpretation of threat information to support detection, response, and prevention activities. Additionally, this module can be related to knowledge areas such as threat intelligence analysis, threat actor and campaign understanding, and threat monitoring and reporting, among others.

3.2Overview of Implemented CSP Modules under T4.4

This section provides an overview of the most relevant elements of all implemented CSP modules, organized according to T4.4. As shown in Table 2, it reports for each CSP module the module code and title, the implementation period indicated by the start and end dates, the level, the provider, and the corresponding sector. In addition, the number of participating learners is documented.

In total, 44 training modules related to Cybersecurity Tools and Technologies 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 T4.4

Module ID	Module Code	Title of the implemented CSP module	Start Date	End Date	Level	Provider	Sector	No. of learners
101	CSP003_S_H	Risk Management and Risk Assessment	2024-08-22	2024-08-22	Basic	LAU, PDMFC	Health	35
129	CSP003_C_H	Hands on Risk Management	2025-01-20	2025-01-20	Basic	PDMFC	Health	55
130	CSP003_W	Cybersecurity Boardgame	2025-01-20	2025-01-20	Basic	PDMFC	General	55
153	CSP003_W	Risk Management and Governance	2025-02-04	2025-02-05	Basic	PDMFC	General	15
160	CSP003_S	Risk Assessment and Management	2025-02-06	2025-02-06	Basic	PDMFC	General	6
179	CSP003_W	Risk management tools demonstration	2025-07-15	2025-07-15	Basic	Ionian University	General	41
187	CSP003_W	Identity and Access Analytics and Governance in the modern workspace	2025-07-23	2025-07-23	Basic	Nexis GmbH	General	41
218	CSP003_S_H	Cybersecurity Risk Management and Governance in the Healthcare sector	2026-01-16	2026-01-16	Advanced	APIRO	Health	9
38	CSP004_C_E	Network Protection for Energy Control Systems	2024-09-23	2024-10-04	Advanced	AIT, UMA	Energy	10
39	CSP004_W	Introduction to Analysing Network Security: Wireshark Hands on Tr...	2023-10-10	2023-10-20	Basic	LAU	General	40
84	CSP004_S_E	Introduction to cybersecurity in healthcare	2024-06-21	2024-06-23	Basic	PDMFC	Energy	7
95	CSP004_S	Foundations of networking and systems security	2024-06-21	2024-06-21	Advanced	FCT, LAU, TalTech, UMA, UNINOVA	General	17
99	CSP004_S_M	Security Aspects for Maritime Networks - Session 3: Cryptography ...	2024-06-21	2024-06-21	Advanced	AIT	Maritime	17
100	CSP004_C_E	Network Protection for Energy Control Systems - Session 4: Web se...	2024-06-21	2024-06-21	Advanced	AIT	Energy	17
113	CSP004_S_M	Security Aspects for Maritime Networks	2024-11-19	2024-11-19	Advanced	AIT, CNR	Maritime	5
138	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2024-06-22	2024-06-22	Basic	ITML	Health	17
141	CSP004_C_E	Network Protection for Energy Control Systems	2025-04-07	2025-04-11	Advanced	AIT, UMA	Energy	19
143	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2024-07-03	2024-07-03	Basic	ITML	Health	35
147	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2024-10-17	2024-10-17	Basic	ITML	Health	51
149	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2024-11-14	2024-11-14	Basic	ITML	Health	14
154	CSP004_W	Network Security Essentials	2025-04-21	2025-04-21	Basic	PDMFC	General	19
158	CSP004_W	Advanced Network Security	2025-04-22	2025-04-24	Advanced	PDMFC	General	5
172	CSP004_C_E	Essential Protection for Energy Control Networks: Topic-3: Essent...	2025-01-21	2025-01-21	Advanced	AIT, UMA	Energy	55
185	CSP004_W	Entry Point - From Digital Foot Print to Enumeration	2025-07-21	2025-07-21	Basic	COFAC	General	41
186	CSP004_W	Web and system security	2025-07-22	2025-07-22	Advanced	Ionian University	General	41
188	CSP004_W	Active Enumeration and Intrusion	2026-07-23	2026-07-23	Advanced	COFAC	General	41
203	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2025-05-30	2025-05-30	Basic	ITML	Health	9
204	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2025-04-25	2025-04-25	Basic	ITML	Health	9
206	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2025-06-19	2025-06-19	Basic	ITML	Health	6
208	CSP004_S_H	Network Security & Health: Endpoint Protection Strategies	2025-05-15	2025-05-15	Basic	ITML	Health	9
223	CSP004_C_E	Network Protection for Energy Control Systems	2026-01-22	2026-01-22	Advanced	AIT, UMA	Energy	35
20	CSP006_C_H	Cyber Threat Intelligence for Health	2024-07-01	2024-07-13	Basic	PDMFC, SINTEF	Health	35
68	CSP006_S_H	Network and IoMT Security	2024-05-29	2024-05-29	Basic	UPRC	Health	30
76	CSP006_S_M	Cyber Threat Intelligence and sharing in the SeaPort	2023-09-13	2023-10-04	Advanced	AIT, UPRC	Maritime	35

Module ID	Module Code	Title of the implemented CSP module	Start Date	End Date	Level	Provider	Sector	No. of learners
79	CSP006_S_H	Threat landscape in healthcare	2024-06-22	2024-06-22	Basic	PDMFC, SINTEF	Health	7
115	CSP006_S_E	Cyber Threat Intelligence and Threat Hunting in the Energy Domain...	2024-11-20	2024-11-20	Advanced	AIT	Energy	10
118	CSP006_S_H	Network and IoMT Security	2025-01-10	2025-01-10	Basic	UPRC	Health	20
120	CSP006_S_H	Network and IoMT Security	2024-06-21	2024-06-23	Basic	UPRC	Health	7
133	CSP006_H	Forensic Investigation	2025-01-25	2025-01-25	Advanced	PDMFC	General	55
159	CSP006_S	Cyber Threat Intelligence	2025-05-19	2025-05-19	Basic	PDMFC	General	14
161	CSP006_C_E	Cyber Threat Intelligence in the Energy Network	2025-03-03	2025-06-27	Advanced	FCT, UNINOVA	Energy	25
178	CSP006_S_E	Cyber Threat Intelligence and Threat Hunting in the Energy Domain	2025-07-15	2025-07-15	Advanced	AIT	Energy	41
189	CSP006_W	Modern Malware Analysis Techniques and Threat Detection Strategies	2025-07-24	2025-07-24	Advanced	PDMFC	General	41
211	CSP006_C_E	Cyber Threat Intelligence in the Energy Network	2025-09-15	2025-12-12	Advanced	FCT, UNINOVA	Energy	25
217	CSP006_H_H	Forensic Investigation	2025-01-24	2025-01-24	Advanced	ZELUS	Health	55
224	CSP006_S_H	Cascading Effects in Complex Health Networks	2026-01-22	2026-01-23	Advanced	AIT	Health	35
232	CSP006_S	Cyber Threat Intelligence	2026-01-04	2026-01-04	Advanced	UPRC	General	18

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

This section describes the framework of the statistical analysis and presents the main implementation results of the CSP modules addressed in this deliverable. Chapter 4.1 provides statistical data on the modules implemented under Task T4.4, including the portion of CSP003 relevant to T4.4, offering a consolidated view of implementation within the tools-and-technologies capability area. Chapter 4.2 outlines key managerial and operational insights observed during delivery, with particular attention to how implementation decisions were planned, coordinated, and carried out.

It should be noted that the figures reflect the CyberSecPro implementation strategy: wherever possible, at least one module was delivered in each targeted area to ensure broad capability coverage. Additional deliveries were then prioritised based on demonstrated demand and uptake from relevant markets and sectors.

4.1 Statistics of Implemented CSP Modules

This section provides an initial statistical snapshot of the CSP modules implemented under T4.4. As noted above, CSP003 “Cybersecurity Risk Management and Governance” spans two capability areas: CSP KA3 (reported in D4.3 / T4.4) and CSP KA4 (reported in D4.2 / T4.3). To ensure coherent reporting, the corresponding figure(s) include the T4.4-relevant share of CSP003 (i.e., the part aligned with KA3), while making the treatment of the overlap explicit to avoid inconsistencies or double counting across deliverables.

The figures summarize key characteristics of the implemented trainings, such as the number of modules delivered per sector, the distribution of learners across sectors, and the balance between training levels (e.g., Basic vs. Advanced). Together, these visualizations provide a clear and transparent representation of implementation data and establish a baseline for monitoring progress and supporting subsequent evaluation and project activities (e.g., deeper analysis of trends, coverage, and participation).

4.1.1 Number of implemented CSP modules per module code

Figure 3 summarizes the number of implemented CSP modules by module code. CSP004 represents the highest volume of delivery, with 23 implementations, followed by CSP006 with 16. CSP003 (which spans both T4.4 and T4.3) is reported here only for its T4.4-aligned component, resulting in 7 recorded implementations under this deliverable.

Overall, the distribution suggests that implementation under T4.4 concentrated primarily on Network Security (CSP004) and Cyber Threat Intelligence (CSP006), reflecting their strong operational relevance and applicability across sectors. At the same time, the inclusion of CSP003 broadens the thematic coverage within the tools-and-technologies capability area and supports a more rounded training portfolio within the CyberSecPro framework.

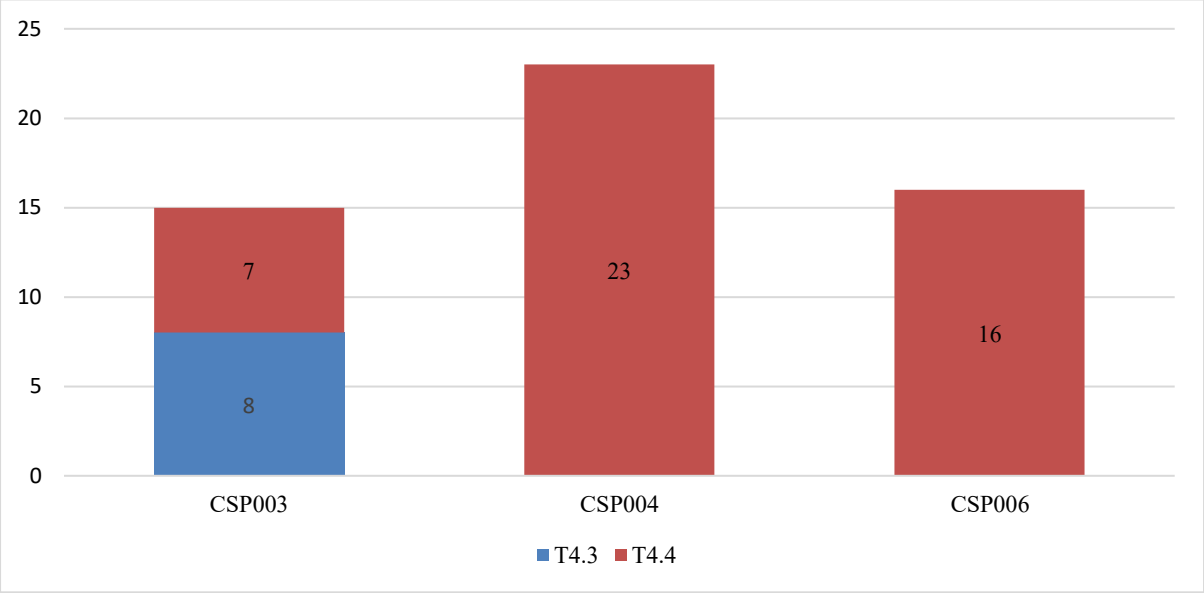

Figure 3: Number of implemented CSP modules per module code

4.1.2 Number of learners in implemented CSP modules per module code

Figure 4 presents the total number of enrolments across implemented CSP modules, aggregated by module code. In line with observed demand, CSP004 and CSP006 attracted the largest number of learners, with 396 and 394 enrolments respectively. CSP003 accounted for 166 enrolments (reported here for the T4.4-related part), indicating sustained engagement in training activities linked to risk management practices and their practical application within the tools-and-technologies capability area. Furthermore, the high volume of implemented modules provided a robust evidence base for the comprehensive evaluation conducted in WP5.

The distribution suggests particularly strong uptake for modules with broad applicability and direct operational relevance, such as network security and threat intelligence. At the same time, the enrolment levels for CSP003, while potentially distributed across two reporting streams due to its overlap with T4.3, contribute to the diversity of the CyberSecPro training portfolio and help ensure balanced coverage across complementary cybersecurity competences.

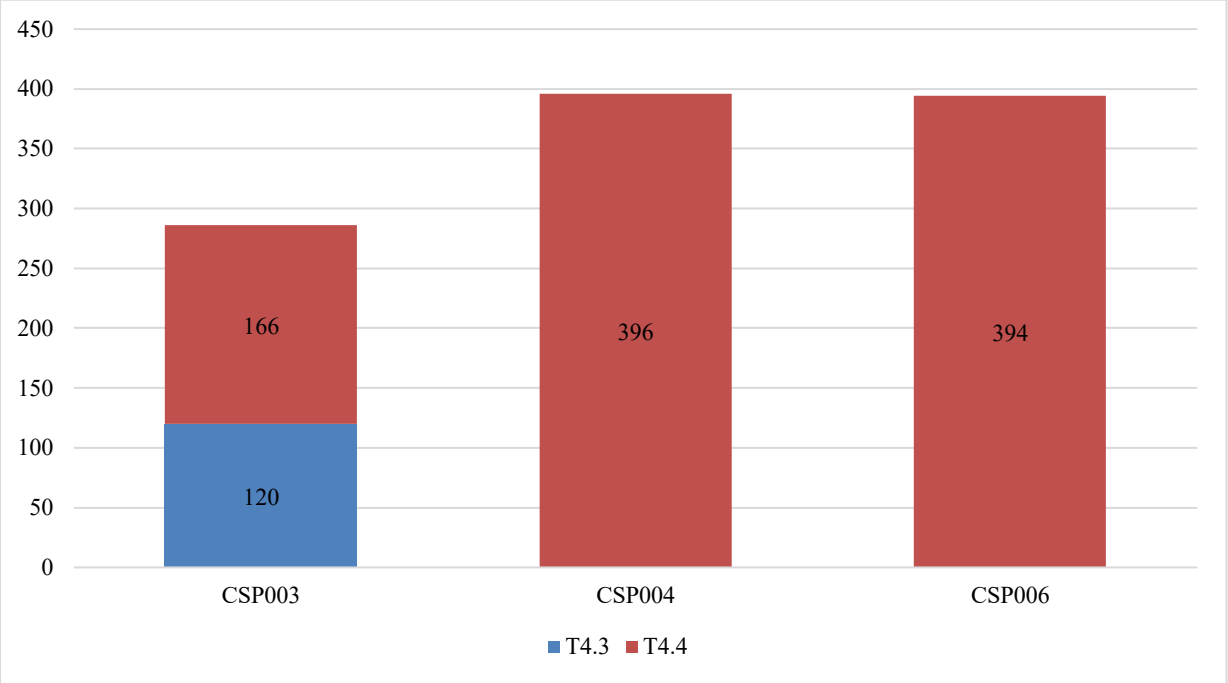

Figure 4: Number of learners in implemented CSP modules per module code

4.1.3 Number of implemented CSP modules per module level

Figure 5 shows the distribution of implemented CSP modules by training level. In line with observed market demand, basic-level offerings account for the majority of implementations under T4.4, with 25 basic modules delivered compared to 21 advanced-level implementations. When the T4.3-related share of CSP003 is included in the overview, the total number of implemented basic modules rises to 29, while advanced modules increase to 25.

Overall, the results indicate an implementation profile that spans both proficiency levels, but with a clear emphasis on introductory and foundational training within the cybersecurity tools and technologies capability area. This pattern suggests that partners and learners prioritised modules that build practical baseline competence, while advanced offerings were delivered more selectively in response to specific needs and audiences.

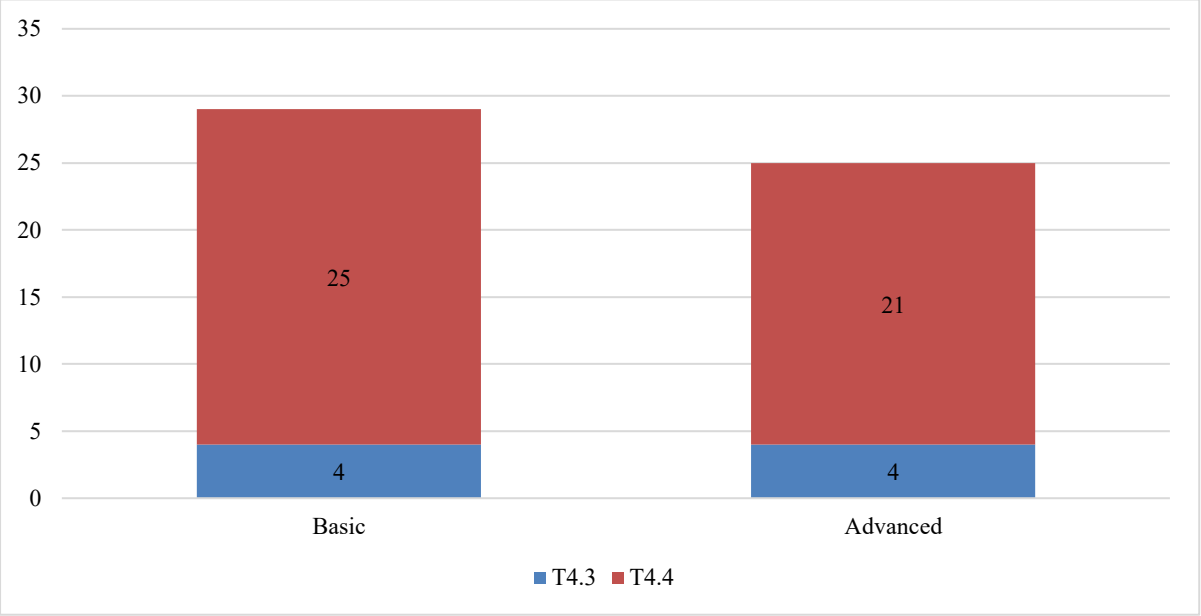

Figure 5: Number of implemented CSP modules per module level

4.1.4 Number of implemented CSP modules per module level and code

Figure 6 presents the distribution of implemented CSP modules by module code and training level. Overall, the results show how delivery choices varied across module areas, reflecting both the intended training pathway (foundation to advanced) and observed demand.

For CSP004, a total of 23 modules were implemented, with the majority delivered at Basic level (12) and a slightly smaller share at Advanced level (11), indicating a strong emphasis on building core competencies in network security. An opposite pattern is observed for CSP006, which includes 16 modules in total, comprising 7 Basic and 9 Advanced implementations.

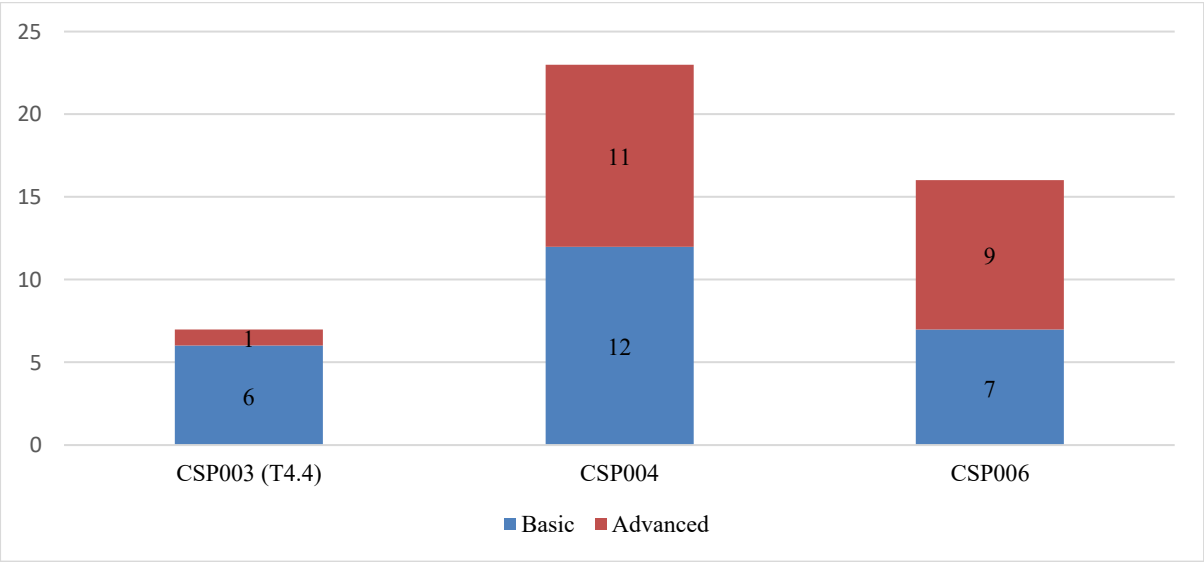

Figure 6: Number of implemented CSP modules per module level and code

For CSP003, the distribution reflects its cross-cutting nature. In this deliverable (D4.3 / T4.4), CSP003 includes 7 implemented modules, with 6 delivered at Basic level and a single one at Advanced level. This indicates that CSP003 under T4.4 is oriented primarily toward foundational coverage, while still including some advanced training where relevant. (The KA4-related part of CSP003 is reported separately under T4.3 / D4.2.)

Taken together, the figure shows a clear preference for Basic-level delivery across the tools-and-technologies capability area, while maintaining a smaller but meaningful set of Advanced implementations to support learners progressing toward more specialised competencies.

4.1.5 Number of implemented CSP modules per module type

Figure 7 presents the distribution of implemented CSP modules by module type. In line with observed demand, seminars represent the largest share of implementations, with 23 delivered modules, followed by workshops (12) and courses (9) while 2 hackathons are recorded in the reporting period.

The distribution suggests a delivery model that prioritises seminar-based formats for scalable knowledge transfer, while also incorporating hands-on formats—particularly workshops and exercises—to support practical engagement with cybersecurity tools and technologies. The resulting mix enables multiple learning pathways, combining conceptual grounding with applied and experiential training opportunities.

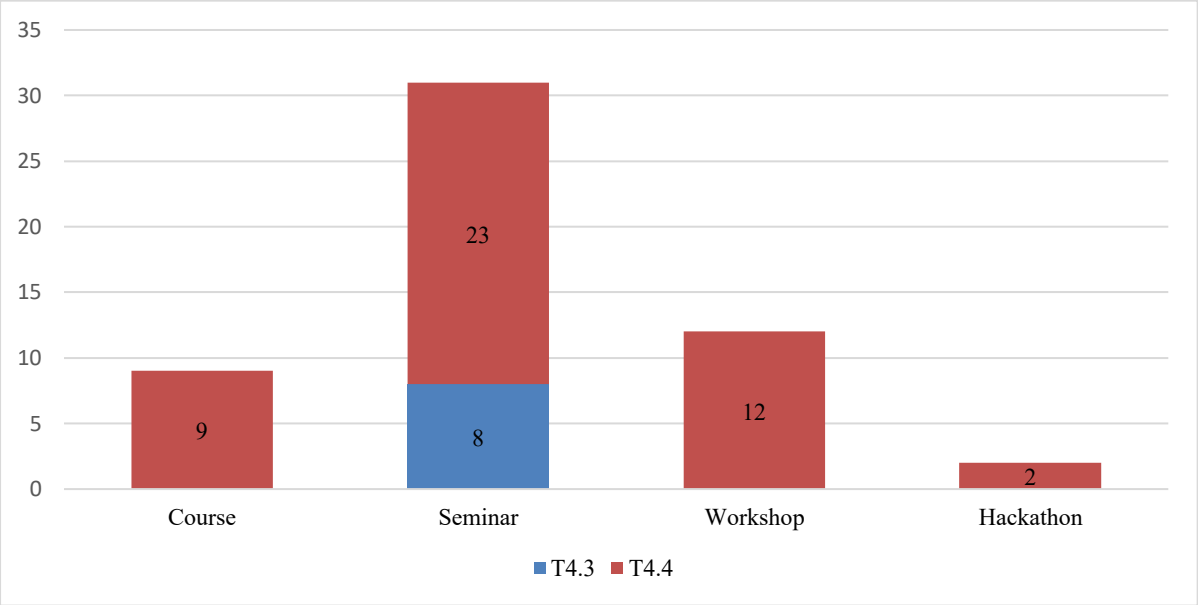

Figure 7: Number of implemented CSP modules per module type

4.1.6 Number of implemented CSP modules per module type and code

Figure 8 shows how the implemented modules are distributed by module type across each CSP code, highlighting clear differences in delivery choices between the three module areas. Overall, the results indicate that format selection is closely linked to both the characteristics of the topic and practical implementation decisions shaped by demand.

For CSP004, delivery is spread across seminars (12), workshops (6), and courses (5), pointing to a deliberate blend of scalable, knowledge-focused sessions and more hands-on formats. CSP006 follows

a broadly comparable approach, with seminars (9) forming the core of delivery, complemented by courses (3), workshops (2), and hackathons (2)—suggesting that threat intelligence content was delivered through a combination of structured instruction and more applied, practice-oriented activities.

For CSP003 (reported here for the T4.4-related share), the distribution is more compact but still varied, comprising workshops (4), seminars (2), and one course (1). This mix reflects the cross-cutting character of CSP003 and its suitability for different learning environments, ranging from guided classroom-style teaching to interactive and applied sessions.

Taken together, the figure confirms the strong role of seminar-based delivery in the overall portfolio, while also showing meaningful variation in how each CSP code is operationalised—supporting a balanced combination of theory-led learning and experiential training formats within the cybersecurity tools and technologies capability area.

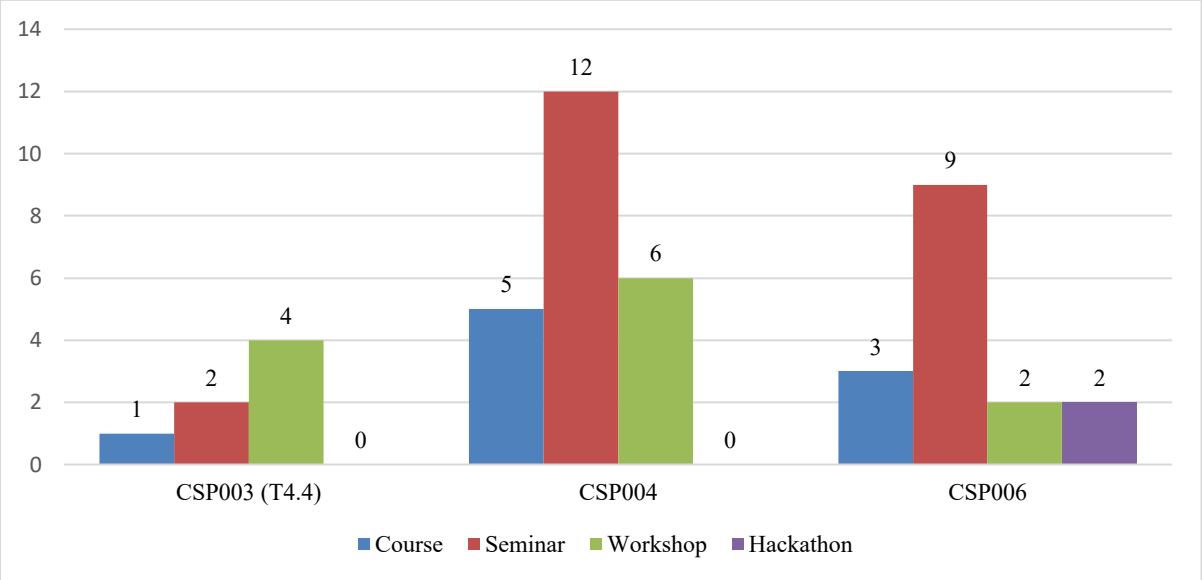

Figure 8: Number of implemented CSP modules per module type and code

4.1.7 Number of implemented CSP modules per module sector

Figure 9 presents the overall distribution of implemented CSP modules across industry sectors, independently of module code. The results indicate that Health and the General sector account for the highest number of implemented modules, with 17 and 16 modules respectively, followed by the Energy sector with 10 modules and the Maritime sector with 3 modules.

Across sectors, the distribution reflects the allocation of modules implemented under T4.4, including the T4.4-related share of CSP003 where applicable.

Overall, the sectoral profile suggests that the CyberSecPro training programme prioritised delivery in sectors with high operational exposure and strong need for applied cybersecurity tools and technologies, while maintaining coverage across additional sectors to support cross-sectoral skills development and broader transferability of competences.

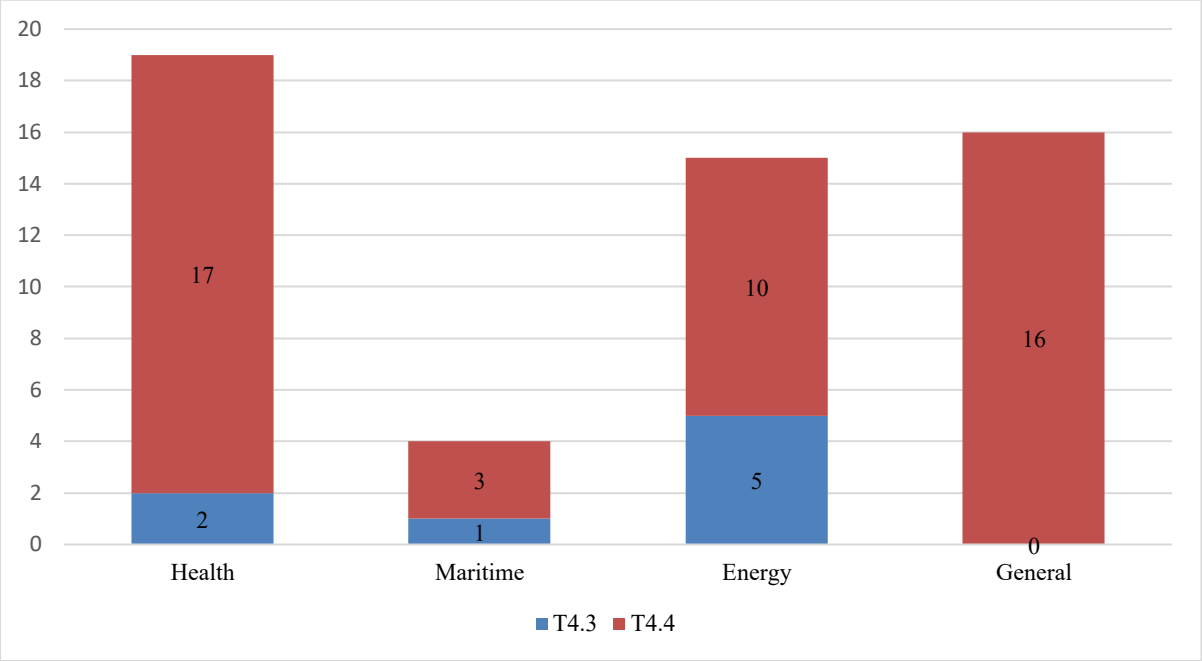

Figure 9: Number of implemented CSP modules per module sector

4.1.8 Number of learners in implemented CSP modules per module sector

Figure 10 presents the distribution of learners across implemented CSP modules by industry sector. The results show that the health sector accounts for the highest number of learners (429). The Energy and General sectors demonstrate broadly comparable levels of participation, with approximately 244 and 226 learners respectively. The Maritime sector had the fewest learners with 57 learners.

Overall, the distribution suggests strong learner engagement across both sector-specific and cross-sectoral training activities. It also indicates that the training offer achieved reach across multiple domains, supporting the CyberSecPro objective of developing practical cybersecurity competences that are transferable while remaining responsive to sectoral needs.

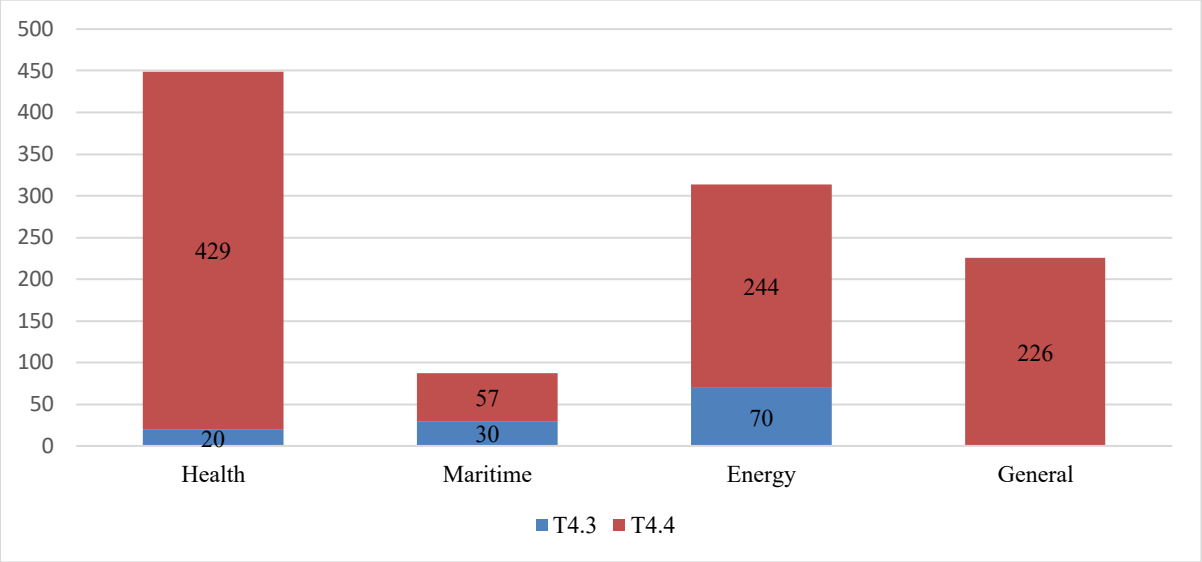

Figure 10: Number of enrolments in implemented CSP modules per module sector

4.1.9 Number of implemented CSP modules per module sector and code

Figure 11 presents the distribution of implemented CSP modules across industry sectors, disaggregated by module code, and reveals clear differences in sectoral uptake within the T4.4 portfolio.

For CSP004 (Network Security), delivery spans all sectors, with the strongest concentration in Health (8), followed by General (7) and Energy (6), while Maritime (2) accounts for a smaller share. CSP006 (Cyber Threat Intelligence) follows a comparable pattern: implementation is highest in Health (7), with more limited delivery in Energy (4) and General (4), and one implementation in Maritime.

For CSP003 (Cybersecurity Risk Management and Governance), this deliverable reports only the T4.4-relevant share (aligned with KA3). Within that scope, the modules are concentrated primarily in the General sector (5 implementations), with additional delivery in Health (2 implementations).

Overall, the figure indicates that implementation was responsive to sectoral demand—particularly in health and general contexts—while still maintaining coverage across multiple domains and balancing sector-specific delivery with cross-sectoral offerings where appropriate.

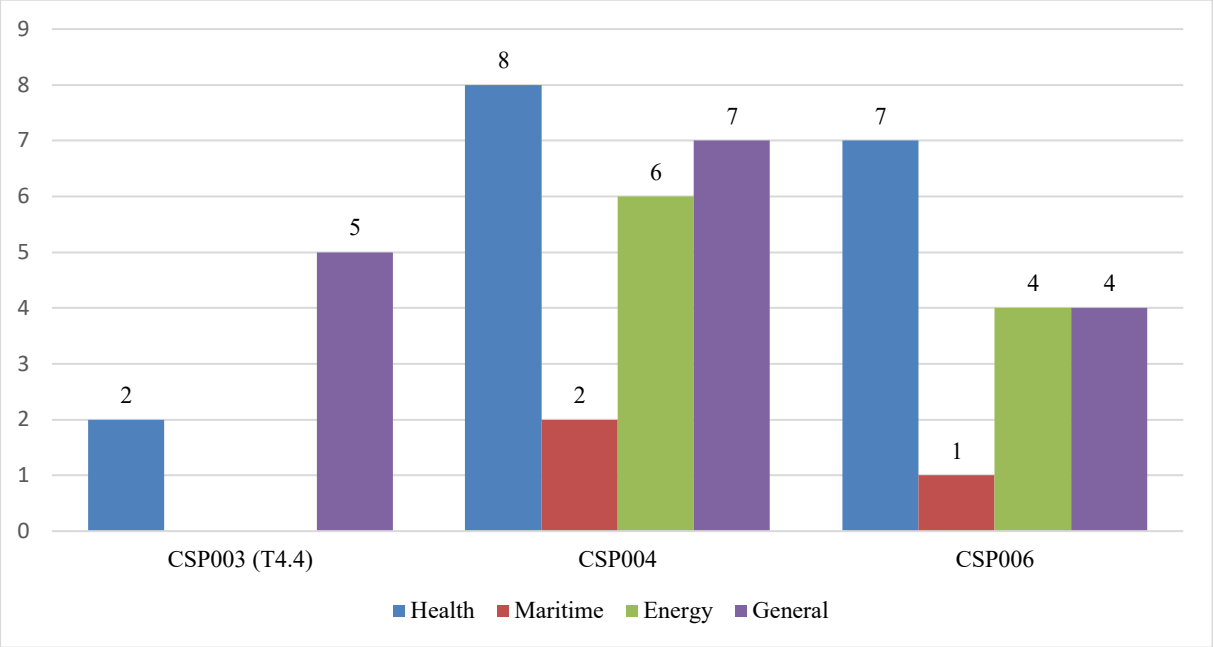

Figure 11: Number of implemented CSP modules per module sector and code

4.1.10 Number of implemented CSP modules per seasonal schools

Figure 12 summarizes the number of CSP modules implemented across the different seasonal schools delivered within the CyberSecPro project under T4.4 (including the T4.4-relevant share of CSP003 where applicable). The highest concentration of implementations is observed during the second Summer School 2025, Novi Sad and Winter School 2025 in Lisbon, with 5 modules delivered in each event. The first Summer School 2025, Novi Sad showed 2 implementations.

Earlier events — Summer School 2024, Porto and Summer School 2024, Madeira and CyberHot 2025—show lower levels of implementation with one Module each, indicating a gradual scaling of delivery over time.

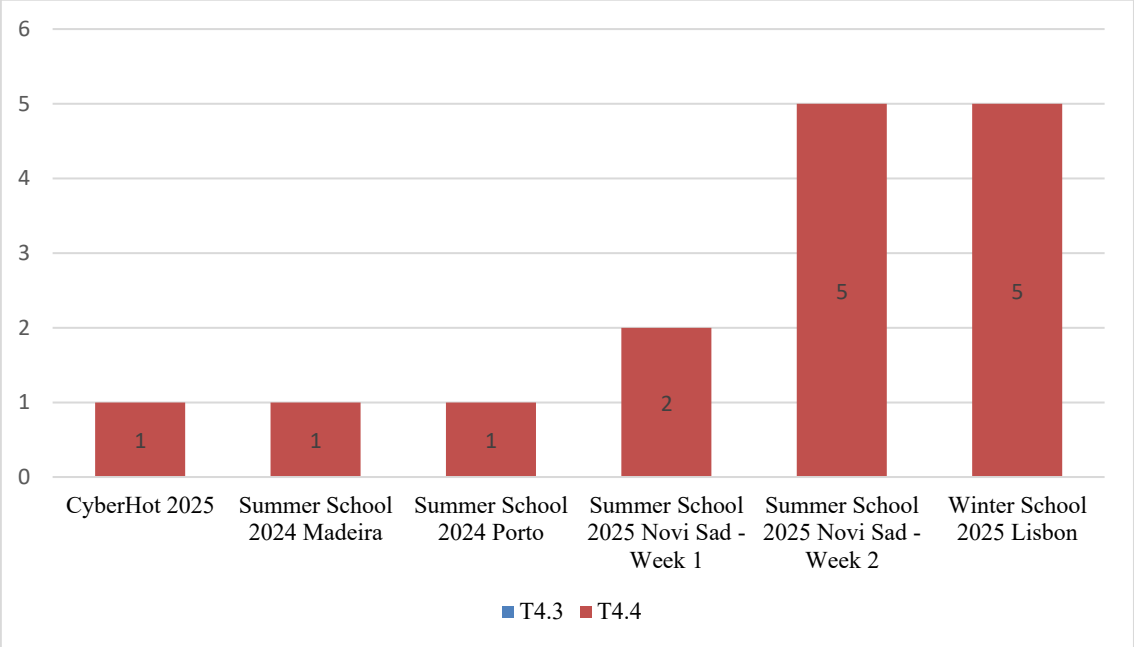

Figure 12: Number of implemented CSP modules per seasonal schools

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 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.
- Students are also often disadvantaged in certain European countries with limited financial and educational resources.

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 13) 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 13: Post messages in the dissemination channel (CyberSecPro project LinkedIn and 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 learners. At IPICS 2024 the registration fee for 2 weeks including hotel room and lunches was €1000, and similar

fees held for other events. This was achieved by finding sponsors for the events. In addition, CSP provided assistance to candidates on finding funding for the fees and travel expenses,

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

4. Flexible and Digital Access

This category relates to accessibility through online and hybrid formats.

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

4.2.2 Income and scholarship/sponsorships

Regarding the income, there was mostly no income achieved from the implemented CSP module under T4.4, except for the below ones and seasonal schools.
In terms of the scholarship/sponsorships, Table 3 presents the scholarships and sponsorships awarded within the CyberSecPro project.
Cybersecro, as the organizer of the seasonal schools did the following things and sometime supported by other sponsors confer in Table 3:

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

Table 3: scholarship/sponsorships provided in the CyberSecPro seasonal schools

Seasonal schools	Sponsorship	Scholarship
Summer School 2024 Madeira	No sponsorships.	CyberSecPro organizer (UNINOVA) enabled 17 scholarships covering the admission-fee.
Summer School 2024 Porto (IPICS 2024)	Some students supported through Erasmus fellowships.	CyberSecPro organizers (PDMFC; COFAC) enabled 34 scholarships covering the admission-fee.
CyberHOT 2024 Piraeus	Projects :SecOPERA, Phoenix, Eddeless, Rewire, synapse, FAITH, CustodesNERO, THEMIS5.0, ReScale, 6GXell, CyberSecDome. Companies/Institutions: Technical University of Crete, University of Piraeus Research Center, Trustilio, Focal Point, Dienekes IKE.	CyberSecPro organizer (University of Piraeus) enabled 20 scholarships covering the admission-fee.

Seasonal schools	Sponsorship	Scholarship
Winter School 2025 Caparica	Some students supported through Erasmus fellowships and private company. Ten students from the University of Piraeus were supported through Erasmus funds. Five students from Laurea University were supported through Erasmus funds.	CyberSecPro organizers (PDMFC, FCT, COFAC) enabled 49 scholarships covering the admission-fee.
CyberHOT Week 2025 Crete	Projects: SecOPERA, Phoenix, Eddeless, Rewire, synapse, FAITH, CustodesNERO, THEMIS5.0, ReScale, 6GXell, CyberSecDome, Elastic, CyberSynchrony, Eudoros. Companies/Institutions: Technical University of Crete, University of Piraeus Research Center, Trustilio, Focal Point, Dienekes IKE. 2 students were supported by the French Erasmus programme.	CyberSecPro organizers (Technical University of Crete) enabled 9 scholarships covering the admission-fee and CyberSecPro organizers (University of Piraeus) enabled 4 scholarships covering the admission-fee. Also, there were lower admission fees for all students.
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	Seven Greek students used Erasmus funds. Two students from Finland were supported by LAU internal funds.	CyberSecPro organizers (PDMFC, UNSPMF, COFAC) enabled 33 scholarships in the first week and 40 scholarships in the second week covering the admission-fee.
Winter School January 2026 Lisbon	Students from Serbia were financially supported by company JetBrains and OSCE office in Serbia. Total number of Serbian students which were supported is 8. 10 students from the University of Piraeus and 6 students-cadets from the Hellenic Airforce Academy were supported through Erasmus fellowships (HAF cooperates with UPRC in the project through Prof. Antonios Andreatos).	CyberSecPro organizers (PDMFC, COFAC) enabled 38 scholarships covering the admission-fee.

4.2.3 Registration process

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

1. **No registration:** Some courses did not require any registration, such as open modules that are freely accessible.
2. **CyberSecPro organizer registration:** Registration is managed directly by the CyberSecPro consortium through dedicated registration pages. This applies to seasonal schools and similar activities, such as Summer School 2024 Madeira, Summer School 2024 Porto, CyberHOT 2024 Piraeus, Winter School 2025 Caparica, CyberHOT 2025 Crete, Summer School 2025-1 and 2 Novi Sad and Winter School January 2026 Lisbon. Table 4 presents a detailed overview of the registration process for CSP Seasonal Schools. Furthermore, Figure 14 presents screenshot from the registration pages of the Winter school 2025 and Summer School 2025- 1 and 2 Novi Sad, highlighting key elements of the registration process. Additionally, some modules also registered via CyberSecPro DCM.

Table 4: Registration process of CSP seasonal schools

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

Seasonal schools	Registration process of CSP seasonal schools
Novi Sad (IPICS 2025)	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/

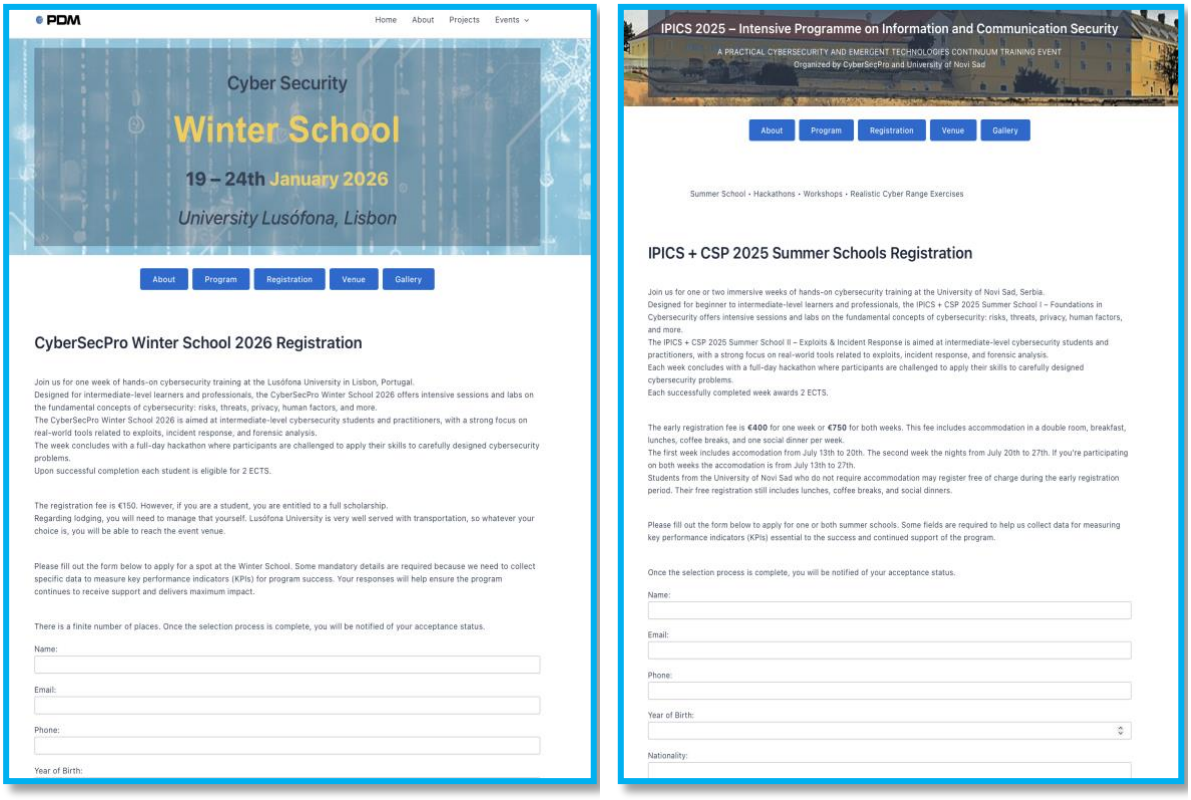

Figure 14: Screenshot of CyberSecPro seasonal registration page (Winter school 2025 & IPICS 2025)

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

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

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

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

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

4.2.4 Pre-requisites and Admission Criteria

The prerequisites for each CSP module are specified in Deliverable D3.1. Further information on the admission criteria for the seasonal schools is outlined below.

Table 5: Admission Criteria from seasonal schools

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

4.2.5 Tangible rewards to learners

Certificates of attendance are mostly used as the tangible rewards across the implemented CSP modules. As illustrated in Figure 15, the majority of modules award certificates upon full attendance, while a smaller number also link with passing exam, or other defined criteria. A number of modules did not provide certificates.

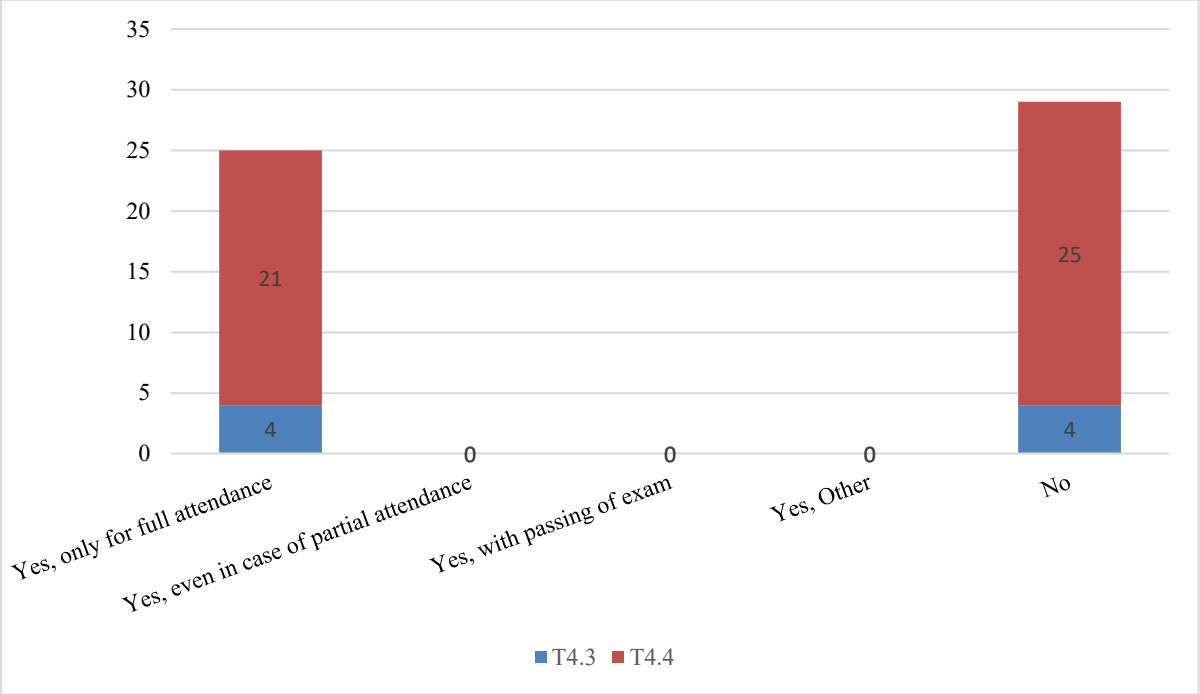

Figure 15: Number of implemented CSP Modules award Certificate

Certificates are issued by several partner organisations, including UPRC, UNINOVA and FCT, PDMFC, the University of West Attica, LAU, TalTech, UNSPMF, APIRO, the Digital Security Authority of Cyprus, and Nova, demonstrating the strong institutional involvement in the organisation of the seasonal schools. As most tangible rewards are associated with the seasonal schools, these are presented in Table 6. Also, ECTS credits as additional tangible rewards for learners were and are being awarded by some events.

Table 6: Tangible reward to learners from seasonal schools

Seasonal schools	ECTS reward	Certification and awarding organization
Summer School 2024 Madeira	No ECTS were awarded.	Learners got certificate of attendance signed by UNINOVA.
Summer School 2024 Porto (IPICS 2024)	4 ECTS upon successful completion of the program (including the two-day long Hackathons) by COFAC.	Learners got certificate of attendance signed by COFAC.
CyberHOT 2024 Piraeus	No ECTS were awarded.	Learners got certificate of attendance signed by the organizers (UPRC, TUC, trustilio, FP, Dienekes).
Winter School 2025 Caparica	2 ECTS upon successful completion of the program by COFAC.	Learners got certificate of attendance signed by UNINOVA and FCT.
CyberHOT 2025 Crete	No ECTS were awarded.	Learners got certificate of attendance signed by the organizers (UPRC, TUC, trustilio, FP, Dienekes).
Summer School 2025-1 and 2 Novi Sad (IPICS 2025)	2 ECTS upon successful completion of the program by COFAC.	Learners got certificate of attendance signed by PDMFC and UNSPMF.
Winter School January 2026 Lisbon	2 ECTS upon successful completion by COFAC.	Learners got certificate of attendance signed by COFAC.

4.2.6 Learning Outcomes

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

Table 7: Learning Outcomes

Related CSP to T4.4	Learning Outcomes
CSP003 - Cybersecurity Risk Management and Governance	By the end of the training, learners gained the following: Knowledge: • Basic definitions related to Information Security Management Systems and Information Security Governance • Risk Management: Basic phases and principles for an effective risk management methodology. • Standards and Methodologies of Risk Management • Legal and Policies related to Risk Management • Measurements, Scales and Metrics of Risks • Technical and non-Technical Mitigation Actions Skills: • Applying a suitable methodology for Information Security Risk Management and Risk Assessment. • Analysing Information Security Risk utilising different methodologies. • Creating policies, procedures and processes compliant with the requirements of the current version of the ISO/IEC 27000x series of standards. • Selecting and implementing appropriate mitigation actions and controls. • Developing security policies and procedures • Developing Business Continuity Plans and Disaster Recovery Plans. • Implementing cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards. • Analysing and consolidating the organisation's quality and risk management practices. • Enabling business asset owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks. • Enabling employees to understand, embrace and follow the controls. • Building a cybersecurity risk-aware environment. • Communicating, presenting and reporting to relevant stakeholders. • Proposing and managing risk-sharing options Competencies: • Lead and participate in strategic, operational, and tactical cybersecurity discussions. • Lead the design, development, operation and improvement of an Information Security Management System. • Support the organisation in the audits of an Information Security Management Systems. • Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories • Knowledge of risk-sharing options and best practices • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks.

Related CSP to T4.4	Learning Outcomes
CSP004 – Network Security	By the end of the training, learners will have gained the following: Knowledge: • General knowledge of communication infrastructures and models as well as the emergence of modern networks and technologies. • Knowledge of the most common vulnerabilities and threats in specific network systems (in traditional networks, mobile networks, virtualised systems, or distributed systems) and their associated protocols. • Knowledge of the most relevant security protocols, such as SSL/TLS and IPSec, and their importance for the protection of systems and communication networks. • Knowledge of the most relevant security mechanisms, such as firewalls and IDS/IPS, to protect network perimeters and access to private domains, such as corporate networks. • Knowledge of the most relevant security mechanisms to protect the endpoints of communication, such as a client and a server, but also the interconnection elements between a client and a server. • Knowledge of the most relevant security mechanisms to protect those advanced communication infrastructures such as mobile networks or virtualized systems. • Knowledge of privacy and anonymity in network management, ensuring the protection of end nodes and their location. • Knowledge of the most relevant authorization models (including access control models, roles and permissions, access monitoring) and authentication methods (including biometrics, dongles, single-sign-on) • Understanding the fundamental concepts of network security and using cryptographic techniques to ensure secure transmissions among interconnected nodes in computer networks. • Knowledge of building secure network architecture by considering network segmentation and isolation. Additionally, understanding the usability of critical security devices such as Firewalls, IDS/IPS, VPNs, tunnelling, and others. • Understanding the basic security mechanisms, services, and attacks in the OSI reference model. Skills: • Planning and designing secure networks according to the most general recommendations and following good security practices. • Analysing communication scenarios and identifying possible misconfigurations or vulnerabilities that could lead to security risks or threats. • Configuring systems following basic security principles (e.g., user control, port control, etc.). • Identifying and applying those security elements or mechanisms that contribute to improving the security of a communication system. Competencies: • Know how to identify possible misconfigurations or errors that may lead to significant security risks. • Lead the design, configuration and deployment of communication systems. • Support the organisation in hardening its systems and enhancing secure communications. • Knowledge of existing security technologies, mechanisms and protocols, useful to protect any peer-to-peer communication.

Related CSP to T4.4	Learning Outcomes
	• Knowledge of recommendations and best practices for securing end nodes and interconnection elements. • Knowledge of privacy weaknesses and existing mechanisms to address threats
CSP006 – Cyber Threat Intelligence	Upon successful completion of this module, the learner will be expected to be able to demonstrate the: Knowledge: • Demonstrate knowledge and understanding of threats to an information and network system. • Taxonomy of cyber threats, actors, and motivations. • Threat intelligence lifecycle and its components. • Variety of threat intelligence sources and their strengths/weaknesses. • Security controls and standards relevant to specific threats. • Vulnerability assessment techniques and tools. • MITRE ATT&CK framework and its application in threat modelling. • Advanced analytical techniques for threat detection and analysis. • Methods for developing and maintaining threat actor profiles. • Effective communication and dissemination of threat intelligence. • Ethical and legal considerations surrounding CTI acquisition and use. • Knowledge on available data sources and collections, how to validate them and how to use the data. • Knowledge on basic and advanced concepts for anomaly detection and log file analysis • Understand how to identify potential threat actors and analyse their tactics. • Knowledge of different threat modelling approaches and an understanding of potential cyber threats and vulnerabilities that could lead to cyber-attacks. Skills: • Analyse and interpret various sources of threat intelligence. • Conduct threat modelling and identify vulnerabilities in systems. • Apply advanced analytical techniques to identify and prioritise threats. • Develop and maintain threat profiles for specific adversaries. • Disseminate actionable threat intelligence to different audiences. • Evaluate and select CTI tools and platforms based on specific needs. • Implement and manage a CTI program within an organization. • Align security controls and standards with identified threat profiles. • Communicate threat intelligence effectively in written and verbal formats. • Conduct ethical threat research and responsibly disclose vulnerabilities. Competencies: • Critical thinking and problem-solving in the context of cyber threats. • Ability to analyse complex data and identify patterns and trends. • Effectively collaborate and share information with diverse stakeholders. • Adapt to evolving threat landscapes and technologies. • Make informed decisions based on threat intelligence. • Maintain ethical and responsible practices in CTI activities. • Demonstrate effective leadership and communication skills in managing a CTI program. • Foundations of Cyber Threat Intelligence (CTI)-Taxonomy, Lifecycle, Security Controls and Standards

Related CSP to T4.4	Learning Outcomes
	• Threat Modelling and Analysis • Data sources and collection • Data analysis and data processing • Threat actors and tactics • Vulnerabilities Assessment Techniques • Advanced Analytical Techniques and Threat Actor Profiling • Threat Intelligence Information Sharing, Dissemination, Communication, and Implementation • Legal and Ethical Considerations • Anomaly detection • Log file analysis. • Practical Threat Modelling and Security Investigation

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

Table 8 presents the number of job placements and internships completed by students. In both cases, the number hosted by consortium member organisations is three times higher than that hosted by external organisations.

Table 8: Number of job-placements/internships carried out by the students

	Related to T4.3	Related to T4.4
in the organization member of the consortium	33	93
in an external organization	10	32

4.2.8 Background of learners

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 implemented CSP modules per gender

Figure 16 shows the number of learners enrolled in CSP modules by gender. The results indicate that male learners are 722 males in T4.4 modules. Female learners are with 234 learners in T4.4. No enrolments are recorded for non-binary learners in either module type. Overall, the figure shows that female learners account for 24.5 percent of the total, positioning this share at the slightly close to industry distribution standard.

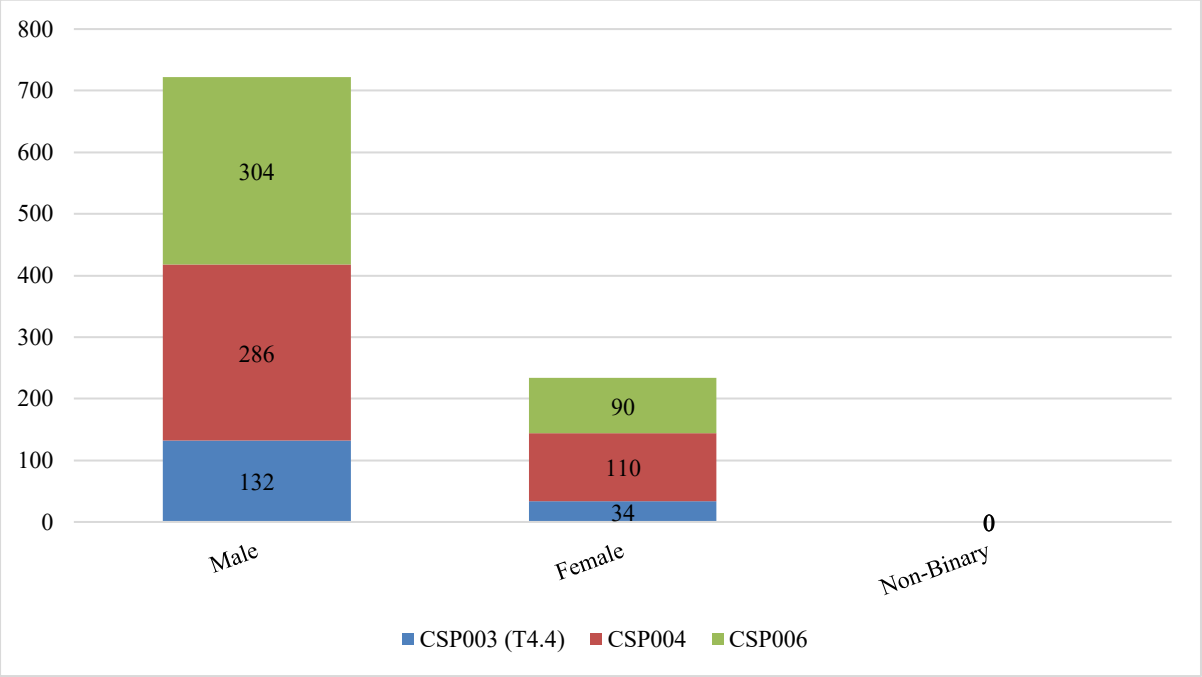

Figure 16: Number of learners in implemented CSP modules per gender

4.2.8.2 Number of learners in CSP modules per Age

Figure 17 illustrates the distribution of learners enrolled in CSP modules by age group. The majority of participants fall within the 18–34 age range, which shows by far the highest level of engagement. While learners aged 35–45 and 45–54 demonstrate moderate participation, their numbers are significantly lower compared to the younger cohorts. There are no learners in the 55–65 age group, nor any participants under 18 or over 65. Overall, the data indicates that CSP modules predominantly attract young adults, particularly those between 18 and 34 years of age.

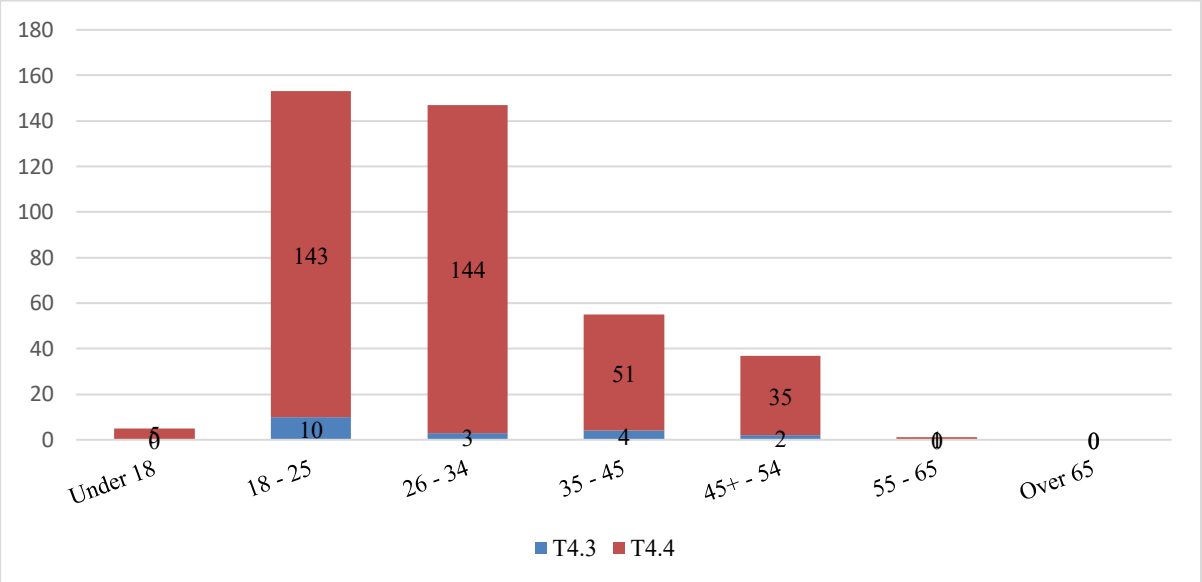

Figure 17: Number of learners in CSP modules per Age

4.2.8.3 Number of learners in implemented CSP modules per Educational Background

Figure 18 presents the distribution of learners enrolled in CSP modules according to educational background. There are no participants with less than a high school education, while 17 learners hold a high school diploma or equivalent qualification. The largest group consists of learners with a Bachelor's degree (177), followed by 130 learners with a Master's degree. Additionally, 42 participants have some college education but no completed degree (almost all of whom are undergraduate students). There are 22 doctoral (PhD) learners, and the "Other" category includes only 2 learners under T4.3.

Overall, the modules are primarily attended by learners with undergraduate-level education, particularly those holding a Bachelor's degree.

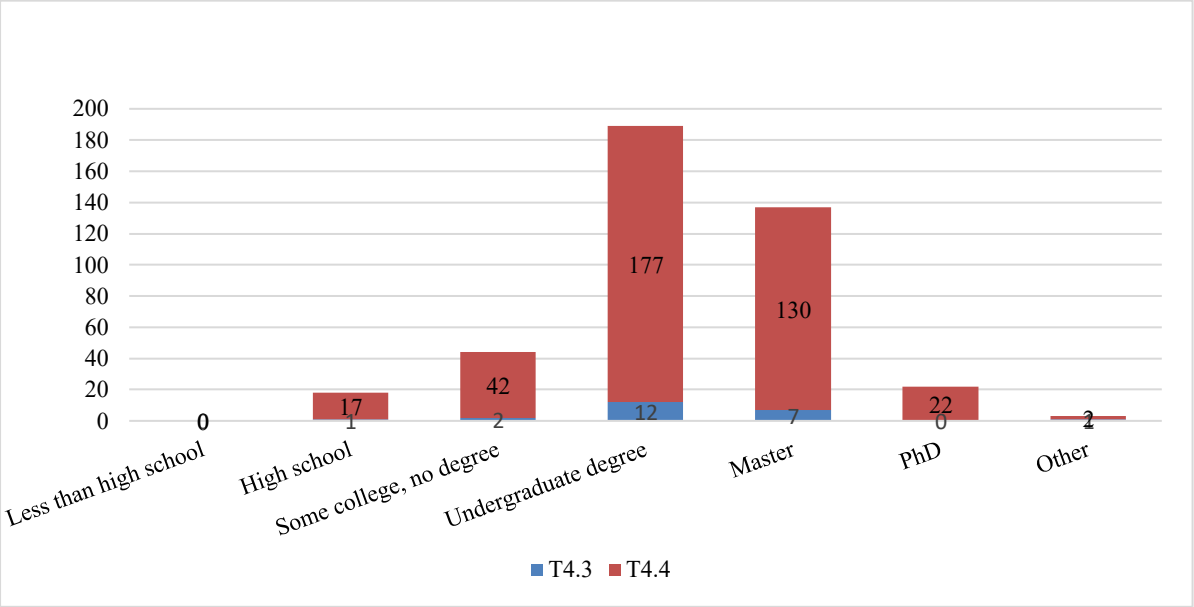

Figure 18: Number of learners in implemented CSP modules per Educational Background

4.2.8.4 Professional Experience and Affiliation

Figure 19 shows the absolute number of learners by professional experience and affiliation category. Since a single learner may match multiple categories, the counts are not mutually exclusive and therefore should not be interpreted as summing to the total number of participants. Instead, the figure provides an overview of how learners are distributed across different professional profiles and organisational affiliations, highlighting the diversity of backgrounds represented in the implemented CSP modules.

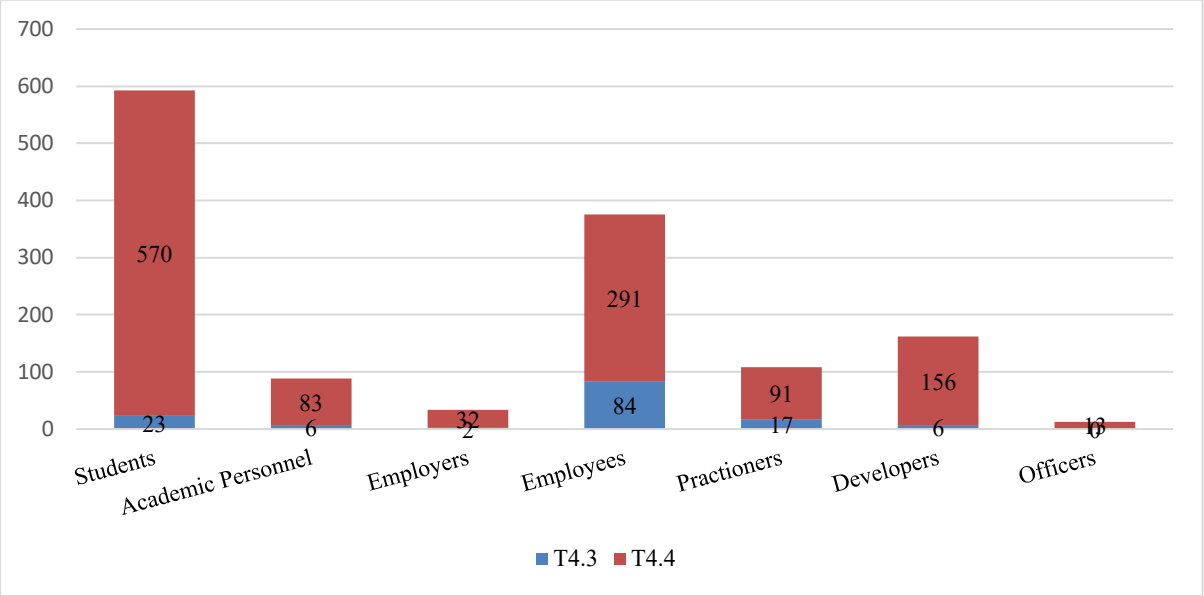

Figure 19: Learners professional Experience and Affiliation

Table 9 presents some project KPIs related to background characteristics of learners. Regarding age distribution, higher number of learners over 45 years old (35 learners). In terms of educational background, it has involved considerable number of non-ICT graduates (76 learners). Also, concerning prior cybersecurity knowledge, T4.3 includes 281 self-trained learners.

Table 9: Project KPIs related to learner's background

Learners Background	T4.4
Number of learners more than 45 years old	35
Number of learners, who are non-ICT graduates	76
Number of learners, who are cybersecurity self-trained	281

4.2.9 Hosting sites

Figure 20 shows the number of implemented CSP modules by type of host. Followed market-demand, the results indicate a relatively balanced distribution between companies and EU HEIs. However, EU HEIs host the largest number of CSP modules, with 18 implemented modules, followed closely by companies with 11 modules. Other types of hosts account for the remaining 16 modules.

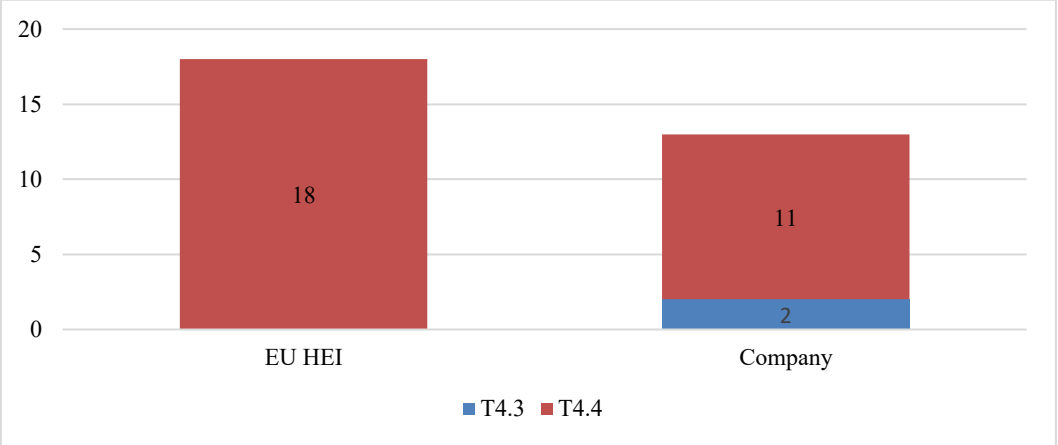

Figure 20: Number of implemented CSP modules per Module host

4.2.10 Evaluation forms of trainees and trainers

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

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

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

CyberSecPro Trainee Evaluation Form

The evaluation is conducted from the learner's perspective through a digital "Evaluation Survey" integrated into the CSP Admin Portal, where trainers can independently designed and customised surveys for each module by selecting relevant pre-defined questions covering areas such as content, structure, instruction, platform, interaction, impact, and overall insights; once finalised, the system automatically generated a unique URL and QR code to enable easy distribution of the survey to learners via multiple digital channels. Figure 21 shows a screen shot of CyberSecPro learner evaluation form in the Admin Portal.

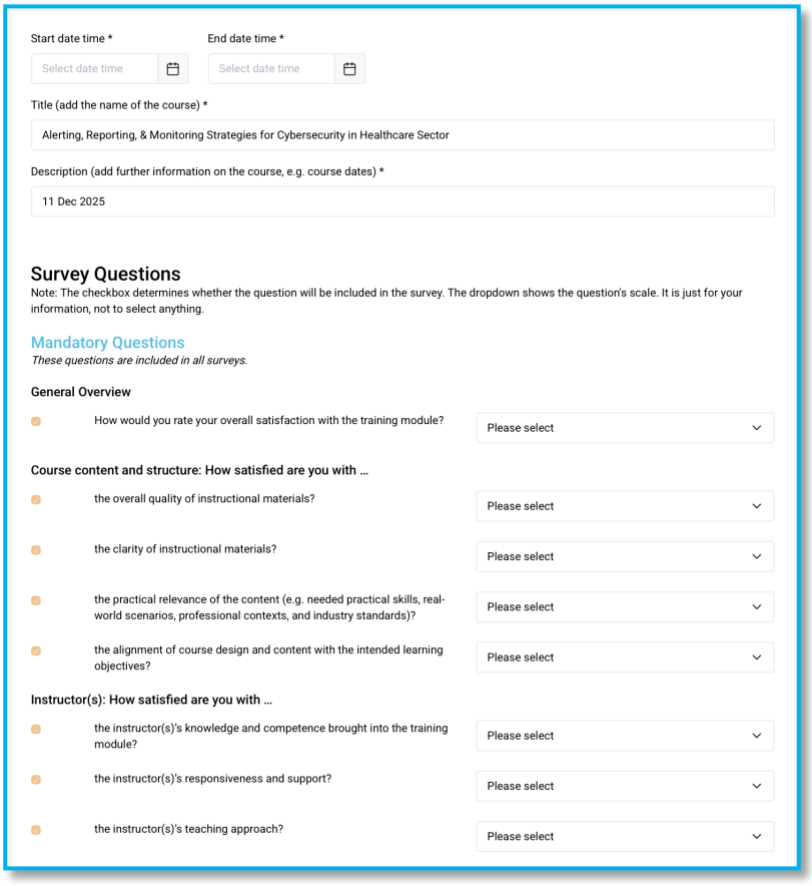

Figure 21: Screen shot of CyberSecPro Trainee Evaluation Form in the admin Portal

CyberSecPro Trainer Evaluation Form

The evaluation of the training implementation from the trainers' perspective conducted using the "Evaluation Survey" feature integrated into the CSP Admin Portal. This feature allows trainers to reflect on and assess their own experience in delivering the module, focusing on aspects such as ease of use of the training materials, interaction with learners, and overall satisfaction with the training implementation process. The trainer survey was automatically generated within the portal for each module implementation. As the survey is standardised, trainers did not need to create the survey from scratch as in the case for learners. The survey can be found under each respective module, allowing trainers to select and complete the survey relevant to their implementation. More information on the survey is described in D5.1 and D5.2 with results reported in D5.2. Figure 22 shows a screen shot of CyberSecPro trainer evaluation form in the Admin Portal.

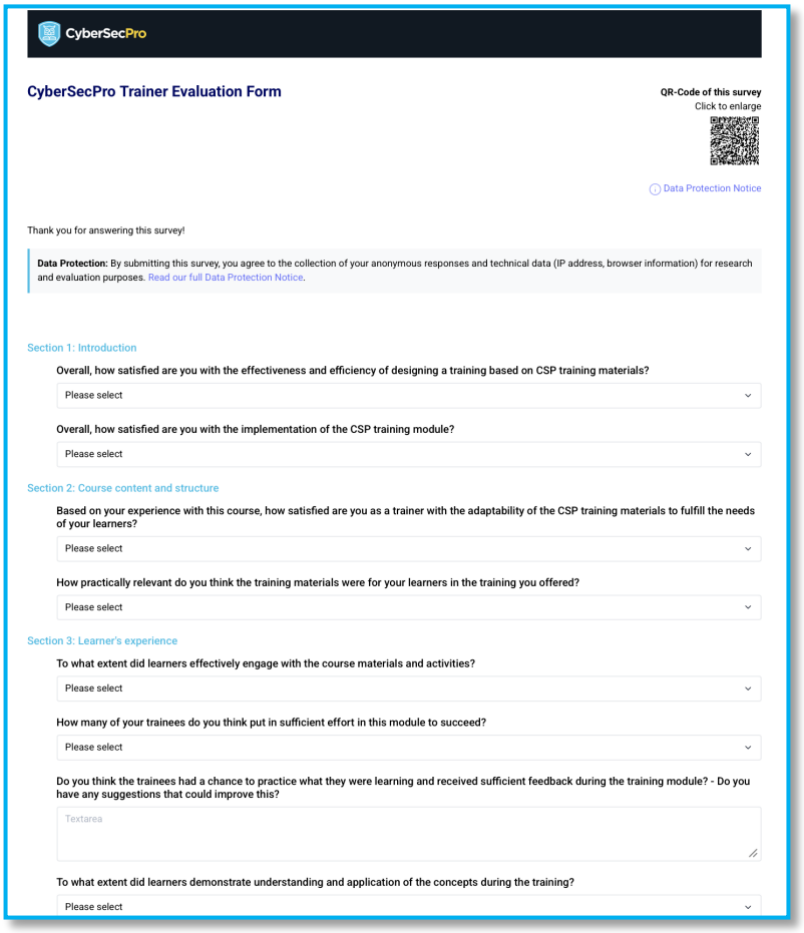

Figure 22: Screen shot of CyberSecPro Trainer Evaluation Form in the admin Portal

Follow-up survey

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

For the follow-up survey, we followed two approaches to ensure that we collected the required data as accurately as possible. In the first approach, individual module implementation providers gather required data from their learners and completed the required information themselves by filling in the seventh tab of the Admin Portal, labelled “Employment.” A screenshot of this survey of the Admin Portal is shown in Figure 23.

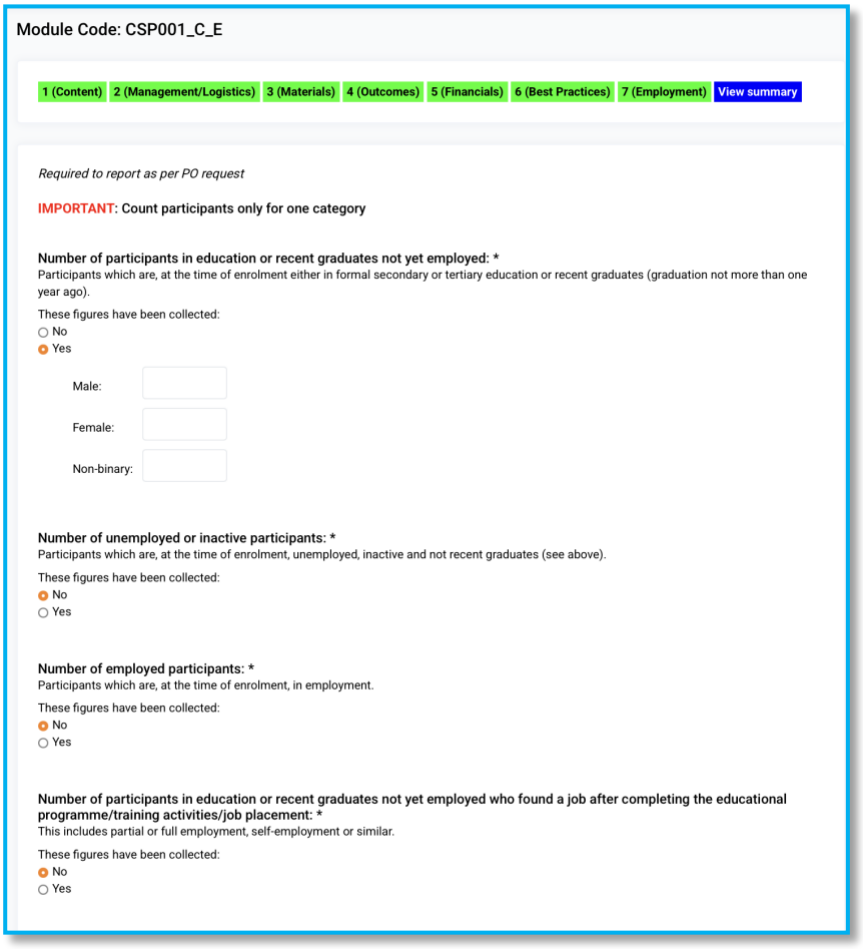

Figure 23: Screen shot of Follow-up survey in the admin portal

In the second approach, as described in D5.2, WP5 followed up with the learners from seasonal schools and collected all the required data. The questionnaire was implemented in the Admin Portal and completed online, with all responses automatically gathered and stored in the system. A screenshot of the implemented questionnaire in the Admin Portal is shown in Figure 24. All results reported in the in the KPI section in the EC SYGMA portal.

Figure 24:Follow-up survey in the admin portal

5. Summary and Conclusion

This deliverable presents the outcomes of Task T4.4 up to Month 39 (February 2026). Accordingly, it documents all implemented CSP modules corresponding to the capability category Cybersecurity Tools and Technologies delivered under Task 4.4 by the end of February 2026 (M39). In addition, 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.

In response to observed demand, the analysis shows that a total of 46 training modules were implemented across multiple industry sectors, including energy, health, maritime, and general cybersecurity. The results indicate [a predominantly basic-level / a mixed-level] implementation profile, a strong emphasis on [seminars/workshops/courses] as delivery formats, and substantial learner participation in both sector-specific and cross-sectoral modules. The distribution of modules and learners across sectors further confirms alignment with the project's focus on critical domains while maintaining broad relevance of the tools-and-technologies training offer.

Overall, this deliverable provides evidence of the effective deployment and reach of the CyberSecPro training programme in the area of Cybersecurity Tools and Technologies. The reported results support monitoring of implementation progress and provide actionable input for refining future training activities, thereby contributing to the CyberSecPro project's broader 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 10 We have also synchronized this template with the descriptions for training modules D3.1.

Table 10: 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)	

CSP Module Elements	CSP Module fields legend	CSP Module information
	Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.	
	Learning outcomes and targets (mandatory) *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1*	
	Type of the implemented CSP module (mandatory) *Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), CyberSecurity Exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.*	
	Affiliated (Summer/Winter) School *Indicates summer school affiliated, (CyberHot 2024, CyberHot 2025, Summer school 2024 Madeira, Summer school 2024 Porto, Winter school 2025 Lisbon, Summer school 2025 Novi Sad- Week 1, Summer school 2025 Novi Sad- Week 2, Winter school 2026, Lisbon*	
	Information on the sector (mandatory) *Indicates General, Maritime, Health, or Energy*	
	Pre-requisites (mandatory) *Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)*	
	Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of the implemented CSP module within the ECSF (currently in this link). It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)*	
	Provision type and location (mandatory) *Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website*	
	Types of assignments *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	
	Level (mandatory) *B (Basic), A (Advanced)*	
	Language (mandatory) *Indicates the spoken and the languages for the material and the assessment/evaluation*	Spoken: Material: Assessment:
Management /Logistics	**Provider(s)** (mandatory) *Name(s) of the providing organisation(s), e.g., beneficiary/ies*	
	Hosted of the module *Select the type of organization that hosted this implemented module (EH HEI, Company, other)*	
	Host details *A freetext to provide additional details about the host organization (name, location, specific department, etc.)*	
	Number of seminars/lectures held by industry experts: * *Required to report these KPIs in relation to the call.*	

CSP Module Elements	CSP Module fields legend	CSP Module information
	Indicate number of "From members of the consortium" as well as number of "Not from members of the consortium"	
	Contact (mandatory) *Full name(s) of the main contact person(s) including their email address*	
	Trainer(s) *All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training*	
	Tool(s) used (mandatory) *A list of tools that have been used for the implemented CSP module* *Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program"*	
	Registration procedure *How (e.g., where and when registration of learner took place) did learner have to register* *If there is no registration procedure, please write, "None"*	
	Admission criteria *Limits of admission (if any), requirements and selection criteria, e.g., knowledge prerequisites, e.g., modules that learners need to have attended before or knowledge that is essential to understand the course (e.g., basics of cryptography or security management).* *If there are no admission criteria, please write, "None"*	
	The actions that were taken to attract learners especially those coming from disadvantaged groups, and the scholarships and mobilities included (if any) *If there are no actions, please write, "None"*	
	ECTS *The number of ECTS* *If there is no ECTS, please write, '0'*	
	Calculation of number of ECTS e.g., (duration of implemented module [hours] + duration of self-study [hours])/25) *Make sure that the number of ECTS matches the learning effort of the training (i.e. 1 ECTS is awarded per 25-30 hours of learning, depending on the national legislation)*	
	Certificate of Attendance (CoA) (mandatory) *Indicates Yes or No (and the conditions for yes, e.g., partial or full attendance, passing of exam)*	
	Provide explanation if Certificate of Attendance (CoA) not happened	
	Exact dates, when offered (mandatory) *Indicates the dates* (year, month, day*) for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information*	
	Schedule and *Duration of the implemented CSP*	

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

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

CSP Module Elements	CSP Module fields legend	CSP Module information
	education institutions *	
	Number of female participants benefitting from financial support	
	Cost-benefit analysis of the modules *The amount of money paid for the course and the amount of income earned from the course* *If there is no money in and no money our and no cost-benefit analysis of the module, please write, "None".*	
Recommendations for Best Practices **Brief suggestions to enhance the effectiveness of CSP training (Lessons learnt)**	**Recommendations for improving the module** *Brief practical suggestions to elevate and improve the future CSP training module quality*	*For example:* • *Enhance the training module with more interactive exercises.* • *Continuously update the module with the latest cybersecurity trends.*
	Recommendations for expanding the reach of the module *Brief practical suggestions to expand the reach to a wider audience and diversifying delivery methods*	*For example:* • *Partner with industry.* • *Promote the module through targeted marketing.*
	Recommendations for future initiatives *Brief practical suggestions and future recommendation for proactive strategies to further strengthen cybersecurity training initiatives and address emerging challenges*	*For example:* • *Implement Standard Cybersecurity Framework in syllabi.* • *Foster collaboration with industry clusters for ongoing professional development opportunities for the participants of the training.* • *Foster EU member state collaboration on cybersecurity training offerings.*
Employment	**Number of participants in education or recent graduates not yet employed** *Participants which are, at the time of enrolment either in formal secondary or tertiary education or recent graduates (graduation not more than one year ago).* *If the answer is yes, indicate the figure by gender.*	
	Number of unemployed or inactive participants *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	

CSP Module Elements	CSP Module fields legend	CSP Module information
	graduates not yet employed who found a job after completing the educational programme/training activities/job placement *This includes partial or full employment, self-employment or similar.* *If the answer is yes, indicate the figure by gender.*	
	Number of unemployed or inactive participants who found a job after completing the educational programme/training activities/job placement *This includes partial or full employment, self-employment or similar.* *If the answer is yes, indicate the figure by gender.*	
	Number of employed participants who improved their employment situation after completing the educational programme/training activities/job placement *This includes transit from precarious to stable employment or from underemployment to full employment or transit to a job requiring higher competences/skills/qualifications and/or more responsibilities or a promotion to a higher-level job.* *If the answer is yes, indicate the figure by gender.*	

Annex B: Template for Planning the Offering of CSP Modules

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

Table 11: Template for planning the CSP Modules offering.

CSP Module Elements	CSP Module [Fields legend]	CSP Module Information
Overview	**Code** *Mandatory field. Code format:* *For general modules: CSP[n]_x* • *[n] is the CSP module number (currently between 001 and 012)* • *x is the module offering type (see below)* *For sector-specific modules: CSP[n]_x_y* • *[n] is the CSP module number (currently between 001 and 012)* • *x is the module offering type (see below) and y is the sector (E, H, M)*	
Content	**Module title as defined in the CSP catalogue** *Mandatory field. The title of the module as defined in the CSP catalogue (currently in D4.1)*	
	Title of the implemented CSP module *Mandatory field. The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned in D3.3, D3.4 or D3.5, but in any case, one that can be proven after the implementation, e.g., from local documentation.*	
	Description of the implemented CSP module *Mandatory field. Usually, the module description from the syllabus (D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module.*	
	Related knowledge area(s) *Mandatory field. Mapping to the 10 selected CSP knowledge areas defined in D2.3.*	
	Indicate whether in the implemented CSP module, learners will learn how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome *Mandatory field. Yes (also if a part of the module covered this topic) or No (otherwise)*	
	Category/ies of capabilities *Mandatory field. Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.*	
	Learning outcomes and targets *Mandatory field. A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1*	
	Type of the implemented CSP module	

	Mandatory field. Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.	
	Information on the sector *Mandatory field. Indicates General, Maritime, Health, or Energy*	
	Pre-requisites *Mandatory field. Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)*	
	Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of the implemented CSP module within the ECSF (currently in this link). It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)*	
	Provision type and location *Mandatory field. Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website*	
	Types of assignments *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	
	Level *Mandatory field. B (Basic), A (Advanced)*	
	Language *Mandatory field. Indicates the spoken and the languages for the material and the assessment/evaluation*	Spoken: Material: Assessment:
Management/ Logistics	**Provider(s)** *Mandatory field. Name(s) of the providing organisation(s), e.g., beneficiary/ies*	
	Contact *Mandatory field. Full name(s) of the main contact person(s) including their email address*	
	Trainer(s) *All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training*	
	Tool(s) to be used *Mandatory field. A list of tools that are to be used for the implemented CSP module.* *Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program".*	
	Registration procedure *How (e.g., where and when registration of learner will take place) will learner have to register.*	
	Admission criteria *Limits of admission (if any), requirements and selection criteria, e.g., knowledge prerequisites, e.g. modules that learners need to*	

	have attended before or knowledge that is essential to understand the course (e.g., basics of cryptography or security management).		
	ECTS *The number of ECTS*		
	Certificate of Attendance (CoA) *Mandatory field. Indicates Yes or No (and the conditions for yes, e.g., partial or full attendance, passing of exam)*		
	Exact dates, when offered *Mandatory field. Indicates the dates (year, month, day) for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information*		
	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

In this section the below evaluation forms template introduce:

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

CyberSecPro Learners Evaluation Form

CyberSecPro learners Evaluation Form

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

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

Mandatory Questions
These questions are included in all surveys.

General Overview
How would you rate your overall satisfaction with the training module?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Course content and structure: How satisfied are you with …
the overall quality of instructional materials?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐
the clarity of instructional materials?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐
the practical relevance of the content (e.g. needed practical skills, real-world scenarios, professional contexts, and industry standards)?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐
the alignment of course design and content with the intended learning objectives?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Instructor(s): How satisfied are you with …
the instructor(s)'s knowledge and competence brought into the training module?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐
the instructor(s)'s responsiveness and support?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐
the instructor(s)'s teaching approach?
Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Impact
How relevant are the skills and knowledge gained to your current or desired job role?
Not Relevant at All☐ Low Relevance☐ Slightly Relevant☐ Somewhat Relevant☐ Moderately Relevant☐ Very Relevant☐ Extremely Relevant☐
To what extent did this course enhance your knowledge and skills?
Not at All☐ to a Very Small Extent☐ to a Small Extent☐ to a Moderate Extent☐ To a Fairly Large Extent☐ To a Large Extent ☐ To a Very Large Extent ☐
How likely are you to further explore the topic of the module (e.g. through self-learning or another course)?
Extremely Unlikely☐ Unlikely☐ Slightly Unlikely☐ Neutral☐ Slightly Likely☐ Likely☐ Extremely Likely ☐

Optional Questions

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

Learning Platform: How satisfied are you with …

the accessibility of the learning platform?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

the ease of navigation of the learning platform?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

the visual appeal of the platform?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Community / Interaction: How satisfied are you with …

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

the interaction facilitated between learners?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Evaluation & Recognition: How satisfied are you with …

the transparency of the examination process?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

the fairness of the examination process?

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Closing Questions

These questions are included in all surveys.

Final questions

How likely are you to recommend this learning experience to someone looking to improve skills in the cybersecurity field?

0 - Not at all likely 1 2 3 4 5 6 7 8 9 10 - Extremely likely

How could the overall learning experience be enhanced? ……

Any further comments you like to share: ……

CyberSecPro Trainer Evaluation Form

CyberSecPro Trainer Evaluation Form

Thank you for answering this survey!

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

Section 1: Introduction

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Section 2: Course content and structure

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

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

Section 3: Learner's experience

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

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

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

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

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

Do you have any suggestions that could improve this?

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

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

Section 4: Learning Platform (optional)

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Section 5: Community / Interaction (optional)

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

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

Strongly Dissatisfied☐ Dissatisfied☐ Somewhat Dissatisfied☐ Neutral☐ Somewhat Satisfied☐ Satisfied☐ Very Satisfied☐

Section 6: Impact on students

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

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

Section 7: Recommendation

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

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

Extremely Unlikely☐ Unlikely☐ Slightly Unlikely☐ Neutral☐ Slightly Likely☐ Likely☐ Extremely Likely☐

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

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

Any further comments you like to share: …….

Additional CyberSecPro Evaluation Template

Additional CyberSecPro Training Module Evaluation Template: Enrolled learner

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

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

3. What is the highest level of education you have completed?
   Less than high school☐ High school☐ Diploma or equivalent☐ Some college, no degree☐ Undergraduate degree (Bachelor's) ☐ Master's degree☐ Doctoral (PhD) ☐ Other☐

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

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

6. Please indicate if you belong to any of the following categories (you may select more than one):
   Student ☐ Academic personal☐ Employer☐ Employee☐ Practitioner☐ Developer☐ Officer☐ In education or a recent graduate not yet employed (either in formal secondary or tertiary education or a recent graduate (graduation not more than one year ago)) ☐ Unemployed, inactive and not a recent graduate☐

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

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

1. What is your gender?
   Male☐ Female☐ Non-Binary☐ Prefer not to answer☐
2. Have you carried out a job-placement/internship? Yes ☐ No ☐
3. If yes, please indicate in which company? _____
4. Have you experienced an improvement in your employment situation since completing the training supported by the program? Yes ☐ No ☐

5. Which of the following best describes your change of situation after completing the educational programme/training activities/job placement?
   a) You were in education or a recent graduate/ not yet employed before educational programme/training activities/job placement and found a job after completing the educational programme/training activities/job placement (This includes partial or full employment, self-employment or similar) □
   b) You were unemployed or inactive before educational programme/training activities/job placement and found a job after completing the educational programme/training activities/job placement (This includes partial or full employment, self-employment or similar) □
   c) You were employed before educational programme/training activities/job placement and improved your employment situation after completing the educational programme/training activities/job placement (This includes transit from precarious to stable employment or from underemployment to full employment or transit to a job requiring higher competences/skills/qualifications and/or more responsibilities or a promotion to a higher-level job) □
   d) Other □
6. Have you participated virtually in a full online course and completed it? Yes □ No □
7. If the answer of question 6 is yes, have you received certification after the successful completion of the full online course? Yes □ No □

   7.1 If yes, please answer the following questions:

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

   b) What is the highest level of education you have completed?
   Less than high school□ High school□ Diploma or equivalent□ Some college, no degree□
   Undergraduate degree (Bachelor's) □ Master's degree□ Doctoral (PhD) □ Other□

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

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

1. What is your age?
   Under 18□ 18- 25□ 26-34□ 35-45□ 45+-54□ 55-65□ More than 65□
2. What is your gender?
   Male□ Female□ Non-Binary□ Prefer not to answer□
3. What is the highest level of education you have completed?
   Less than high school□ High school□ Diploma or equivalent□ Some college, no degree□ Undergraduate degree (Bachelor's) □ Master's degree□ Doctoral (PhD) □ Other□
4. What is your Country of origin (the country where you were born)? _____

Annex E: Additional statistics of Implemented CSP Modules

Number of learners in CSP modules per module level

Figure 25 presents the distribution of learners across CSP modules by training level. The data indicate a slightly higher number of learners enrolled in Basic-level modules (489) compared to Advanced-level modules (467). When the T4.3-relevant share of CSP003 is also included, the totals rise to 559 learners at Basic level and 517 learners at Advanced level.
Overall, the figures point to strong interest in both proficiency levels, with a modest tilt toward foundational training. This aligns with the implementation profile, where Basic-level delivery was marginally more frequent (25 Basic modules vs. 20 Advanced modules). At the same time, the comparatively high participation in Advanced modules shows that the CyberSecPro training programme engages learners across different competency stages and supports progression toward more specialised skills within the cybersecurity tools and technologies capability area.

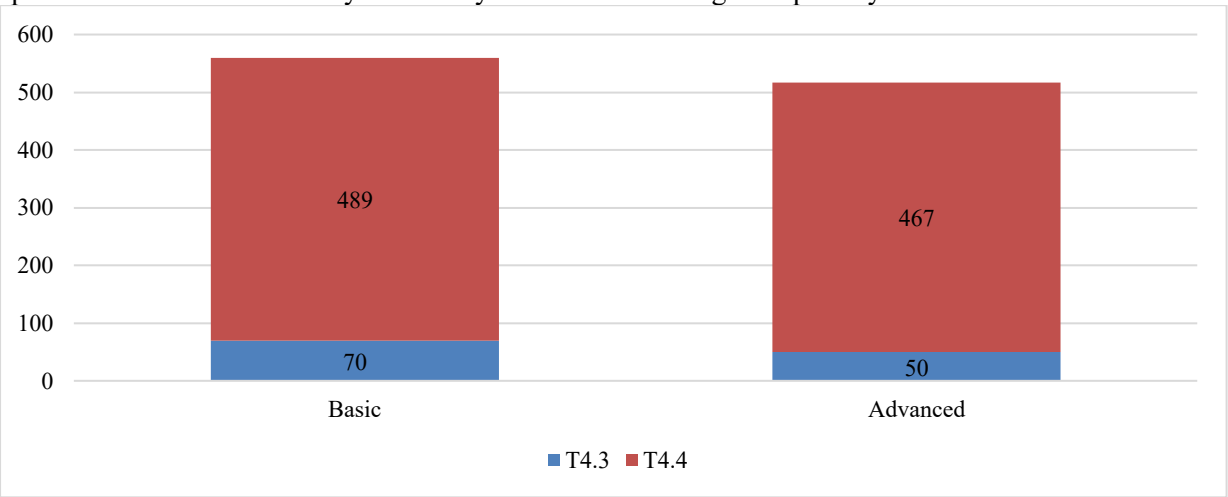

Figure 25: Number of learners in implemented CSP modules per module level

Number of learners in CSP modules per module type

Figure 26 presents the distribution of learners across CSP modules by module type. The results indicate that seminars attracted the highest number of learners (436), followed by courses (276), workshops (134), and hackathons (110). When the T4.3-relevant share of CSP003 is also included in the overview, the corresponding totals rise to 556 learners for seminars.

Overall, the pattern suggests that the more scalable formats (seminars and workshops) drove the largest participation, while courses and exercises provided more targeted learning experiences that complement the wider training offer.

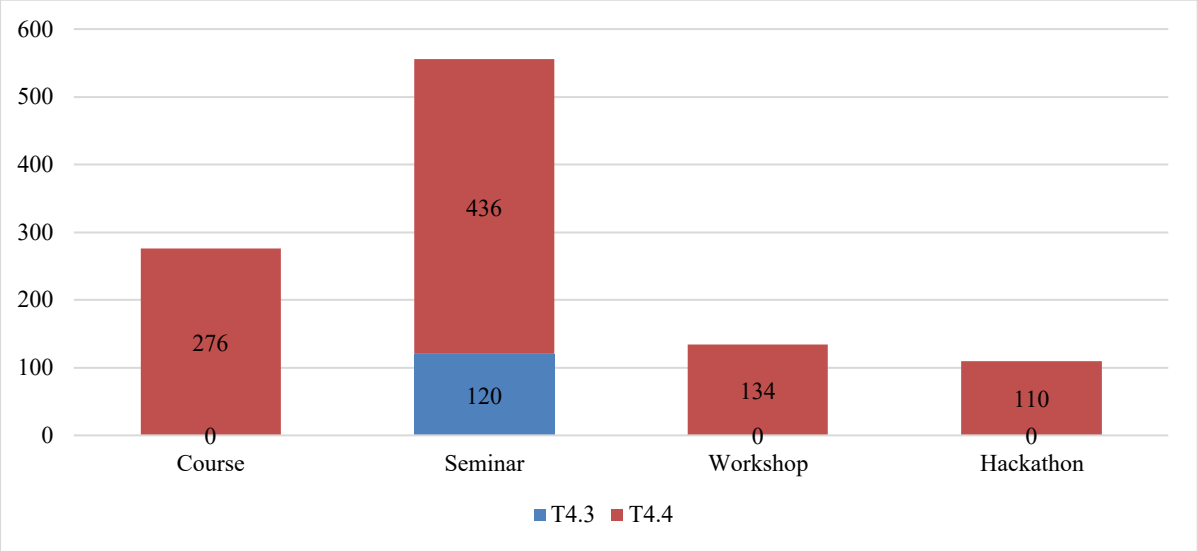

Figure 26: Number of learners in implemented CSP modules per module type

Number of implemented CSP modules per module sector and level

In line with observed demand, Figure 27 presents the distribution of implemented CSP modules across industry sectors and training levels. For Basic-level delivery, Health accounts for the highest number of implemented modules (15), followed by General (9), while Energy and Maritime record the lowest numbers (1 and 0).

Across all sectors, the number of Advanced-level implementations is comparable. Energy and General show a higher level of Advanced delivery (9 and 7 modules respectively) compared to Maritime (3) and Health (2) suggesting targeted implementation of advanced training where demand and learner profiles supported it.

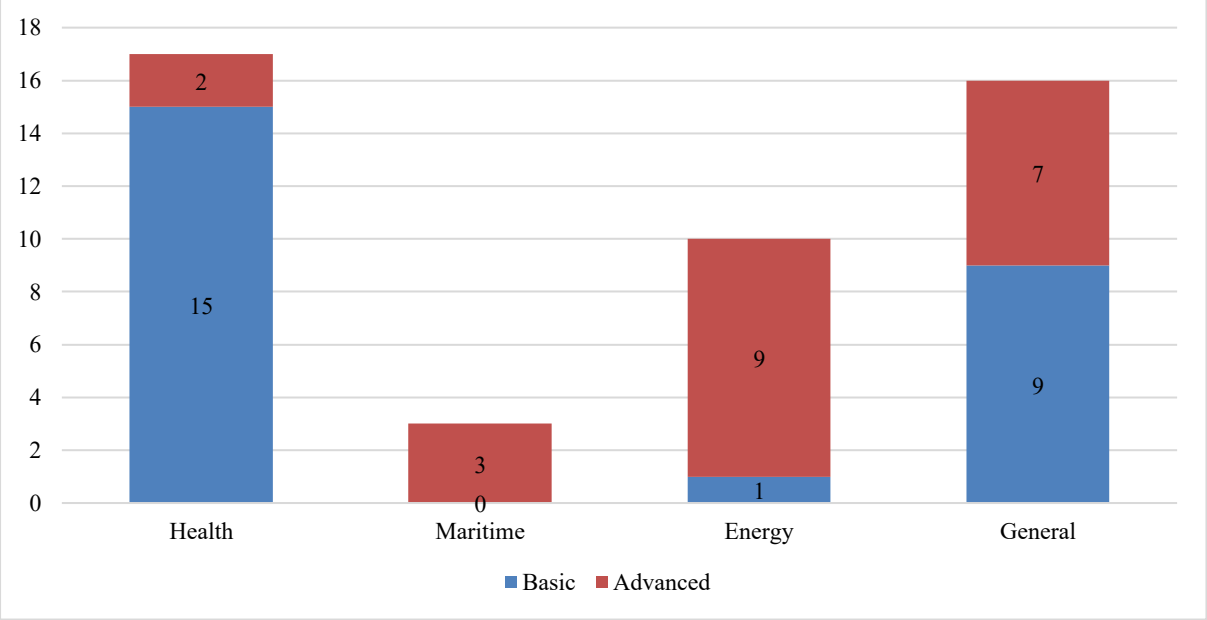

Figure 27: Number of implemented CSP modules per module sector and level (T4.4 only)