Project No. 101083594 Project start: 2022-12-01
Call: DIGITAL-2021-SKILLS-01 Project duration: 36 months

CyberSecPro

D4.1
CyberSecPro Training Operational Plan

Document Identification	
Due date	2023-10-30
Submission date	2024-01-03
Version	1.0

Related WP	WP4	Dissemination Level	PU
Lead Participant	SINTEF	Lead Author	Nektaria Kaloudi, Per Håkon Meland
Contributing Participants	UMA, UPRC, LAU, GUF, PDMFC, TALTECH, TUC, UCY, TUBS, AIT, COFAC, UNINOVA, APIRO, C2B, FP, ITML, SEA, SGI, SLC, TRUSTILIO, ZELUS, FCT, UNSPMF, MAG	Related Deliverables	D2.2 – Blended CyberSecPro technological training interactive technologies and academic practice, D2.3 – CyberSecPro programme specifications

Abstract: The CyberSecPro Deliverable D4.1 deliverable reflects the outcomes of tasks T4.1 and T4.2 till Month 11. Therefore it outlines the operational scalable offering for the CyberSecPro training modules, which cover the ten prioritized CyberSecPro knowledge areas. Consequently, this deliverable lists all the training modules that each partner intends to develop and offer. These are then grouped into a list of 12 CyberSecPro modules, with various synergies proposed to assist in crafting their syllabi and facilitating their operation. Evaluation forms for trainers and trainees are provided, as well as a methodology for planning and implementing Massive Open Online Courses (MOOCs). Moreover, the deliverable aims at providing mobilization mechanisms in order to attract and engage internal and external trainees and trainers.

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

The CyberSecPro Deliverable D4.1 introduces a catalogue of 12 CyberSecPro training modules. Therefore it outlines the operational scalable offering for the CyberSecPro training modules, which cover the ten prioritized CyberSecPro knowledge areas.

Methodology: In order to achieve Deliverable D4.1, this report followed a systematic process with concrete steps that enabled to:

- Create a template to collect information from partners about training modules they intend to develop and offer, contributing to CyberSecPro training modules' catalogue.
- Collect training modules from each CyberSecPro partner.
- Analyse and cluster the collected training modules to create a feasible and harmonized dynamic CyberSecPro operational plan. The initial scheduling is also provided.
- Provide mobilization mechanisms to attract and engage internal and external trainees and trainers

This work was conducted as part of tasks 4.1 "*Planning of Trainings*" and 4.2 "*Trainees and Trainers Mobilization"* of CyberSecPro project. A core objective of both tasks is to create a consolidated and harmonized catalogue of unique CyberSecPro training modules and to foster mobilization mechanisms in order to engage as many trainees and trainers as feasible.

Findings and outcomes: The main findings from this deliverable are as follows.

- A collection of a total of 128 training modules from partners, with 116 as individual offerings and 12 as joint modules involving collaboration between at least two partners.

- A list of 12 proposed 12 CyberSecPro training modules that form the basis of the catalogue. These modules will be further developed in order to create their syllabi and facilitate their operation.

- Based on the results, recommendations for synergies are provided to promote collaboration between academia and industry, ultimately delivering a unique professional training programme comprised of innovative hands-on training modules.

Conclusion: This CyberSecPro deliverable D4.1 reflects the outcomes of tasks T4.1 and T4.2 at Month 11. Therefore it lists all the training modules each partner intends to develop and offer. These modules are then grouped into a list of 12 CyberSecPro modules, with various synergies proposed to assist in crafting their syllabi and facilitating their operation. Consequently, the deliverable presents a catalogue of CyberSecPro training modules. Moreover the deliverable provides mobilization mechanisms to attract and engage internal and external trainees and trainers. In this way the deliverable lays the ground for the collaboration in designing and implementing the CyberSecPro programme and its modules.

Document information

Contributors

Name	Beneficiary
Nektaria Kaloudi, Per Håkon Meland	SINTEF
Cristina Alcaraz, Javier Lopez, Ana Isabel Cerezo Domiguez	UMA
Nineta Polemi, Theodoros Karvounidis, Panagiotis Kotzanikolaou, Christos Douligeris, Spyros Papageorgiou, Antonios Andreatos	UPRC
Paresh Rathod, Paulinus Ofem, Kaci Bourdache, Pasi Kämppi, Anssi Mattila, Soili Martikainen, Seppo Koponen, Outi Grotenfelt, Timo Ryynänen, Veli Sulkava, Jyri Rajamäki, Eveliina Hytönen	LAU
Stylianos Karagiannis, Luís Miguel Campos	PDMFC
Kai Rannenberg, Atiyeh Sadeghi	GUF
Dan Heering, Adrian Venables, Rain Ottis, Risto Varandi, Ricardo Gregorio Lugo	TALTECH
Pinelopi Kyranoudi, Charalampos-Ioannis Mitropoulos, Manos Athanatos	TUC
Elias Athanasopoulos	UCY
Stefan Schauer, Martin Latzenhofer	AIT
Nuno Mateus-Coelho	COFAC
Vasco Delgado-Gomes	UNINOVA
Argyro Chatzopoulou, Apostolis Karras	APIRO
Bruno Bender	C2B
Christos Grigoriadis	FP
Dimitra Siaili	ITML
Sebastian Pape	SEA
Martin Bärmann	SGI
Shareeful Islam, Athina Labropoulou	SLC
Kitty Kioskli, Maria Lambrou	TRUSTILIO
Stella Markopoulou, Christos Kargatzis	ZELUS
José Fonseca	FCT
Danijela Boberić Krstićev	UNSPMF
Fabio Martinelli	CNR
Spiros Borotis	MAG

Reviewers

Name	Beneficiary
Danijela Boberić Krstićev	UNSPMF
Fabio Martinelli	CNR

History

Version	Date	Contributor(s)	Comment(s)
0.01	2023-07-04	Nektaria Kaloudi	1st Draft of ToC
0.02	2023-08-26	Cristina Alcaraz, Nineta Polemi/ Theodoros Karvounidis	Comments and Feedback

0.03	2023-08-31	Nektaria Kaloudi/Per Håkon Meland	Updated ToC
0.04	2023-09-11	Nektaria Kaloudi, Nineta Polemi, Paresh Rathod, Stylianos Karagiannis, Cristina Alcaraz	CSP training modules – First iteration (Section 3)
0.05	2023-09-14	Nektaria Kaloudi	Content writing in Introduction and Methodology. Revisions in the Section 3. Integrate inputs of CSP training modules from partners from the first iteration.
0.05	2023-09-18	Nineta Polemi, Kai Rannenberg/Atiyeh Sadeghi, Danijela Boberic Krstićev	Feedback from the first high-level review
0.06	2023-09-23	Stylianos Karagiannis	Updates on Section 4
0.07	2023-09-26	Paresh Rathod, Paulinus Ofem	Updates on Section 5
0.08	2023-10-11	All partners	CSP training modules – Second iteration (Section 3)
0.09	2023-10-12	Kai Rannenberg/ Atiyeh Sadeghi	Further improvements on Section 5
0.10	2023-10-13	Stylianos Karagiannis	Updates on Section 4
0.11	2023-10-13	Nektaria Kaloudi	Incorporating training modules from partners (Section 3)
0.12	2023-10-13	Nektaria Kaloudi/Per Håkon Meland	Evaluation templates and creating initial CSP programme (Section 3)
0.13	2023-10-16	Paresh Rathod, Nineta Polemi	Feedback
0.14	2023-10-16	Nektaria Kaloudi/Per Håkon Meland	Verify content and send deliverable for review
0.15	2023-10-20	Nektaria Kaloudi, Cristina Alcaraz	Add diagrams
0.16	2023-10-21	Danijela Boberić Krstićev, Fabio Martinelli, Adisa Ejubovic	Feedback on the deliverable as part of the first review
0.17	2023-10-23	Nektaria Kaloudi	Revisions based on the collected feedback, Diagrams improvements
0.18	2023-10-24	Nektaria Kaloudi	Further updates after WP4 meeting, Content writing
0.19	2023-10-25	Nektaria Kaloudi, Spiros Borotis	Updating of training modules
0.20	2023-10-27	Nektaria Kaloudi	Final changes after feedback received, editorial fixes.
0.21	2023-11-02	Vasco Delgado-Gomes, Nektaria Kaloudi, Paresh Rathod, Paulinus Ofem, Per Håkon Meland, Nineta Polemi, Kai Rannenberg	Alignment between D3.1 and D4.1
0.22	2023-11-03	Carlos Nuno Marques	Inputs in Section 4
0.23	2023-11-07	Nektaria Kaloudi/Per Håkon Meland	Further improvements

0.24	2023-11-09	Paresh Rathod, Paulinus Ofem, Per Håkon Meland, Nektaria Kaloudi	Feedback from LAU, Improvements on the deliverable, editorial fixes, CSP modules consolidation work
0.25	2023-11-29	Kai Rannberg/ Atiyeh Sadeghi	Further improvements
0.26	2023-12-11	Nektaria Kaloudi/Per Håkon Meland	Further improvements based on the feedback in the second review
0.27	2023-12-19	Kai Rannberg/ Atiyeh Sadeghi	Further improvements based on the feedback from LAU
0.1	2024-01-03	Atiyeh Sadeghi	Final check, layout refinement and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AIT**	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
	APIRO	APIROPLUS SOLUTIONS LTD
C	**C2B**	C2B CONSULTING
	CNR	CONSIGLIO NAZIONALE DELLE RICERCHE
	COFAC	COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL
	CSP	CyberSecPro
E	**ECSF**	European Cybersecurity Skills Framework
F	**FCT**	UNIVERSIDADE NOVA DE LISBOA
	FP	FOCAL POINT
G	**GUF**	JOHANN WOLFGANG GOETHE-UNIVERSITAET FRANKFURT AM MAIN
H	**HEIs**	Higher Education Institutions
I	**ITML**	INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP
L	**LAU**	LAUREA-AMMATTIKORKEAKOULU OY
M	**MAG**	MAGGIOLI SPA
	MOOC	Massive Open Online Courses
P	**PDMFC**	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA
S	**SEA**	SOCIAL ENGINEERING ACADEMY GMBH
	SGI	SERIOUS GAMES INTERACTIVE APS
	SINTEF	SINTEF AS
	SLC	SECURITY LABS CONSULTING LIMITED
	SVN	Subversion versioning tool
T	**TalTech**	TALLINNA TEHNIKAÜLIKOOL
	TRUSTILIO	TRUSTILIO BV
	TUBS	TECHNISCHE UNIVERSITAET BRAUNSCHWEIG
	TUC	POLYTECHNEIO KRITIS
U	**UCY**	UNIVERSITY OF CYPRUS
	UMA	UNIVERSIDAD DE MALAGA
	UNINOVA	UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIASASSOCIACAO
	UNSPMF	UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES
	UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER
W	**WP**	Work Package
Z	**ZELUS**	ZELUS IKE

1 Introduction

1.1 Background

Cybersecurity will continue to pose a significant challenge for the foreseeable future for companies and industries of all sizes across every sector. Existing studies and several market analyses indicate that our digitally connected world faces a growing shortage of qualified professionals equipped to handle specific roles and responsibilities in cybersecurity. This workforce shortage and skills gap is a pressing concern for professionals in the field of cybersecurity, both in the private and public sectors. The EU is not immune from these cybersecurity-related issues due to a lack of cybersecurity professionals and overall cybersecurity capacity. Thus, there is an imperative need to both train the new generation workforce and upskill the existing one to meet the challenging and ever-growing cybersecurity challenges.

Strengthening collaboration between Higher Education Institutions (HEIs) and industries is essential to ensure an agile and dynamic way to monitor cybersecurity industrial challenges, cater to practical training needs, and to provide the necessary skills and capabilities.

The CyberSecPro initiative aims to bridge the gap between degrees, working life, and marketable cybersecurity skill-set necessary in the EU's digitization efforts. It also seeks to offer best practice examples for cybersecurity training programmes. The CyberSecPro project intends to provide dynamic capabilities and emerging skills needed in the market to existing programmes that are part of the academic rigid, static programmes, ensuring they can effectively address the hands-on, dynamic capabilities and emerging cybersecurity skills needed in the market.

Therefore, the CyberSecPro project seeks to introduce a unique professional training programme comprised of innovative hands-on training modules. These modules will address various training needs and levels of expertise, including general and sector-specific modules for the maritime, health, and energy industries.

1.2 Purpose and Scope

This deliverable is produced within the context of CyberSecPro Work Package 4, titled "*Operating CyberSecPro Professional Training Program*". It presents the outcomes of Task 4.1 "*Planning of Trainings*" and Task 4.2 "*Trainees and Trainers Mobilization*". The high-level objective of this deliverable is to establish a comprehensive training operational plan that will be utilized to operationalize the CyberSecPro training programme and its training modules. This plan will facilitate the operation of both the general and sector-specific training modules. These modules will be offered at two different levels of competencies (basic and advanced) within HEIs and companies.

The scope of this deliverable emphasizes planning the deployment and operation of the CyberSecPro hands-on cybersecurity trainings. The resulting plan from this deliverable D4.1 is designed to provide support for the planning phase of the CSP training programme. To realize this, we have developed a catalogue of the CSP training modules, which includes the essential information required for the initial scheduling of the CSP programme.

Additionally, the deliverable includes identifying mechanisms and programmes for fostering trainees' and trainers' mobility to CyberSecPro. These mechanisms may include scholarships and financial aid to make mobility accessible, internship opportunities that bridge the gap between academia and industry, and active engagement of internal and external trainees and trainers. These efforts aim to enrich trainees' educational experiences and ensure the programme's high-quality training by attracting experienced trainers. Partners will leverage their dissemination channels to attract a diverse pool of trainers and trainees, fostering collaboration between educational institutions and industry partners, and enhancing cybersecurity education.

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 of the CyberSecPro trainings, and the operation of the CyberSecPro professional training programme. This WP interacts with the other CyberSecPro work packages in the following manner as follows: it receives information (e.g., knowledge areas as defined in Deliverable D2.3) from WP2 and gathers feedback from WP3. In turn, WP3 receives information about the type and number of training modules that CyberSecPro providers are planning to offer.

1.4 Structure of the Deliverable

The deliverable is organized as follows. Section 2 explains the overall methodological approach used for this deliverable work. In Section 3, we provide the CyberSecPro training modules per CyberSecPro provider that we would like to offer as part of the CyberSecPro programme and a detailed schedule for planning the trainings. This CyberSecPro programme schedule has been analyzed in terms of the CyberSecPro knowledge areas, type and number of training modules, and based on the joint CyberSecPro training modules. Additionally, evaluation forms for both trainers and trainees are provided. In Section 4, we provide the design of mobilization mechanisms between European universities, research centres and industry. Section 5 provides the initial design of MOOCs that will be utilized to provide parts of the training to ensure that they fulfil the planning requirements and the learning targets. Section 6 concludes the document.

2 Methodology

2.1 Overall Approach

For the detailed planning of trainings, our primary objective is the development of the CSP training modules' catalogue. The creation of this catalogue was pursued through a structured, iterative process. The work has been led by SINTEF.

Step 1: Preliminary Meetings and Feedback Collection

We began by organizing initial meetings, during which we presented and received feedback on an initial template designed for capturing training module details.

Step 2: Pilot Collection from a Small Group of CSP Partners

To pilot the collection process of the training modules, we first reached out to a small group of CSP partners, namely (i.e., UMA, UPRC, LAU, PDMFC, and GUF). This group provided the initial collection of information on about which CSP training modules they plan to develop and offer, using the initial template as a guideline for their submissions (as shown in Table 1) for our scheduling. The CSP partners informed us about the specific training modules they plan to develop and offer, whether individually and/or jointly with other partners. They follow the format provided in the template (in Section 2.2). The template is common for the various types of CSP training modules, such as courses, workshops, seminars, cybersecurity exercises, summer school, and hackathons. By following this iterative process and starting from a small sample/group of partners, we could evaluate the effectiveness of our initial template and help to determine if changes to the initial template are needed for the creation of the CSP programme scheduling.

Step 3: Template Synchronization

Working closely with the Task Leader of T3.1 (LAU), we synchronized the work with the templates regarding the modules' syllabus template (or general/common curriculum template) to ensure that the general curriculum template and the template for the CSP training modules' catalogue cover all the information we need to collect.

Step 4: Feedback Incorporation

Before making the template available to all CSP partners, we sought additional feedback from the high-level review process. This feedback enabled us to refine and enhance the template, ensuring its efficacy in capturing the required information.

Step 5: Broader Distribution and Final Data Collection

Then, after this revision period, we distributed the finalized template to all CSP partners. We aimed to collect information about the CSP training modules that partners are planning/intending to develop as part of WP3 and operate as part of WP4 within the CSP project. This data collection phase allowed partners in the CSP project to expand their offerings by providing completely new training modules and considering collaboration for joint module offerings. For example, proposals of co-hosted workshops or seminars jointly with other partners as well or to keep or withdraw the already provided training modules in the WP2 catalogue.

Step 6: CSP Modules Catalogue and Initial Scheduling

The derived training modules that the CSP partners are willing to offer in the CSP programme were further analyzed, categorized, interrelated, and labelled (e.g., some modules coincided, and they were labelled under one main topic). The modules have been described in three dimensions: (i) the knowledge areas they cover, (ii) the categories of capabilities they enhance, and (iii) the sectors they can potentially be applied to. Then, a clustering was done based on the training offerings to construct a catalogue of general modules. The initial scheduling of CSP modules' catalogue was provided. Various CSP partners will offer the modules at various times and locations. The CSP catalogue of modules and the schedule will remain live on our website, and updates will be further indicated there. Figure 1 shows the general process followed in order to create the CSP catalogue of training modules, as shown in Section 3.4.

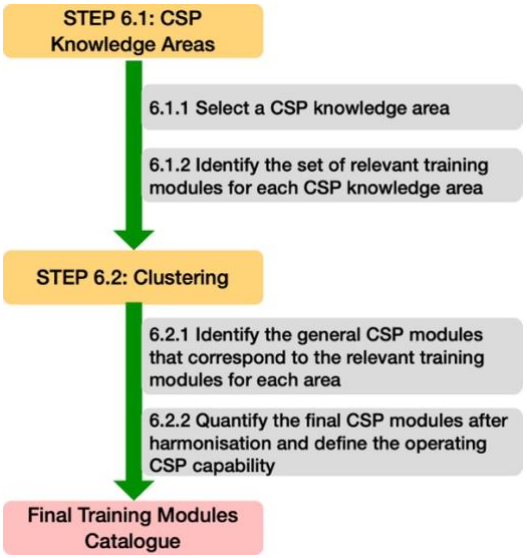

Figure 1. Process for creating the initial CSP catalogue

Rationales for general CSP training module selection:

The final selection of resulting general CSP modules is based on the following considerations:

- **Demand-side analysis:** The general CSP modules aim to provide a full coverage of the whole CSP knowledge areas derived from the D2.3 and consider the full coverage of the identified areas from the market analysis.
    - *Coverage of CSP Knowledge Areas:* The modules aim to cover the entire range of CSP knowledge areas derived from D2.3 and market analysis to ensure relevance.
    - *Micro-Level Selection Criteria:* Specific criteria listed in deliverable D2.3 are considered to align with the identified demand factors.
- **Supply-side alignment:** The clustering is based on the training offerings and expertise of the CSP partners in the project consortium. The general CSP modules are derived from the partners' supply side. The rationale for the CSP module titles is matched with the partners' training offerings and overview.
    - *Utilizing Consortium Expertise:* The modules are derived from the expertise and offerings of CSP partners within the project consortium.
    - *Matching Module Titles:* The rationale for the module titles aligns with the partner institutions' expertise and training offerings.
- **CSP harmonisation:** The consolidation of the general CSP module names took place in collaboration with the WP3 and Task 3.1 Leaders, who will continue developing the CSP modules' syllabi. We aimed for an alignment between D4.1 and D3.1, as well as with the outcomes of the D2.1, D2.2, and D2.3 from WP2. The entire workflow between WP2, WP3 and WP4 gave special attention to harmonising the cybersecurity education and training offerings in EU HEIs.
    - *Collaboration with Other Work Packages:* Close collaboration with the leaders of WP3 and Task 3.1 ensures alignment in developing the syllabi of the CSP modules.
    - *Alignment Across Deliverables:* Consideration of alignment between D4.1, D3.1, and outcomes from D2.1, D2.2, and D2.3 within WP2 to harmonise cybersecurity education and training in Europe.
    - *HEIs Cybersecurity Education and Training Harmonisation:* The process acknowledges the need for harmonization due to the identified fragmentation in cybersecurity training in Europe. The project aims to address this by proposing a clustering of CSP modules and contribute to the development process of syllabi in WP3, while considering the overarching goal of harmonizing cybersecurity education and training across HEIs and industries within the European landscape.

- **European Cybersecurity Workforce Capacity Building Target:** One of the key targets of the CSP project is to consolidate the European cybersecurity workforce working closely with Industry-academia partnerships.
    - *Industry-Academia Partnerships:* The importance of industry-academia partnerships in addressing the cybersecurity workforce shortage is paramount. The CSP general module selection incorporated input from industry-academia participants to ensure that the modules meet the needs of both academia and industry.

The operation of the general CSP modules and their specific module types, will take place in Tasks 4.3 till 4.6. The distribution over four tasks enabled CyberSecPro to distribute and balance the management of the operation among different partners. The four related categories were based on the experiences with aiming for capabilities and skills through cybersecurity education, training, and learning. These experiences were considered during the preparation of the CyberSecPro project proposal and led to the following four CSP capability categories:

1. "Cybersecurity Principles and Management" provides the basis of necessary knowledge and skills and is therefore the first category.
2. "Cybersecurity Tools" follows as a second category, as the support of practical skills is a major goal of CyberSecPro, and these skills often involve tools.
3. "Emerging technologies" is the third category, as for newly emerging technologies there is usually a lack of related cybersecurity capabilities and people with those capabilities. This deficit eases attacks. Overcoming it is another major goal of CyberSecPro.
4. "Cybersecurity offensive practices" are a very relevant, but delicate and controversial area, e.g. because of the ethical and control issues involved when building the respective capabilities. Therefore this area deserves its own category to handle the respective issues.

2.2 Template for the CSP Training Modules' Catalogue

The following Table 1 shows the template used for the CSP training modules' catalogue.

Table 1: Template for CSP training modules' catalogue

Training Module fields	Training Module information
Code (mandatory field) *Code format: PROVIDER NAME(S)_CSP001 (for example, LAU_CSP001). The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*	
Module name (mandatory field) *The title of the training module.*	
Module type (mandatory field) *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	
Training Provider (mandatory field) *Name(s) of training providers.*	
Contact (mandatory field) *Name(s) of the main contact person and their email address.*	
Level (mandatory field) *Training level: B (Basic), A (Advanced)*	
Year – semester – exact dates offered (mandatory field) *Indicates the year / semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP project).*	
Duration (mandatory field) *Duration of the training.*	
Training method and provision (mandatory field)	

Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.	
Evaluation method(s) (mandatory field) *Indicates physical and/or virtual tests, participation, exercises, etc.*	
Module overview (mandatory field) *The topics that the training module covers.*	
Module description *Please note that this field will be defined later. More information will be provided with syllabus /.ppt/ video teaser, registration procedures, developed in WP3.*	TBA
Knowledge area(s) (mandatory field) *Mapping to the 10 selected CSP knowledge areas.* *1. Penetration Testing* *2. Cybersecurity Tools and Technologies* *3. Cybersecurity Management* *4. Cybersecurity Threat Management* *5. Cybersecurity Risk Management* *6. Cybersecurity Policy, Process, and Compliance* *7. Cyber Incident Response* *8. Network and Communication Security* *9. Privacy and Data Protection* *10. Human Aspects of Cybersecurity*	
Tools to be used (mandatory field) *A list of tools that will be used for the operation of this training module.*	
Language (mandatory field) *Indicates the spoken language and the language for the material and the assessment/evaluation.*	Spoken: Material: Assessment:
ECTS (optional field) *If applicable, the number of ECTS.*	
Certificate of Attendance (CoA) (optional field) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates (optional field) *Indicates the enrolment dates for the operation of this training module.*	
Other important dates (optional field) *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	

3 CSP Training Modules and Schedule

This chapter describes the path from the training modules as offered by the CSP partners to a grouping and schedule of a joint operation of CSP modules. Section 3.1 describes the origin, the training modules on the CSP knowledge areas per CSP provider. Section 3.2 offers a first analysis of these modules. Section 3.3 decribes the initial design of the CSP Programme by clustering the modules under the knowledge areas. Then Section **Error! Reference source not found.** offers the CSP training modules' catalogue and schedule. Section 3.5 concludes the chapter with evaluation templates.

3.1 Training Modules on the CSP Knowledge Areas per CSP Provider

This section includes the training modules the partners are willing to offer in the knowledge areas selected in the deliverable D2.3. All partners that will develop and offer training modules as part of the CSP programme, either individually or jointly with other partners, should provide their summarized schedule for each type of module using the general template in Section 2.2. The general template for the CSP training modules' catalogue will include the information needed from each one of the CSP partners (both HEIs and security companies).

3.1.1 JOHANN WOLFGANG GOETHE-UNIVERSITAET FRANKFURT AM MAIN (GUF), Germany

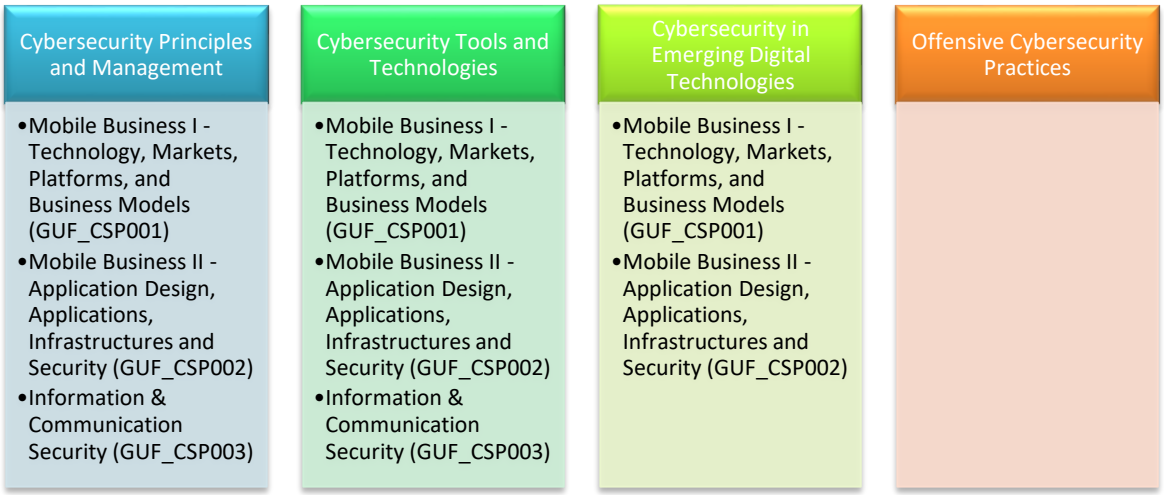

Figure 2. The full overview of GUF's training modules per CSP capability categories

Figure 2 presents the full overview of GUF's training modules per CSP capability categories. The following tables summarize the training modules that GUF is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	GUF_CSP001
Module name	Mobile Business I–Technology, Markets, Platforms, and Business Models
Module type	Course (C)
Training Provider	GUF
Contact	Kai Rannenberg, (kai.rannenberg@m-chair.de)

Level	A (Advanced)
Year – semester – exact dates offered	Semester: 1st - 4th
Duration	15 weeks, In average 3 hours per week (4 hours and 2 hours alternating)
Training method and provision	Physical (Germany, Goethe University Frankfurt)
Evaluation method(s)	Physical tests
Module overview	Mobile Business I cover the following topics: Starting with the basics of mobile communication services, emphasis will be put on an analysis of the interaction between individuals and mobile devices/services. This includes a historical overview of the development of mobile communication infrastructures, services, and protocols. Based on this, students will be qualified to identify the possibilities and limitations of mobile business applications and business models in order to consider the resulting opportunities and challenges when deriving the success factors. Characteristic attributes of mobile services, especially in contrast to electronic services, will be outlined and considered in an analysis of the current market environment for mobile business applications. Furthermore, traditional as well as emerging business models will be discussed. Architectures for mobile services and their development are the focus of the first part of the course Mobile Business 1. This includes topics such as security and privacy, usability, and the role of standardisation. The presentation of exemplary application areas will allow students to understand and question how different design aspects are considered in current scenarios. The course concludes with a state-of-the-art overview of current mobile business research topics and activities, enabling students to understand the lines of research and draw connections to already existing mobile business applications and scenarios. Students will be able to reflect on specific attributes of mobile applications, analyse new scenarios, and draw connections to traditional and established scenarios. The overall objective of the course is to provide advanced knowledge about mobile applications and mobile services, ranging from technical to economic aspects. Students will be qualified to realise the inherent commercial potential proactively and to identify and address challenges and problems in the area of mobile business. An important facet of this is the discussion of international regulation and its implications on the development and application scenarios for mobile services.
Module description	TBA
Knowledge area(s)	8. Network and Communication Security, 9. Privacy and Data Protection
Tools to be used	Visual (graphical) simulation of movement profiles in cellular mobile networks, https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html
Language	English
ECTS	6
Certificate of Attendance (CoA)	No
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	GUF_CSP002
Module name	Mobile Business II–Application Design, Applications, Infrastructures and Security
Module type	Course (C)
Training Provider	GUF
Contact	Kai Rannenberg, (kai.rannenberg@m-chair.de)

Level	A (Advanced)
Year – semester – exact dates offered	Semester: 1st - 4th
Duration	15 weeks, In average 3 hours per week (4 hours and 2 hours alternating)
Training method and provision	Physical (Germany, Goethe University Frankfurt)
Evaluation method(s)	Physical tests
Module overview	Mobile Business II focuses on the variety of opportunities and challenges that are offered by mobile communication technologies and their specific properties and which need to be considered and addressed by companies and regulators. The overall objective of the course is to provide advanced knowledge about mobile applications and mobile services, ranging from technical to economic aspects. Students will be qualified to realise the inherent commercial potential proactively and to identify and address challenges and problems in the area of mobile business. An important facet of this is the discussion of international regulation and its implications on the development and application scenarios for mobile services.
Module description	TBA
Knowledge area(s)	6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	Visual (graphical) simulation of movement profiles in cellular mobile networks, https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html
Language	English
ECTS	6
Certificate of Attendance (CoA)	No
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	GUF_CSP003
Module name	Information & Communication Security
Module type	Course (C)
Training Provider	GUF
Contact	Kai Rannenberg, (kai.rannenberg@m-chair.de)
Level	A (Advanced)
Year – semester – exact dates offered	Semester: 1st - 4th
Duration	15 weeks, In average 3 hours per week (4 hours and 2 hours alternating)
Training method and provision	Physical (Germany, Goethe University Frankfurt)
Evaluation method(s)	Physical tests
Module overview	The following contents are covered: Authentication, Access Control, Cryptography I, Cryptography II, Electronic Signatures, Identity Management, Privacy Protection I, Privacy Protection II, Computer System Security, Network Security I, Network Security II, Selected and varying contributions from (industry) guest speakers, e.g., Security Management and Biometrics.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management

	9. Privacy and Data Protection
Tools to be used	Visual (graphical) simulation of movement profiles in cellular mobile networks, https://interactive.zeit.de/opendata/widgets/vorratsdatenspeicherung/index.html
Language	English
ECTS	6
Certificate of Attendance (CoA)	No
Module enrolment dates	TBD
Other important dates	TBD

3.1.2 LAUREA-AMMATTIKORKEAKOULU OY (LAU), Finland

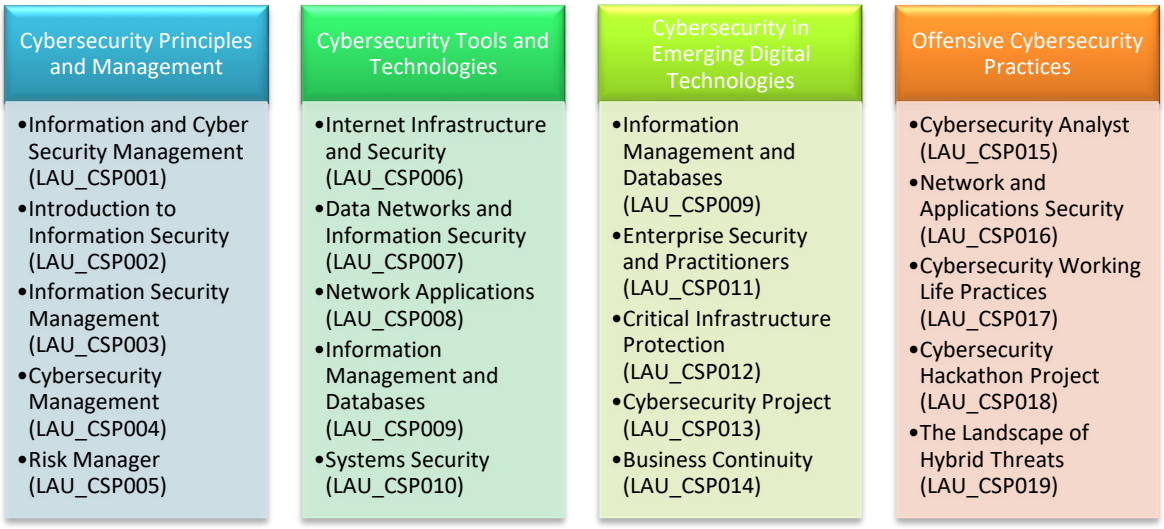

Figure 3. The full overview of LAU's training modules per CSP capability categories

Figure 3 presents the full overview of LAU's training modules per CSP capability categories. The following tables summarize the training modules that LAU is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	LAU_CSP001
Module name	Information and Cyber Security Management
Module type	C
Training Provider	LAU
Contact	Kaci Bourdache (kaci.bourdache@laurea.fi)
Level	A
Year – semester – exact dates offered	01.01.2024 - 31.07.2024
Duration	A full semester
Training method and provision	Both: Laurea Leppävaara campus, Vanha maantie 9, 02650 Espoo https://ops.laurea.fi/212701/fi/68153/206649/2497
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments

Module overview	- Requirements and best practices for information and cyber security - Information and cyber security risks management - Administrative, operational, technical and structural procedures - Information and cyber security planning, evaluation and development
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 10. Human Aspects of Cybersecurity
Tools to be used	
Language	English / Finnish
ECTS	10
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP002
Module name	Introduction to Information Security
Module type	C
Training Provider	LAU
Contact	Pasi Kämppi (Pasi.Kämppi@laurea.fi)
Level	B
Year – semester – exact dates offered	3rd semester 01.08.2024 - 31.12.2024
Duration	One full semester
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34034
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Act ethically as a member of study group and community - Recognize and comprehend the importance of confidentiality, integrity and availability model for the information and cybersecurity - Recognize and comprehend different threats, attacks and vulnerabilities - Comprehend and describe security technologies and tools - Comprehend and describe security architectures and designs - Comprehend and describe identity and access management approaches - Comprehend, describe and apply risk management principles - Comprehend and describe cryptography and PKI concepts - Differentiate cybersecurity domains and subdomains from each other - Comprehend and explain the importance of the cybersecurity in the modern society - Reflect and develop their own learning process
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Privacy and Data Protection 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity

Tools to be used	Embedded Linux Shell with iFrame (HTML based shell), PicoCTF (Catch the flag platform)
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP003
Module name	Information Security Management
Module type	C
Training Provider	LAU
Contact	Pasi Kämppi (pasi.kamppi@laurea.fi)
Level	B
Year – semester – exact dates offered	Two times per calendar year; spring and autumn semester. Planned for 3rd semester / 01.01.2024-31.07.2024
Duration	11 weeks
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34035
Evaluation method(s)	Multiple choice question tests, submittable assignments
Module overview	- Information security program, development and management principles - Risk management, incident management and compliance principles - Risk assessment process - Typical information security management related problems and draw solutions to them
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	Canvas LMS, Percipio LMS, Risk assessment sheet with Word or Excel, OSINT framework
Language	English
ECTS	5
Certificate of Attendance (CoA)	-
Module enrolment dates	Enrolment two times per calendar year; for spring and autumn semester. 22.05.2023 - 28.05.2023 - English 11.09.2023 - 17.09.2023 - English
Other important dates	Volunteer tutoring every two weeks.

Training Module fields	Training Module information
Code	LAU_CSP004
Module name	Cybersecurity Management
Module type	C

Training Provider	LAU
Contact	Anssi Mattila (anssi.m.mattila@laurea.fi)
Level	A
Year – semester – exact dates offered	01.01.2024 - 31.07.2024
Duration	9 weeks
Training method and provision	Virtual https://ops.laurea.fi/68096/fi/68153/69176/2536/0/26735?lang=en
Evaluation method(s)	Virtual tests and assignments, group discussion and reflection
Module overview	- Recognize and assess the significance and impact of cybersecurity on the operations of businesses and organizations. - Identify and evaluate critical threats and risks targeting the information networks of businesses and organizations. - Enhance the organization's information security as well as risk and continuity management.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	Canvas LMS, Percipio
Language	Finnish
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP005
Module name	Risk Manager
Module type	C, W
Training Provider	LAU
Contact	Soili Martikainen (Soili.Martikainen@laurea.fi)
Level	A
Year – semester – exact dates offered	Two times per calendar year; spring and autumn semester. 19.09.2023 - 04.12.2023
Duration	One full semester
Training method and provision	Both: Laurea Leppävaara campus, Vanha maantie 9, 02650 Espoo https://www.laurea.fi/koulutus/taydennyskoulutukset/risk-manager--koulutus/
Evaluation method(s)	Multiple choice questions, submittable assignments, proctored exam for certification
Module overview	- Threat identification - Security of information systems - Standards
Module description	TBA
Knowledge area(s)	All
Tools to be used	Canvas LMS, Percipio
Language	Spoke: Finnish

	Materials: Finnish & English Assessment: Finnish & English
ECTS	5
Certificate of Attendance (CoA)	Proctored exam for certification
Module enrolment dates	Enrolment two times per calendar year; for spring and autumn semester. September 4 2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP006
Module name	Internet Infrastructure and Security
Module type	C
Training Provider	LAU
Contact	Seppo Koponen (Seppo.Koponen@laurea.fi)
Level	B
Year – semester – exact dates offered	3rd semester 01.08.2024 - 31.12.2024
Duration	A full semester
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34032
Evaluation method(s)	Virtual tests, bonus tasks, assignments
Module overview	- Comprehension and description of the operations and protocols in global IP networks - Calculation of IP subnets and supernets - Comprehension and description of security vulnerabilities in IP network infrastructure - Comparison and contrasting of IPv6 to IPv4 - Comprehension and description of the functional concepts and security risks in wireless networking - Comprehension and description of the functional concepts and security risks in cloud computing
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	Canvas LMS, Percipio, Cisco Packet Tracer
Language	English
ECTS	10
Certificate of Attendance (CoA)	-
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP007
Module name	Data Networks and Information Security
Module type	C

Training Provider	LAU
Contact	Seppo Koponen (Seppo.Koponen@laurea.fi)
Level	B
Year – semester – exact dates offered	2nd semester / 01.01.2024-31.07.2024
Duration	Full semester
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/27157
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Description of the structure and operation of data networks in relation to the following terms: Local area networks, wireless networks, internet - Description of the functionality of IP-networks and key internet protocols - Implementation and maintenance of basic services in a local area network o Justification of the importance of information security according to the CIA model (Confidentiality, Integrity and Availability) o Identification of common information security threats faced by organisations - Implementation of basic level information security safeguards for local area network
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	Hands-on TCP/IP Level Network Practice, Canvas LMS, Percipio
Language	English / Finnish
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP008
Module name	Network Applications
Module type	C
Training Provider	LAU
Contact	Seppo Koponen (Seppo.Koponen@laurea.fi)
Level	B
Year – semester – exact dates offered	2nd semester 01.08.2024 - 31.12.2024
Duration	A full semester
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/26590
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Design and implementation of web sites using fundamental web development tools and techniques - Design, create, and publish www content - Design and implement web site layouts according to customer needs - Evaluate web site development needs
Module description	TBA

Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	Canvas LMS, Percipio
Language	English / Finnish
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP009
Module name	Information Management and Databases
Module type	C
Training Provider	LAU
Contact	Outi Grotenfelt (Outi.Grotenfelt@laurea.fi)
Level	B
Year – semester – exact dates offered	1st semester / 01.01.2024-31.07.2024
Duration	Full semester
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/27156
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Design and implementation of databases - Management and usage of databases - Query languages to search and modify data in a database
Module description	TBA
Knowledge area(s)	9. Privacy and Data Protection
Tools to be used	Canvas LMS, Percipio, SQL
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP010
Module name	Systems Security
Module type	C
Training Provider	LAU
Contact	Paresh Rathod (paresh.rathod@laurea.fi)
Level	B
Year – semester – exact dates offered	4th / 5th semester 01.01.2024 - 31.07.2024

Duration	5 months (full semester)
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34040
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- - Threats, vulnerabilities and risks associated with organisation's systems - - Confidentiality, integrity and availability model for the information and cybersecurity in practice - - Differences regarding different cryptographic methods, its applications and techniques - - Risk assessment, risk analysis and risk management - - Security controls for workstation and server environments - - Authentication and authorization mechanisms This module will enable participants learn the knowledge and competencies concerning designing, implementing, and managing secure information systems. The knowledge and competencies gained in this module that are equivalent to the topics of Certified Information Systems Security Professional (CISSP) by acquiring the knowledge to design, implement, and manage secure information systems. It is an advanced level professional study unit within Laurea Cybersecurity Education and Professional Training offerings.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection
Tools to be used	Virtual Practice Labs Environment for CISSP KAs (proprietary third-party environment)
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP011
Module name	Enterprise Security and Practitioners
Module type	C
Training Provider	LAU
Contact	Paresh Rathod (paresh.rathod@laurea.fi)
Level	A
Year – semester – exact dates offered	4th and 5th semester / 01.01.2024-31.07.2024
Duration	5 months (a full semester)
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34036
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Identification of threats, vulnerability and risks associated with web applications and web servers

	- Common attack tactics, techniques used when hacking web servers, applications and wireless networks - Security controls for information systems against common threats - Hacking exercises in virtualized training environment This module provides trainees with advanced-level cybersecurity skills for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness. It enables trainees to gain knowledge and competencies equivalent to the topics of CompTIA Advanced Security Practitioner (CASP+) professional certifications. It is an advanced level professional study unit within Laurea Cybersecurity Education and Professional Training offerings.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 7. Cyber Incident Response 10. Human Aspects of Cybersecurity
Tools to be used	Virtual Practice Labs Environment for CASP KAs (proprietary third-party environment), Canvas LMS, Percipio,
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP012
Module name	Critical Infrastructure Protection
Module type	C
Training Provider	LAU
Contact	Veli Sulkava (veli.sulkava@laurea.fi) Timo Ryynänen (timo.ryynänen@laurea.fi)
Level	B
Year – semester – exact dates offered	4th/5th Semester 01.08.2024 - 31.12.2024
Duration	One full semester
Training method and provision	Both https://ops.laurea.fi/212701/en/68153/206648/2743/0/32105
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- define critical infrastructure operators and their roles - define critical infrastructure protection compliance requirements, best practices and apply those - assess and manage critical infrastructure's risks - plan, assess and develop critical infrastructure risks
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 10. Human Aspects of Cybersecurity
Tools to be used	Canvas LMS, Percipio

Language	Finnish / English
ECTS	10
Certificate of Attendance (CoA)	No
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP013
Module name	Cybersecurity Project
Module type	C
Training Provider	LAU
Contact	Jyri Rajamäki (jyri.rajamaki@laurea.fi)
Level	A
Year – semester – exact dates offered	Planned for 4th / 5th semester Two times per calendar year; spring and autumn semester. 01.01.2024 - 31.07.2024
Duration	16 weeks
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34078
Evaluation method(s)	Reports and on-line presentations
Module overview	- Working as a member cybersecurity analyst team (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defence projects) - Ethical actions as a member of team, community and working-life partners - Planning, implementation and documentation of a cybersecurity research project - Frameworks and methods for cybersecurity research project - Presenting research results in the academic and business format Cybersecurity professional practices and applying practitioners' skills in the community Module 1: Introduction to the topic and forming of research teams Module 2: Determination of the RDI problem Module 3: Project idea focusing and project plan Module 4: Project work Module 5: Project results presentation Module 6: Project finalising
Module description	TBA
Knowledge area(s)	All
Tools to be used	Canvas LMS, Teams, Zoom, PowerPoint
Language	English / Finnish
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	27.11.2023 - 03.12.2023 20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP014
Module name	Business Continuity
Module type	C
Training Provider	LAU
Contact	Eveliina Hytönen (eveliina.hytönen@laurea.fi)
Level	B
Year – semester – exact dates offered	01.05.2024 - 31.08.2024 01.08.2024 - 31.12.2024
Duration	One full semester
Training method and provision	Both https://ops.laurea.fi/212701/en/68153/206648/2743/0/32109
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	The unit will include the following topics: Managing Risks, Business Impact, BCP Process and Systems, Security of Supply. After completing the unit, the student is able to: • define business continuity compliance requirements, best practices and apply those • identify critical business operations and their needs for business continuity • assess and manage business continuity risks • plan, assess and develop business continuity
Module description	TBA
Knowledge area(s)	6. Cybersecurity Policy, Process, and Compliance 7. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	Canvas LMS, Percipio
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	01.04.2024 - 07.04.2024 20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP015
Module name	Cybersecurity Analyst
Module type	C
Training Provider	LAU
Contact	Paresh Rathod (paresh.rathod@laurea.fi)
Level	A
Year – semester – exact dates offered	4th / 5th semester 01.08.2024 - 31.12.2024
Duration	5 months (full semester)
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34037

Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Network discovery, reconnaissance, harvesting and vulnerability analysis techniques - Tools for network discovery reconnaissance, harvesting and vulnerability analysis - Network vulnerabilities with network discovery, reconnaissance, harvesting and analysing tools - Reducing the attack surface of a network host - Presenting the results of network reconnaissance and vulnerability analysis in professional format
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management
Tools to be used	Virtual Practice Labs Environment for CySA+ KAs (proprietary third-party environment)
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP016
Module name	Network and Application Security
Module type	C
Training Provider	LAU
Contact	Paresh Rathod (paresh.rathod@laurea.fi)
Level	A
Year – semester – exact dates offered	4th / 5th semester 01.08.2024 - 31.12.2024
Duration	5 months (full semester)
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34039
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- The role of ethical hacking in the offensive and defensive network and applications security - Penetration testing processes including footprinting, reconnaissance, scanning networks, enumeration, vulnerability analysis and system hacking - Tools and techniques used in penetration testing process - Security controls to network security based on vulnerability analysis - Common penetration testing tools in virtualized training environment This module primarily provides Ethical Hacker hands-on scenarios to enable trainees to learn offensive and defensive security in the ICT network and applications environment. The Network and Applications Security's learning objectives and outcomes are mapped with the majority of Certified Ethical Hacker (CEHv11) domains.
Module description	TBA

Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies
Tools to be used	Virtual Practice Labs Environment for CISSP KAs (proprietary third-party environment)
Language	English
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

Training Module fields	Training Module information
Code	LAU_CSP017
Module name	Cybersecurity Working Life Practices
Module type	C, W, CS-E
Training Provider	LAU
Contact	Pasi Kämppi (pasi.kamppi@laurea.fi)
Level	A
Year – semester – exact dates offered	Two times per calendar year; spring and autumn semester. Planned 4th / 5th semester 01.08.2024 - 31.12.2024
Duration	9 weeks
Training method and provision	Both: Laurea Leppävaara campus, Vanha maantie 9, 02650 Espoo https://ops.laurea.fi/212701/en/69076/230740/2521/0/34043
Evaluation method(s)	Multiple choice question tests, submittable assignments, CTF score
Module overview	- Cybersecurity professional working life events including industrial visits, seminars, workshops, hands-on, cyber ranges, cyber drill and cyber defense activities - Ethical actions as a member of team, community and working-life partners - Networking with other cybersecurity professionals - Cybersecurity professional practices and applying practitioners skills in the community
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 10. Human Aspects of Cybersecurity
Tools to be used	Canvas LMS, Azure virtual machine (Splunk), Splunk with BOTSv3, Google dork sheets, Google dork sheets, Shodan, DNS Dumbster, OpintelLinks, Exploit Database, Dorksearch, Investigator, Similarweb, Builtwith, Virustotal, Reallygoodemails
Language	English
ECTS	2
Certificate of Attendance (CoA)	-
Module enrolment dates	Enrolment two times per calendar year; for spring and autumn semester. 20.05.2024 - 26.05.2024
Other important dates	Volunteer tutoring every two weeks.

Training Module fields	Training Module information
Code	LAU_CSP018
Module name	Cybersecurity Hackathon Project
Module type	C, W, CS-E
Training Provider	LAU
Contact	Pasi Kämppi (pasi.kamppi@laurea.fi)
Level	A
Year – semester – exact dates offered	Two times per calendar year; spring and autumn semester. Planned for 4th / 5th semester 21.08.2023 - 05.11.2023
Duration	10 weeks
Training method and provision	Virtual https://ops.laurea.fi/212701/en/69076/230740/2521/0/34042
Evaluation method(s)	Multiple choice question tests, submittable assignments, workshop presentation
Module overview	- Working as a member cybersecurity analyst team (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defence projects) - Participating and acting ethically as a member of team, community and working-life partners - Selecting appropriate tools and strategies for network reconnaissance and vulnerability analysis project in real exercise or company environment - Presentation of the results of network reconnaissance and vulnerability analysis in a professional format - Critical analysis of the project outcomes
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	Canvas LMS, VirtualBox, UTM Virtualization (Mac), Kali Linux, Azure virtual machine (target), Nessus, Burpsuite, Nmap, Sqlmap, OWASP ZAP, OWASP Websccarab, Hydra, Drupageddon2, Metasploits, Social engineering tookit, Curl, Nikto, Gobuster, WP Zoom, Hascat, Wireshark, Dirb, John the Ripper, Dirbuster, Ncrack, Metagoofil, Wappalyzer, Wfuzz, XSStrike, XSS Hunter, WhatWeb
Language	English
ECTS	2
Certificate of Attendance (CoA)	-
Module enrolment dates	Enrolment two times per calendar year; for spring and autumn semester 22.05.2023 - 28.05.2023
Other important dates	Volunteer tutoring every two weeks.

Training Module fields	Training Module information
Code	LAU_CSP019
Module name	The Landscape of Hybrid Threats
Module type	C

Training Provider	LAU
Contact	Pasi Kämppi (Pasi.Kämppi@laurea.fi)
Level	B
Year – semester – exact dates offered	1st semester 18.09.2023-10.12.2023
Duration	One full semester
Training method and provision	Virtual https://canvas.laurea.fi/courses/8167
Evaluation method(s)	Virtual tests, participation, bonus tasks, assignments
Module overview	- Take sole responsibility for working as a member cybersecurity analyst team (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defense projects) - Participate and act ethically as a member of team, community and working-life partners - Select appropriate tools and strategies for network reconnaissance and vulnerability analysis project in real exercise or company environment - Present the results of network reconnaissance and vulnerability analysis in a professional format - Analyze critically the outcome of the project - Manifest cybersecurity professional practices and apply practitioners skills in the communityComprehend and describe cryptography and PKI concepts - Differentiate cybersecurity domains and subdomains from each other - Comprehend and explain the importance of the cybersecurity in the modern society - Reflect and develop their own learning process
Module description	TBA
Knowledge area(s)	1. Penetration Testing 4. Cybersecurity Threat Management 7. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	Embedded Linux Shell with iFrame (HTML based shell), PicoCTF (Catch the flag platform), Canvas LMS, Percipio
Language	English
ECTS	5
Certificate of Attendance (CoA)	-
Module enrolment dates	20.05.2024 - 26.05.2024
Other important dates	

3.1.3 TALLINNA TEHNIKAÜLIKOOL (TalTech), Estonia

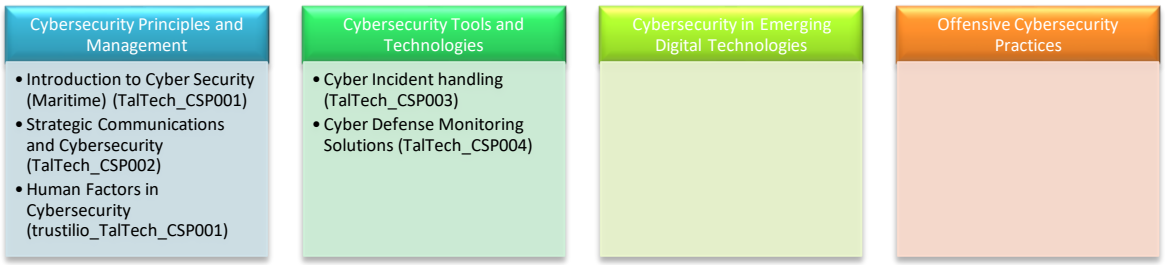

Figure 4. The full overview of TalTech's training modules per CSP capability categories

Figure 4 presents the full overview of TalTech's training modules per CSP capability categories. The following tables summarize the training modules that TalTech is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	TalTech_CSP001
Module name	Introduction to Cyber Security (Maritime)
Module type	Course
Training Provider	TalTech
Contact	Dan.Heering@taltech.ee
Level	Basic
Year – semester – exact dates offered	Autumn and Spring
Duration	15 weeks (weekly lectures)
Training method and provision	Both
Evaluation method(s)	Physical tests, participation, exercises Final assessment: Pass/fail
Module overview	The aim of the course is to provide the overview of main aspects of cyber security and provide the knowledge and skills to mitigate the cyber risks on ships. The student: - understands the concept of the security; - understands the terminology of cyber security; - understands the main cyber risks and threats to ships and organisations; - is familiar with the cyber security guidelines developed for maritime sector; - understands the main threats to information society, the main courses and outcomes of the problems in information security; - is able to employ best practices of cyber hygiene and can also explain them to others; - understands the ethical aspects of cyber security.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management

	6. Cybersecurity Policy, Process, and Compliance 10. Human Aspects of Cybersecurity
Tools to be used	
Language	English, Estonian
ECTS	6
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	TalTech_CSP002
Module name	Strategic Communications and Cybersecurity
Module type	Course
Training Provider	TalTech
Contact	adrian.venables@taltech.ee
Level	Advanced
Year – semester – exact dates offered	Spring
Duration	15 weeks (weekly lectures)
Training method and provision	Physical
Evaluation method(s)	Physical tests, participation, exercises Final assessment: graded assessment
Module overview	This course aims to provide students with a wider contextualisation of the role of cybersecurity in the information environment and how it contributes to a nation's Strategic Communications strategy. The general objective of the course is to provide a broader understanding of how students' technical knowledge and skills can contribute to the production of cyber security strategy and policy. By the end of the course the student will: - understand and explain the nature of cyberspace beyond that of a purely technical description; - understand the concept on Strategic Communication and Information Operation, is familiar with different Influence Activities and is able to discuss in their related disciplines; - is able to analyse and explain the role of strategy, policy, processes and procedures in achieving national objectives in the information environment; - understand and describe the nature of hybrid warfare and asymmetric operations in the _grey zone_ of conflict; - understand how the behaviour of target audiences are influenced through the use of strategic communication, and understand the role of cyber security in facilitating or denying those activities
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 10. Human Aspects of Cybersecurity
Tools to be used	
Language	English
ECTS	6

Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	TalTech_CSP003
Module name	Cyber Incident handling
Module type	Course
Training Provider	TalTech
Contact	Rain.Ottis@taltech.ee
Level	Advanced
Year – semester – exact dates offered	Autumn - Spring
Duration	15 weeks (weekly lectures)
Training method and provision	Both
Evaluation method(s)	Physical tests, participation, exercises Final assessment: graded assessment
Module overview	The aim of this course is to give the student foundational knowledge required to work in a security operation center (SOC) and participate in cyber incident response. • Triage and basic incident handling • Creating incident handling procedures and testing • Large scale incident handling • Cooperation with Law Enforcement agencies • Identifying and handling cyber-crime traces • Incident handling and cooperation during phishing campaign • Law enforcement view of computer security incidents • Law enforcement needs for evidence analysis • Role of (tabletop) exercises in developing incident handling capability After completing this course, the student: - is able to establish incident handling team and typical team designs; - manages cyber incidents, preserving needed evidence and chain of evidence; - builds incident management system and manages cooperation between law enforcement and incident handlers; - establishes procedures for evidence and incident management
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 7. Privacy and Data Protection
Tools to be used	
Language	English
ECTS	6
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	TalTech_CSP004
Module name	Cyber Defense Monitoring Solutions
Module type	Course
Training Provider	TalTech
Contact	Risto.Vaarandi@taltech.ee
Level	Advanced
Year – semester – exact dates offered	Autumn
Duration	15 weeks (weekly lectures)
Training method and provision	Both
Evaluation method(s)	Physical tests, participation, exercises Final assessment: individual work, examination
Module overview	The aims of course is to give an overview of monitoring techniques and solutions in cyber defense The following topics will be covered: - Main monitoring solutions and techniques in cyber defense, - Log and event generation for firewalls, IDS/IPS sensors, services, and applications, - Collecting and monitoring logs and events, - Intrusion detection and prevention. On completion of the course the student: • has an overview of the principles and standards of log collecting (BSD and IETF syslog) • can tune the UNIX logging software syslogd, rsyslog ja syslog-ng • is able to filter the network packets and generate log messages using netfilter firewall • knows different dialects of the regular expression languages (ERE, Perl) and is able to use these in the log monitoring • has an overview of the event correlation principles • is able to correlate events using Simple Event Correlator and use it for discovering and responding to attacks using different correlation techniques • has an overview of the network-based intrusion detection and prevention systems (network IDS/IPS) • is able to use Snort for intrusion detection and prevention
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies
Tools to be used	
Language	English
ECTS	6
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	Trustilio_TalTech_CSP001
Module name	Human Factors in Cybersecurity
Module type	´Seminar
Training Provider	Trustilio jointly with TalTech
Contact	Kitty Kioskli (kitty.kioskli@trustilio.com) Ricardo Gregorio Lugo (ricardo.lugo@taltech.ee)
Level	Basic
Year – semester – exact dates offered	01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Virtual
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The seminar on Human Factors in Cybersecurity offers a comprehensive exploration of the intricate relationship between human cognitive and behavioral dynamics and the realm of cybersecurity. This seminar provides an in-depth analysis of the psychological, sociological, and cognitive factors that underpin individuals' interactions with digital systems, and subsequently shape the efficacy of cybersecurity protocols. Through a meticulous examination of empirical research and pertinent case studies, attendees will scrutinize the psychological mechanisms that underlie susceptibility to phishing attacks, the challenges posed by user authentication processes, and the cognitive decision-making paradigms during cyber incidents. By fostering a nuanced comprehension of human factors, participants will acquire the expertise necessary to engineer user-centric interfaces, formulate targeted training regimens, and deploy strategies tailored to enhance user compliance and overall cybersecurity robustness. The seminar offers a platform to navigate the intricate terrain of human-centric cybersecurity, contributing to the fortification of the digital domain.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

3.1.4 TECHNISCHE UNIVERSITAET BRAUNSCHWEIG (TUBS), Germany

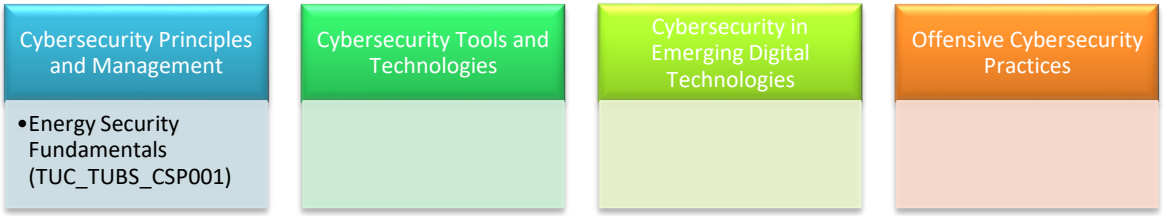

Figure 5. The full overview of TUBS's training modules per CSP capability categories

Figure 5 presents the full overview of TUC's training modules per CSP capability categories. The following table summarizes the training module that TUC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	TUC_TUBS_CSP001
Module name	Energy Security Fundamentals
Module type	Seminar (S)
Training Provider	TUC (jointly with TUBS)
Contact	Pinelopi Kyranoudi (pkyranoudi@tuc.gr) Charalampos-Ioannis Mitropoulos (cmitropoulos@tuc.gr) Manos Athanatos (mathanatos@tuc.gr)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Virtual and/or Physical Link: TBD
Evaluation method(s)	Virtual and/or physical participation
Module overview	• Energy and cyber-physical security principles • Networks and architectures • Threats, vulnerabilities, and possible attacks • Known energy security incidents • Ways of protection • EU action
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Openstack with VMs for Demo, Kali Linux/Other Debian-Arch based distributions targeted for Security, Wireshark.Tools delivered with the aforementioned distributions. Other tools: ELITEWOLF(GIHUB REPOSITORY), ICS-Security-Tools (GITHUB REPOSITORY)
Language	English

ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	-

3.1.5 POLYTECHNEIO KRITIS (TUC), Greece

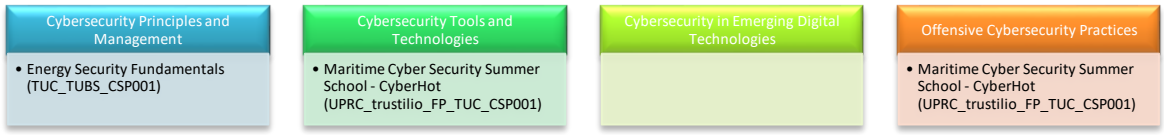

Figure 6. The full overview of TUC's training modules per CSP capability categories

Figure 6 presents the full overview of TUC's training modules per CSP capability categories. The following tables summarize the training modules that TUC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	TUC_TUBS_CSP001
Module name	Energy Security Fundamentals
Module type	Seminar (S)
Training Provider	TUC (jointly with TUBS)
Contact	Pinelopi Kyranoudi (pkyranoudi@tuc.gr) Charalampos-Ioannis Mitropoulos (cmitropoulos@tuc.gr) Manos Athanatos (mathanatos@tuc.gr)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Virtual and/or Physical Link: TBD
Evaluation method(s)	Virtual and/or physical participation
Module overview	• Energy and cyber-physical security principles • Networks and architectures • Threats, vulnerabilities, and possible attacks • Known energy security incidents • Ways of protection • EU action
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security

Tools to be used	Openstack with VMs for Demo, Kali Linux/Other Debian-Arch based distributions targeted for Security, Wireshark.Tools delivered with the aforementioned distributions. Other tools: ELITEWOLF(GIHUB REPOSITORY), ICS-Security-Tools (GITHUB REPOSITORY)
Language	EN
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UPRC_trustilio_FP_TUC_CSP001
Module name	Maritime Cyber Security Summer School - CyberHot
Module type	Summer School (SS)
Training Provider	UPRC jointly with trustilio, Focal Point, TUC
Contact	Despoina Polemi (dpolemi@gmail.com)
Level	A (Advanced)
Year – semester – exact dates offered	(Summer) 01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Physical
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The "Maritime Cyber Security Summer School - CyberHot" is an immersive and intensive program designed to equip participants with essential knowledge and practical skills in safeguarding maritime systems and infrastructure against cyber threats. Throughout this comprehensive seminar, trainees will delve into the intricate realm of maritime cyber security, exploring the diverse spectrum of threats and attacks that can potentially compromise the safety and functionality of ships and ports. Through hands-on training, participants will learn to identify vulnerabilities, assess risks, and implement mitigation actions, ensuring the resilience of maritime operations in an increasingly digitalized world. Additionally, the program will provide a thorough examination of the legal, standards, and regulatory frameworks governing the maritime industry, enabling trainees to navigate compliance challenges and foster a secure and compliant maritime cyber ecosystem. By the end of the seminar, participants will emerge with practical skills and a deep understanding of cyber security tailored specifically to the maritime domain, positioning them as capable guardians of maritime cyber infrastructure.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes

Module enrolment dates	N/A
Other important dates	N/A

3.1.6 UNIVERSITY OF CYPRUS (UCY), Cyprus

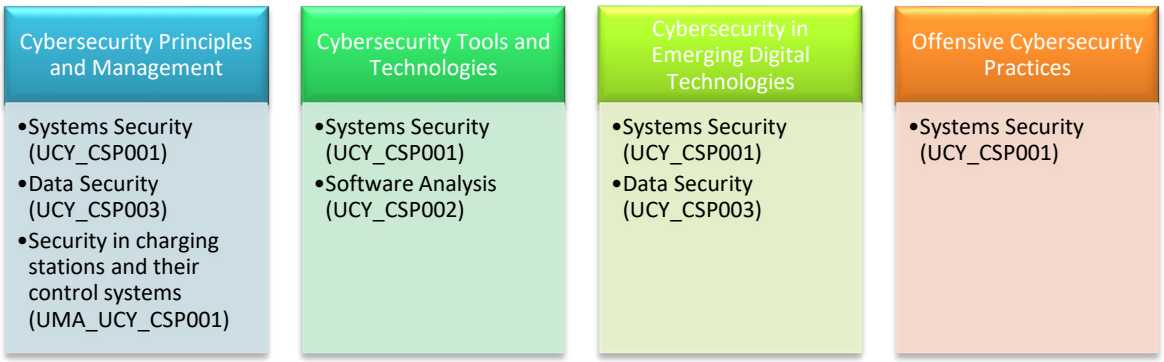

Figure 7. The full overview of UCY's training modules per CSP capability categories

Figure 7 presents the full overview of UCY's training modules per CSP capability categories. The following tables summarize the training modules that UCY is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	UCY_CSP001
Module name	Systems Security
Module type	C
Training Provider	UCY
Contact	Elias Athanasopoulos (athanasopoulos.elias@ucy.ac.cy)
Level	B
Year – semester – exact dates offered	Spring semester, University of Cyprus
Duration	13 weeks
Training method and provision	Physical
Evaluation method(s)	Homework, midterm exam, final exam
Module overview	Introduction to applied cryptography (symmetric, asymmetric, and stream ciphers, cryptographic hash functions, cryptographic protocols) and security models (CIA). Software vulnerabilities and memory errors (buffer overflows, integer overflows, use-after-free, dangling pointers). Attacks (code injection, code reuse). Defenses (non-executable pages, stack canaries, code randomi-zation, CFI, SFI, side channels). Mobile security (Android iOS). Web security (cross-site script-ing, CSRF, clickjacking, phishing). Network security (botnets, DDoS, spam, security economics). Privacy and anonymity (TOR).
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	OpenSSL, gdb

Language	Spoken: Greek Material: English Assessment: Greek/English
ECTS	7.5
Certificate of Attendance (CoA)	No
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UCY_CSP002
Module name	Software Analysis
Module type	C
Training Provider	UCY
Contact	Elias Athanasopoulos (athanasopoulos.elias@ucy.ac.cy)
Level	A
Year – semester – exact dates offered	Spring semester, University of Cyprus
Duration	13 weeks
Training method and provision	Physical
Evaluation method(s)	Homework, midterm exam, final exam
Module overview	ELF format of Unix binaries. Tools that can work and explore binaries in Unix (show different sections, symbols, shared libraries, etc.). How relocations and shared libraries work in binaries (e.g., the usage of GOT). Using ptrace(). Disassembling binaries using the Capstone framework. Re-writing binaries programmatically. Pre-loading binaries. Dynamic and static analysis of binary code. C/C++ instrumentation through LLVM passes. Applications of software analysis.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies
Tools to be used	binutils/libbfd, readelf/libelf, strace, gdb, Clang/Clang++, LLVM, Pintool, Z3 solver
Language	Spoken: Greek or English Material: English Assessment: Greek/English
ECTS	7.5
Certificate of Attendance (CoA)	No
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UCY_CSP003
Module name	Data Security
Module type	C
Training Provider	UCY

Contact	Elias Athanasopoulos (athanasopoulos.elias@ucy.ac.cy)
Level	A
Year – semester – exact dates offered	Spring semester, University of Cyprus
Duration	13 weeks
Training method and provision	Physical
Evaluation method(s)	Project, final exam
Module overview	Applied cryptography concepts (AES, RSA, Elliptic Curves, SHA256/SHA3, MACs). Building applications with data encryption (OpenSSL). Transport Layer Security (TLS) and attacks. Attacks for exfiltrating data from systems and possible defenses (oblivious memory, differential privacy, k-anonymity). ML-based attacks (adversarial input generation, membership inference attack) and defenses.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	No tools
Language	Spoken: Greek or English Material: English Assessment: Greek/English
ECTS	8
Certificate of Attendance (CoA)	No
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UMA_UCY_CSP001
Module name	Security in charging stations and their control systems
Module type	Seminar (S)
Training Provider	UCY (jointly with UMA)
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	B (Basic)
Year – semester – exact dates offered	Summer / annually
Duration	2h
Training method and provision	Virtual
Evaluation method(s)	Virtual tests and activities
Module overview	Cyber-physical systems integrated as part of electric vehicle charging infrastructures are mainly composed of software components and specific communication protocols. This makes them particularly susceptible to threats that may abuse the network protocol's implementation or software errors for exploiting a target system. The seminar therefore offers an overview of basic principles and management of security in charging infrastructure control systems.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management

Tools to be used	TBD
Language	English (spoken, material, evaluation)
ECTS	Not applicable
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	-

3.1.7 UNIVERSIDAD DE MALAGA (UMA), Spain

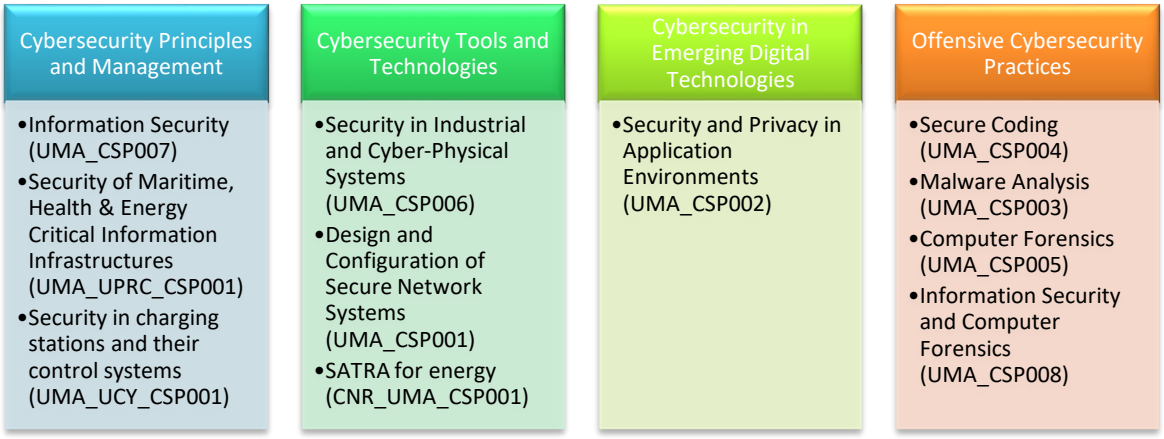

Figure 8. The full overview of UMA's training modules per CSP capability categories.

Figure 8 presents the full overview of UMA's training modules per CSP capability categories. The following paragraphs summarize the training modules that UMA is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	UMA_CSP001
Module name	Design and Configuration of Secure Network Systems
Module type	Course (C)
Training Provider	UMA
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	1st semester / approximately September to January / annually
Duration	Approximately 3-4 months; 3 hours per week.
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Physical exams
Module overview	This course aims to introduce advanced cybersecurity principles and management in terms of network security and hardening. To this end, it includes an in-depth understanding of cyber-attacks at different network levels, as well as the security requirements needed to mitigate these cyber-attacks and the countermeasures to be taken to strengthen network systems. In addition, all this knowledge will enable learners to design secure networks and learn to make decisions on how to configure secure network systems at a higher level, as well as to identify vulnerabilities in operating systems and learn the main features of systems for comprehensive security management in large-scale networks.

Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	GNS3, SCP, Putty, Etherape, Nmap, Hping3 / nping, Legion, Etthercap / ARPSpoof, Yersinia, Scpay, Netstat, OPenVPN, OpenSSL, XCA, Metasploitable 2, Snort, Snorpy, IPTables, OpenVAS / Nessus, Kali Linux / Parrot. Please note that this list may change from course to course.
Language	Spanish (spoken), English (material, evaluation)
ECTS	6
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP002
Module name	Security and Privacy in Application Environments
Module type	Course (C)
Training Provider	UMA
Contact	Ruben Rios (ruben.rdp@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	2nd semester / approximately February to June / annually
Duration	Approximately 3-4 months; 3 hours per week
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Group laboratory assignments
Module overview	This course provides an overview of security and privacy problems and solutions in different application scenarios, including the Internet of Things, Cloud Computing and the World Wide Web. The course is based on lectures that present students with the problems arising in the aforementioned scenarios. After the lectures, the students are provided with laboratory assignments where they must work in groups to devise and implement solutions to these problems.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	Python cryptography library, Google Cloud KMS, Amazon KMS, ARX, OWASP OWASP Secure Headers Project, OWASP Vulnerable Web Applications, OWASP Zap, Github repositories
Language	Spanish, English, and English/Spanish, respectively
ECTS	4.5
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP003
Module name	Malware Analysis
Module type	Course (C)
Training Provider	UMA
Contact	Jose A. Onieva (onieva@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	1st semester / approximately September to January / annually
YDuration	Approximately 3-4 months; 3 hours per week.
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Lab exercises, participation and virtual tests
Module overview	This course aims to introduce basic and advanced cybersecurity techniques in order to analyze malware samples. To that end, the student will learn the main techniques used by malware to exploit OS vulnerabilities and misconfiguration. Techniques like persistence and process injection will show the students how the malware behaves when running and different tools allow them to learn how to spot such malware techniques.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 7. Cyber Incident Response
Tools to be used	REMNUX toolset**,** VirtualBox, IDA Pro Educational, Wireshark, Regshot, PEStudio, CFF Explorer, Process Explorer, Autoruns, ProcMon
Language	Spanish (spoken), English (material, evaluation)
ECTS	4.5
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP004
Module name	Secure Coding
Module type	Course (C)
Training Provider	UMA
Contact	José A. Montenegro Montes (jmmontes@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	1st semester / approximately September to January / annually
Duration	Approximately 3-4 months; 3 hours per week
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Presentations of work or practices
Module overview	This course covers the principles and practices of secure programming. We will expose security models, threats, design principles and secure coding practices. A developer with the proper knowledge of these techniques will minimize vulnerabilities in the software, avoiding that the developed software can be vulnerable and exposed to possible attacks. For the

	development of the subject from the theoretical and practical point of view we will take into account the most representative platforms, from traditional platforms to mobile devices, including web platforms. To make the student aware of the dimension of the problem, we have added a module dealing with vulnerabilities in Machine Learning.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 10. Human Aspects of Cybersecurity
Tools to be used	Gdb, Immunity Debugger, Visual C, Cppcheck, Sonarqube, OWASP ZAP, Drozer y Sieve, Python, Jupiter.
Language	English, Spanish, and English/Spanish, respectively.
ECTS	4.5
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP005
Module name	Computer Forensics
Module type	Course (C)
Training Provider	UMA
Contact	Rodrigo Román (rroman@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	3rd semester / approximately September to January / annually
Duration	Approximately 3-4 months; 3 hours per week.
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Physical exams
Module overview	During this course, the student will acquire the technical skills to carry out computer forensic analysis and those methodologies that are fundamental for the successful training of a forensic computer practitioner. In particular, the course covers in a horizontal manner the different phases of identifying, obtaining, analysing and presenting electronic evidence.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management
Tools to be used	FTK Imager, Autopsy, John the Ripper, ExifTool, OpenPuff, Veracrypt.
Language	Spanish (spoken), English (material, evaluation).
ECTS	4.5
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP006
Module name	Security in Industrial and Cyber-Physical Systems

Module type	Course (C)
Training Provider	UMA
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	A (Advanced)
Year – semester – exact dates offered	3rd semester / approximately September to January / annually
Duration	Approximately 3-4 months; 3 hours per week
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Physical exams
Module overview	This course is focused on the security and privacy issues related to the deployment of Cyber-physical Systems, including their secure interactions with related technologies, such as the (Industrial) Internet of Things and Cloud Computing, and their secure integration with Smart Infrastructures. Therefore, the main goal of this course is to offer the necessary knowledge and tools to analyze, select, develop, deploy, and evaluate security solutions in these heterogeneous and complex ecosystems.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	GNS3, ESP32 (Arduino), Raspberry Pi, Nmap, Hping3 / nping, Etthercap / ARPSpoof, Scapy, Wireshark (for ModbusTCP, OPC-UA), OpenVPN, Python (pycryptodome), XCA, Anomaly-based IDS (Machine-Learning), Snort/Suricata, among others.
Language	Spanish (spoken), English (material, evaluation).
ECTS	4.5
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP007
Module name	Information Security
Module type	Course (C)
Training Provider	UMA
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	B (Basic)
Year – semester – exact dates offered	5th semester / approximately September to January / annually
Duration	Approximately 3-4 months; 4 hours per week
Training method and provision	Physical / ETSI Informática, University of Malaga, Malaga Spain
Evaluation method(s)	Physical exams
Module overview	This course aims to introduce the basic cybersecurity principles and management in computer and communications environments. For that reason, the course is oriented to provide a broad knowledge of the techniques, mechanisms, protocols and tools that allow providing protection at different levels of these environments, from the lowest level (networks) to the highest (applications and services).
Module description	TBA

Knowledge area(s)	2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	Pycryptodome (Python package for cryptography), XCA, Thunderbird for OpenPGP and S/MIME, IPTables, NMAP, Wireshark.
Language	Spanish (spoken, material), Spanish/English (evaluation)
ECTS	6
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_CSP008
Module name	Information Security and Computer Forensics
Module type	Course (C)
Training Provider	UMA
Contact	Rodrigo Román (rroman@uma.es)
Level	B (Basic)
Year – semester – exact dates offered	7th semester / approximately September to January / annually
Duration	Approximately 3-4 months; 3 hours per week
Training method and provision	Physical / Facultad de Derecho (Law School), University of Malaga, Malaga Spain
Evaluation method(s)	Physical exams
Module overview	This course is intended for criminology students who need to understand the context of a digital forensic investigation. To this end, the course will provide students with both the basic knowledge and the basic security and computer forensic skills required to carry out the various stages of the electronic evidence lifecycle from an introductory perspective.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management
Tools to be used	FTK Imager, Autopsy, John the Ripper, ExifTool, OpenPuff, Veracrypt
Language	Spanish (spoken, material, evaluation)
ECTS	6
Certificate of Attendance (CoA)	Not applicable
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_UCY_CSP001
Module name	Security in charging stations and their control systems
Module type	Seminar (S)
Training Provider	UMA (jointly with UCY)
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	B (Basic)

Year – semester – exact dates offered	Summer / annually
Duration	2h
Training method and provision	Virtual
Evaluation method(s)	Virtual tests and activities
Module overview	Cyber-physical systems integrated as part of electric vehicle charging infrastructures are mainly composed of software components and specific communication protocols. This makes them particularly susceptible to threats that may abuse the network protocol's implementation or software errors for exploiting a target system. The seminar therefore offers an overview of basic principles and management of security in charging infrastructure control systems.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management
Tools to be used	TBD
Language	English (spoken, material, evaluation)
ECTS	Not applicable
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UMA_UPRC_CSP001
Module name	Security of Maritime, Health & Energy Critical Information Infrastructures
Module type	Seminar (S)
Training Provider	UMA (jointly with UPRC)
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	B (Basic)
Year – semester – exact dates offered	Summer / annually
Duration	2h
Training method and provision	Virtual
Evaluation method(s)	Virtual tests and activities
Module overview	Hybrid and interconnected threats in maritime (e.g., ports), energy (e.g., LNG refueling stations at ports) and health (e.g., drug disposal, lack of access to immediate resources) infrastructures are analyzed, mitigating measures are presented and policy recommendations are made to reduce as much as possible the cascading effect between critical domains and sectors after threats.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	TBD
Language	English (spoken, material, evaluation)
ECTS	Not applicable
Certificate of Attendance (CoA)	Yes

Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	CNR_UMA_CSP001
Module name	SATRA for energy
Module type	O (self assessment method and tool)
Training Provider	CNR (jointly with UMA)
Contact	artsiom.yautsiukhin@iit.cnr.it
Level	B
Year – semester – exact dates offered	During the cybersecurity master in italy
Duration	2 hours
Training method and provision	Virtual
Evaluation method(s)	Virtual tests
Module overview	Basic terms and concepts Risk Management vs. Risk Assessment Risk assessment Risk identification Assets Threats Vulnerabilities/Security controls Risk analysis Risk evaluation Risk Treatment
Module description	TBA
Knowledge area(s)	5. Cybersecurity Risk Management
Tools to be used	SATRA – Self-Assessment Tool for Risk Analysis
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

3.1.8 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT), Austria

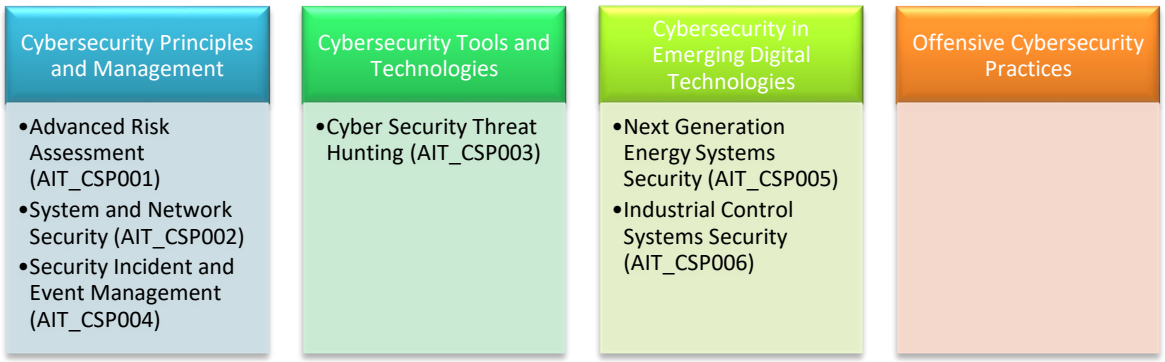

Figure 9. The full overview of AIT's training modules per CSP capability categories

Figure 9 presents the full overview of AIT's training modules per CSP capability categories. The following tables summarize the training modules that AIT is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	AIT_CSP001
Module name	Advanced Risk Assessment
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer (stefan.schauer@ait.ac.at)
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	3 Days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Risk Management Approaches, Risk Concepts and Models, Risk Management Process and Context establishment, Hazard Identification, Threat Analysis, Risk Evaluation, Risk Treatment, Risk Acceptance, Interdependencies, Cascading Effects
Module description	TBA
Knowledge area(s)	5. Cybersecurity Risk Management
Tools to be used	None
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	AIT_CSP002
Module name	System and Network Security
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer (stefan.schauer@ait.ac.at)
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	4 Days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Essentials, Holistic approach, Security policy, Monitoring and Recovery, Testing, Documentation
Module description	TBA
Knowledge area(s)	8. Network and Communication Security
Tools to be used	
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	AIT_CSP003
Module name	Cyber Security Threat Hunting
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer (stefan.schauer@ait.ac.at)
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	3-4 Days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Threat Intelligence, Anomaly identification, Log analysis, Forensic investigations, Network monitoring, Endpoint Detection and Response (EDR), Vulnerability assessment, Incident Response
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management
Tools to be used	None
Language	English
ECTS	

Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	AIT_CSP004
Module name	Security Incident and Event Management
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer (stefan.schauer@ait.ac.at)
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	3 days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Protocol collection and correlation, Real-time monitoring, Automated threat detection, Incident response functions, Protocol analysis and reporting, Integration with other security solutions
Module description	TBA
Knowledge area(s)	7. Cyber Incident Response
Tools to be used	
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	AIT_CSP005
Module name	Next Generation Energy Systems Security
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer stefan.schauer@ait.ac.at
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	4 days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Basic knowledge of Next Generation Energy Systems, Cyber security challenge insight, Secure architecture capabilities, Specialist technical expertise in secure communication protocols

Module description	TBA
Knowledge area(s)	3. Cybersecurity Management
Tools to be used	
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	AIT_CSP006
Module name	Industrial Control Systems Security
Module type	Course
Training Provider	AIT
Contact	Stefan Schauer stefan.schauer@ait.ac.at
Level	Advanced
Year – semester – exact dates offered	TBD
Duration	5 days
Training method and provision	Physical (Vienna)
Evaluation method(s)	Participation, Exercises
Module overview	Securing of ICS Environments, Risks in ICS environments, ICS security framework, Detecting ICS attacks, complexities of ICS analysis, Advanced ICS security tests
Module description	TBA
Knowledge area(s)	8. Network and Communication Security
Tools to be used	
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

3.1.9 CONSIGLIO NAZIONALE DELLE RICERCHE (CNR), Italy

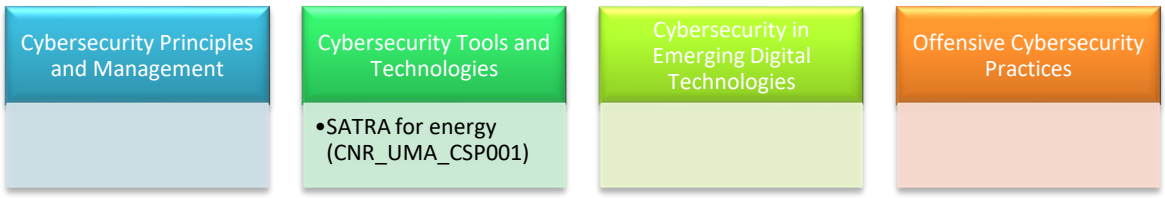

Figure 10. The full overview of CNR's training modules per CSP capability categories

Figure 10 presents the full overview of CNR's training modules per CSP capability categories. The following table summarizes the training module that CNR is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	CNR_UMA_CSP001
Module name	SATRA for energy
Module type	O (self assessment method and tool)
Training Provider	CNR (jointly with UMA)
Contact	Artsiom Yautsiukhin (artsiom.yautsiukhin@iit.cnr.it)
Level	B
Year – semester – exact dates offered	During the cybersecurity master in italy
Duration	2 hours
Training method and provision	Virtual
Evaluation method(s)	Virtual tests
Module overview	Basic terms and concepts Risk Management vs. Risk Assessment Risk assessment Risk identification Assets Threats Vulnerabilities/Security controls Risk analysis Risk evaluation Risk Treatment
Module description	TBA
Knowledge area(s)	5. Cybersecurity Risk Management
Tools to be used	SATRA – Self-Assessment Tool for Risk Analysis
Language	English
ECTS	
Certificate of Attendance (CoA)	

Module enrolment dates	
Other important dates	

3.1.10 COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL (COFAC), Portugal

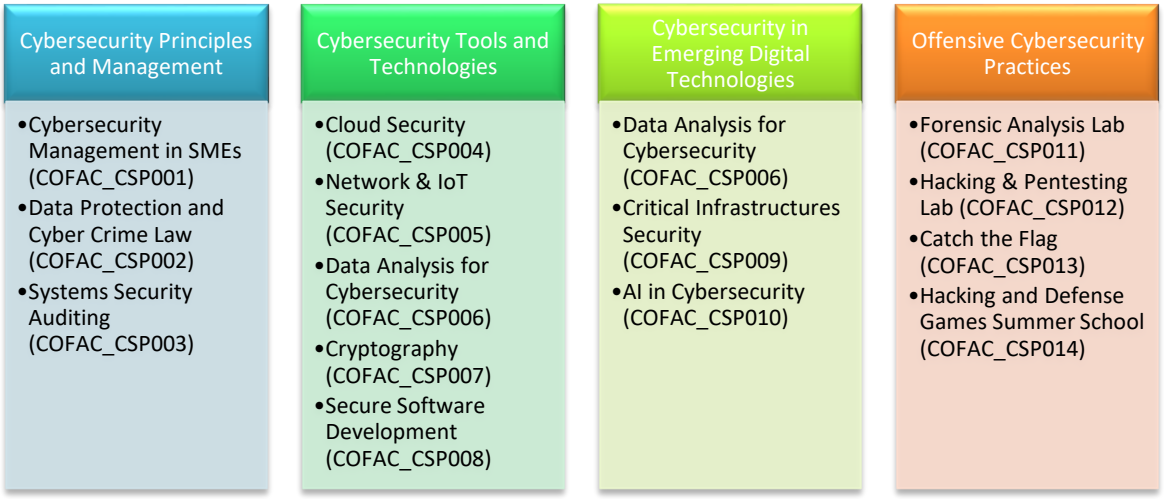

Figure 11. The full overview of COFAC's training modules per CSP capability categories

Figure 11 presents the full overview of COFAC's training modules per CSP capability categories. The following tables summarize the training modules that COFAC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	COFAC_CSP001
Module name	Cybersecurity Management in SMEs
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, Virtual exams, work reports.
Module overview	The "Cybersecurity Management in SMEs" module is a comprehensive exploration of the principles, strategies, and best practices tailored to the unique needs of Small and Medium-sized Enterprises (SMEs) in the realm of cybersecurity. In an era where cyber threats are indiscriminate, SMEs represent attractive targets due to their vulnerabilities and limited resources. This module is designed to empower students with the knowledge and skills necessary to navigate the complex world of cybersecurity within SMEs, ensuring the security of digital assets, business continuity, and compliance with regulations.

	1. Understanding Cybersecurity in SMEs 2. Cybersecurity Risk Assessment 3. Cybersecurity Strategy for SMEs 4. Security Controls and Best Practices 5. Incident Response and Recovery for SMEs 6. Compliance and Regulations 7. Third-party Risk Management 8. Security Awareness and Training 9. Cybersecurity Budgeting and Resource Allocation 10. Case Studies and Practical Exercises from cyber threats.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response
Tools to be used	Normative, Policies (NIST, 27001/*, TISAX among others) Risk Assessment Policies, Worksheets, Risk Software, and additional frameworks.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP002
Module name	Data Protection and Cyber Crime Law
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, Virtual exams, work reports.
Module overview	The "Data Protection and Cybercrime Laws" module is designed to provide students with a comprehensive understanding of the legal frameworks governing data protection and cybersecurity. In today's interconnected digital world, data is a valuable asset, and the module aims to equip students with the knowledge and skills necessary to navigate the complex landscape of data protection laws and regulations, as well as the legal aspects of combating cybercrime. 1. Introduction to Data Protection Laws 2. Key Data Protection Regulations 3. Data Privacy Compliance 4. Cybersecurity Legal Frameworks 5. Data Breach Notification Laws 6. Digital Forensics and Cybercrime Investigations

	7. Intellectual Property and Cybercrime 8. Emerging Legal Challenges in Cyberspace 9. Cybersecurity Incident Response and Legal Compliance 10. Case Studies and Legal Analysis
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response
Tools to be used	Westlaw, LexisNexis, Privacy Impact Assessments, NIST Cybersecurity Framework and ISO 27001, Data Protection Impact Assessments, EnCase, FTK, and Autopsy among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP003
Module name	Systems Security Auditing
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, Virtual exams, work reports.
Module overview	The "Systems Security Auditing" module is designed to equip students with the knowledge and skills required to assess, analyse, and improve the security of information systems within organizations. System security auditing is a critical component of cybersecurity, helping organizations identify vulnerabilities, ensure compliance with security policies, and enhance their overall security posture. This module provides a comprehensive understanding of auditing methodologies, tools, and best practices. 1. Introduction to Systems Security Auditing 2. Auditing Frameworks and Standards 3. Auditing Methodologies 4. Risk Assessment and Management 5. Security Policy and Compliance Auditing 6. Technical Auditing Tools 9. Auditing Network Security 10. Application Security Auditing 12. Incident Response Auditing 13. Reporting and Documentation 14. Ethical and Legal Considerations 14. Practical Auditing Scenarios

Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	ISO 27001, NIST, CIS, Nessus, Wireshark, OpenVAS, among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP004
Module name	Cloud Security
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Cloud Security" module is designed to provide students with a deep understanding of the unique challenges and best practices associated with securing cloud computing environments. As organizations increasingly migrate their data and services to the cloud, there is a growing need for professionals who can ensure the security and compliance of cloud-based infrastructures. This module covers cloud security concepts, strategies, and technologies to prepare students for the complexities of safeguarding data and applications in the cloud. 1. Introduction to Cloud Security 2. Cloud Deployment Models 3. Cloud Security Architecture 4. Data Security in the Cloud 5. Network Security in the Cloud 6. Cloud Compliance and Governance 7. Cloud Threat Detection and Response 8. Security Automation and Orchestration 9. Cloud Security Best Practices 10. Cloud Security Challenges and Emerging Trends 11. Practical Cloud Security Scenarios
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 5. Cybersecurity Risk Management

	6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	IAM solutions, DLP, VPCs, ACLs, GDPR, HIPAA, Zero Trust.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP005
Module name	Network & IoT Security
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Network and IoT Security" module is designed to provide students with a comprehensive understanding of the principles, strategies, and best practices for securing modern networks and the Internet of Things (IoT) ecosystems. In an increasingly interconnected world, the security of networks and IoT devices is paramount. This module covers the fundamentals of network security and delves into the unique challenges posed by IoT devices, preparing students to protect critical data and infrastructure. 1. Introduction to Network Security 2. Authentication and Access Control 3. Introduction to Network Security 4. Network Security Architecture 5. Authentication and Access Control: 6. Cryptography in Network Security 7. Network Security Protocols 8. Wireless Network Security 9. Network Threat Detection and Response 10. IoT Security Fundamentals 11. IoT Device Authentication and Authorization 12. IoT Network Security 13. IoT Vulnerability Assessment: 14. IoT Security Best Practices Emerging Trends in Network and IoT 15. Security
Module description	TBA
Knowledge area(s)	1. Penetration Testing 3. Cybersecurity Management

	5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	IDS, VPNs, RBAC, SSL/TLS, IPsec, SSH, MQTT, CoAP among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP006
Module name	Data Analysis for Cybersecurity
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Data Analysis in Cybersecurity" module is designed to equip students with the knowledge and skills needed to harness the power of data analytics and machine learning in the context of cybersecurity. In today's rapidly evolving threat landscape, organizations rely on data-driven insights to detect and respond to cyber threats effectively. This module explores various data analysis techniques and tools, emphasizing their application to cybersecurity scenarios. 1. Introduction to Data Analysis in Cybersecurity 2. Data Collection and Preparation 3. Data Visualization and Exploration 4. Statistical Analysis for Threat Detection 5. Machine Learning in Cybersecurity 6. Feature Engineering for Cybersecurity Data Intrusion Detection and Prevention 7. Malware Analysis and Behavioural Analytics 8. SIEM Integration 9. Threat Intelligence and Threat Hunting 10. Cybersecurity Data Privacy and Ethics 11. Practical Cybersecurity Data Analysis Projects
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security 9. Privacy and Data Protection

	10. Human Aspects of Cybersecurity
Tools to be used	Python, Jupiter notebooks, TensorFlow, Power BI, SQL OLAP, Wireshark among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP007
Module name	Cryptography
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Cryptography" module offers a comprehensive exploration of the principles, algorithms, and applications of cryptography in the realm of cybersecurity. Cryptography plays a pivotal role in safeguarding sensitive information, securing communications, and ensuring data integrity. This module equips students with the knowledge and skills required to understand, apply, and evaluate cryptographic techniques effectively. 1. Introduction to Cryptography 2. Cryptography Foundations 3. Classical Cryptographic Techniques 4. Modern Symmetric Cryptography 5. Public-Key Cryptography 6. Cryptographic Protocols 7. Hash Functions and Message Authentication 8. Cryptographic Applications 9. Cryptanalysis and Attacks 10. Quantum Cryptography 11. Cryptography in Blockchain and Cryptocurrencies
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security 9. Privacy and Data Protection
Tools to be used	OpenSSL, GnuPG, PyCryptodome, Solidity among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes

Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP008
Module name	Secure Software Development
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Secure Software Development" module is designed to educate students about the principles, methodologies, and best practices for developing software with security in mind. In an era of increasing cyber threats and data breaches, it is crucial for developers to incorporate security measures throughout the software development lifecycle. This module equips students with the knowledge and skills necessary to design, code, test, and deploy software securely. 1. Introduction to Secure Software Development 2. Security Threats and Vulnerabilities 3. Secure Software Development Lifecycle (SDLC) 4. Secure Coding Practice 5. Authentication and Authorization: 6. Secure API Development 7. Data Security: 8. Secure Development Tools 9. Threat Modelling 10. Security Testing and Quality Assurance Secure DevOps and Continuous Integration/Continuous Deployment (CI/CD) 11. Secure Software Architecture 12. Secure Software Documentation 13. Secure Software Deployment and Maintenance
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management
Tools to be used	Visual Studio Code, SonarQube, Nexus Lifecycle, Burp Suite, Jenkins among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP009
Module name	Critical Infrastructures Security
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Critical Infrastructures Security" module focuses on the protection and resilience of vital systems and assets that underpin a nation's functionality, including energy, transportation, telecommunications, and water supply. This module explores the unique challenges and strategies required to safeguard critical infrastructures against physical and cyber threats. Students will gain an understanding of the principles, policies, and technologies essential for ensuring the security of these critical systems. 1. Introduction to Critical Infrastructures 2. Types of Critical Infrastructures 3. Threat Landscape for Critical Infrastructures 4. Regulatory Framework and policies 5. Risk Assessment and Management 6. Physical Security Measures 7. Cybersecurity for Critical Infrastructures 8. Incident Response and Disaster Recover 9. Resilience and Redundancy 10. Critical Infrastructure Protection Exercises
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 7. Cyber Incident Response
Tools to be used	IBM QRadar, ArcSight, SCADA/ICS, Dragos, OnSolve among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP010
Module name	AI in Cybersecurity
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)

Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Artificial Intelligence in Cybersecurity" module is designed to provide students with a comprehensive understanding of how artificial intelligence (AI) and machine learning (ML) technologies are applied to address cybersecurity challenges. As cyber threats continue to evolve, AI plays a crucial role in enhancing threat detection, incident response, and overall security. This module explores AI algorithms, techniques, and applications within the context of cybersecurity. 1. Introduction to AI in Cybersecurity 2. AI Fundamentals 3. Cyber Threat Landscape 4. AI for Threat Detection 5. Machine Learning Models for Cybersecurity 6. Deep Learning for Cybersecurity 7. AI-Enhanced Security Analytics 8. AI in Endpoint Security 9. AI in Network Security 10. Natural Language Processing (NLP) in Security
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security
Tools to be used	Python, TensorFlow, Zeek, Open-source AI libraries among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP011
Module name	Forensic Analysis Lab
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Forensic Analysis" module is designed to equip students with the knowledge and skills required to conduct digital forensic investigations

	effectively. Digital forensics is crucial in uncovering evidence related to cybercrimes, data breaches, and other security incidents. This module covers the principles, techniques, and tools used in forensic analysis, enabling students to collect, preserve, analyse, and present digital evidence in a legal and ethical manner. 1. Introduction to Digital Forensics 2. Digital Evidence Types 3. Forensic Investigation Process 4. Evidence Acquisition 5. Data Recovery and Preservation 6. File System Analysis 7. Memory Forensics 8. Network Forensics 9. Malware Analysis 10. Digital Forensics Tools 11. Mobile Device Forensics 12. Database Forensics 13. Incident Response and Forensic Analysis
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	Python, TensorFlow, Zeek, Open-source AI libraries among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP012
Module name	Hacking and Pentesting Lab
Module type	C
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	A
Year – semester – exact dates offered	1st Semester 2024 (01.09.24) -> TBD 2nd Semester 2024 (01.01.25) -> TBD
Duration	15 weeks
Training method and provision	Physical, Virtual (Zoom)
Evaluation method(s)	Physical, virtual exams, work reports.
Module overview	The "Hacking and Pentest Lab" module is a practical and hands-on learning experience designed to immerse students in the world of ethical hacking and penetration testing. In today's cybersecurity landscape, organizations need skilled professionals who can identify and mitigate security vulnerabilities. This module provides students with the opportunity to gain practical expertise in identifying, exploiting, and securing systems, networks, and applications. 1. Vulnerability Assessment

	2. Penetration Testing Techniques 3. Exploitation and Post-Exploitation 4. Network Intrusion Testing 5. Security Controls and Countermeasures 6. Database and Software Exploitation 7. Ethical Hacking and Responsible Disclosure 8. Hands-On Labs and Simulations 9. Reporting and Documentation
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	Nessus, OpenVAS, Metasploit, Nmap, Aircrack-ng, SQLMap, John the Ripper, shcat Utopsy, Kali Linux among other.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP013
Module name	Catch the Flag (CTF) Workshop
Module type	W
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	2nd Semester 2024 (01.01.25) -> TBD
Duration	1 Day 4 + 4 hours.
Training method and provision	Physical
Evaluation method(s)	TBD
Module overview	The "Capture The Flag (CTF) Workshop" is an interactive and hands-on learning experience designed for cybersecurity challenges and real-world scenarios. Capture The Flag events are widely recognized as effective tools for enhancing cybersecurity skills, teamwork, and problem-solving abilities. This workshop provides an immersive environment where participants can apply their knowledge in a fun and competitive atmosphere. 1. Understand CTF Concepts 2. Apply Technical Skills 3. Team Collaboration 4. Problem-Solving Abilities 5. Time Management 6. Ethical Hacking and Responsible Conduct 7. Hands-On Experience
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 7. Cyber Incident Response 8. Network and Communication Security

Tools to be used	Burp Suite, Tcpdump, OpenSSL, John the Ripper, Reaver, SQLMap, Kali Linux among others.
Language	Portuguese & English
ECTS	5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	COFAC_CSP014
Module name	Hacking and Defence Games Summer School
Module type	SS
Training Provider	COFAC
Contact	Nuno Mateus-Coelho (nuno.coelho@ulusofona.pt)
Level	B
Year – semester – exact dates offered	2nd Semester 2024 (01.01.25) -> TBD
Duration	2 Day 8 + 8hours.
Training method and provision	Physical
Evaluation method(s)	Participation in hands-on labs and exercises, Completion of practical cybersecurity challenges, Group discussions and quizzes.
Module overview	The "Summer School of Cybersecurity" is an intensive and immersive two-day programme designed to provide participants with a comprehensive introduction to the field of cybersecurity. In an era of increasing digitalization and cyber threats, this summer school offers a unique opportunity for students and enthusiasts to gain foundational knowledge, hands-on experience, and insights into the world of cybersecurity. 1. Introduction to Cybersecurity 2. Network Security 3. Information Security 4. Threats and Vulnerabilities 5. Risk Management 6. Cryptography and Encryption 7. Security Best Practices 8. Ethical Hacking Fundamentals 9. Cybersecurity Career Paths
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	5

Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

3.1.11 SINTEF AS (SINTEF), Norway

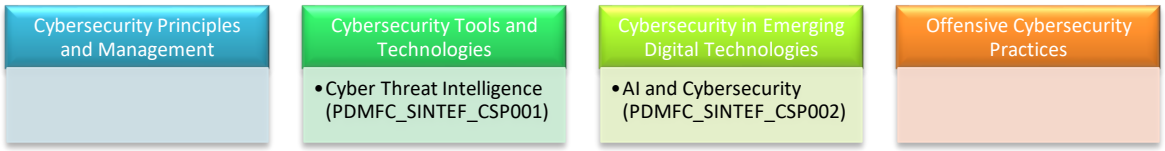

Figure 12. The full overview of SINTEF's training modules per CSP capability categories

Figure 12 presents the full overview of SINTEF's training modules per CSP capability categories. The following tables summarize the training modules that SINTEF is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	PDMFC_SINTEF_CSP001
Module name	AI and Cybersecurity
Module type	Seminar (S)
Training Provider	PDMFC (jointly with SINTEF)
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com) Nektaria Kaloudi (nektaria.kaloudi@sintef.no)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Both
Evaluation method(s)	Participation and exercises
Module overview	The module explores the reciprocal influence of AI and cybersecurity. It will cover the three dimensions in which AI and cybersecurity intersect, covering both challenges and opportunities from the offensive and defensive aspects. Examples will include adversary penetration testing and emerging challenges of adversarial AI through a blend of theoretical and practical exercises. It covers various facets of this intersection, including adversary penetration testing, intrusion detection systems (IDS), Security Information and Event Management (SIEM) systems, and the emerging challenge of adversarial AI. Through a blend of theoretical knowledge and practical exercises, students gain a comprehensive understanding of how AI can be applied defensively and offensively in cybersecurity, with a focus on building expertise in AI-driven penetration testing, enhancing IDS and SIEM with AI, and defending against adversarial AI attacks.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 8. Network and Communication Security

Tools to be used	NFStream, Wireshark, Tshark, Python, Tensorflow, PySyft
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_SINTEF_CSP002
Module name	Cyber Threat Intelligence
Module type	Seminar (S)
Training Provider	PDMFC (jointly with SINTEF)
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com) Nektaria Kaloudi (nektaria.kaloudi@sintef.no)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Both
Evaluation method(s)	Participation and exercises
Module overview	Comprehensive exploration of the core principles and practical applications of cyber threat intelligence. It equips students with a deep understanding of threat identification, threat actor analysis, and motives. The module emphasizes hands-on training with industry-standard tools, including STIX and TAXII for structured threat information sharing and security, OpenCTI for effective threat intelligence management and integration, and MISP for structured threat data sharing. Depending on scenarios within the sectors (e.g., health, energy, maritime), the module will show the integration of the TORC tool with cyber threat intelligence-based cybersecurity trainings and best practices in a way that enhances stakeholders' resilience and adaptability in the face of cyber threats.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	STIX, TAXII, OpenCTI, and MISP, Digital TORC
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

3.1.12 UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIASASSOCIACAO (UNINOVA), Portugal

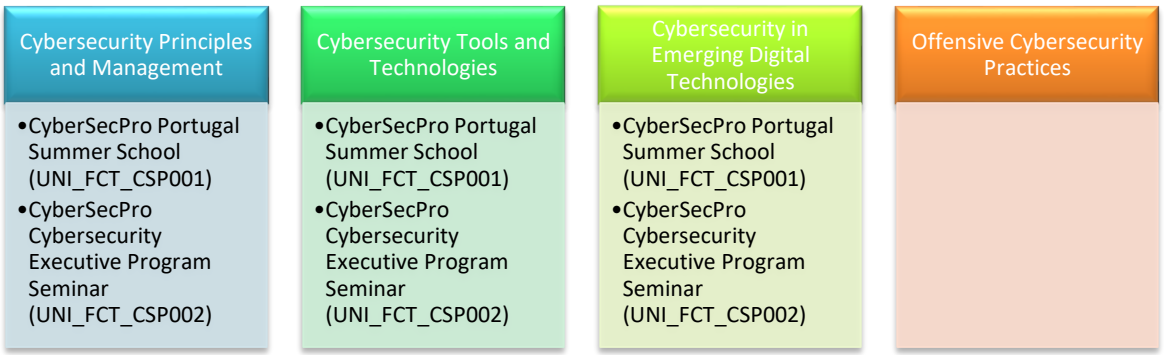

Figure 13. The full overview of UNINOVA's training modules per CSP capability categories

Figure 13 presents the full overview of UNINOVA's training modules per CSP capability categories. The following tables summarize the training modules that UNINOVA is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	UNI_FCT_CSP001
Module name	CyberSecPro Portugal Summer School
Module type	SS – Summer School
Training Provider	UNINOVA (jointly with FCT)
Contact	Vasco Delgado-Gomes vmdg@uninova.pt José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	TBD (expected between 24-28 June 2024)
Duration	2 days
Training method and provision	Physical – Madeira, Portugal (hotel will be informed later)
Evaluation method(s)	Summer School participation and engagement
Module overview	The CSP Summer School 2024 will focus on basic Cyber Security training for SMEs based in Portugal and other European countries, and in the domains of Health, Energy, and Maritime. It will provide a general comprehensive view on the threats and issues associated with insufficient security and privacy measures and how to tackle such threats in the context of SMEs.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese

ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	UNI_FCT_CSP002
Module name	CyberSecPro Cybersecurity Executive Program Seminar
Module type	S -Seminar
Training Provider	UNINOVA (jointly with FCT)
Contact	Vasco Delgado-Gomes vmdg@uninova.pt José Fonseca jmrf@fct.unl.pt
Level	A - Advanced
Year – semester – exact dates offered	TBD (expected June 2025)
Duration	3-4 days
Training method and provision	Physical – Lisbon, Portugal
Evaluation method(s)	Seminar participation and engagement
Module overview	The Cybersecurity Executive Program will be composed by 3 different and independent modules: **1 - Strategic Leadership and Governance:** This module will focus on providing executives with a strategic understanding of cybersecurity, enabling them to lead cybersecurity initiatives, make informed decisions, and effectively communicate cybersecurity risks and investments to stakeholders. **2- Incident Response and Risk Management:** This module will emphasize the preparedness and response aspects of cybersecurity. Executives will learn how to effectively respond to incidents, manage crises, mitigate risks associated with vendors and third parties, and integrate cybersecurity into business continuity planning. **3 - Emerging Trends and Collaboration:** This module will explore emerging trends, technologies, and collaboration in the cybersecurity landscape. Executives will gain insights into ethical and legal implications, international cooperation, cyber threat intelligence, security operations, and the impact of emerging technologies on cybersecurity. This seminar will focus on executives and leaders from SMEs in the domains of Health, Energy, and Maritime.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	N/A

Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

3.1.13 UNIVERSITY OF PIRAEUS RESEARCH CENTER (UPRC), Greece

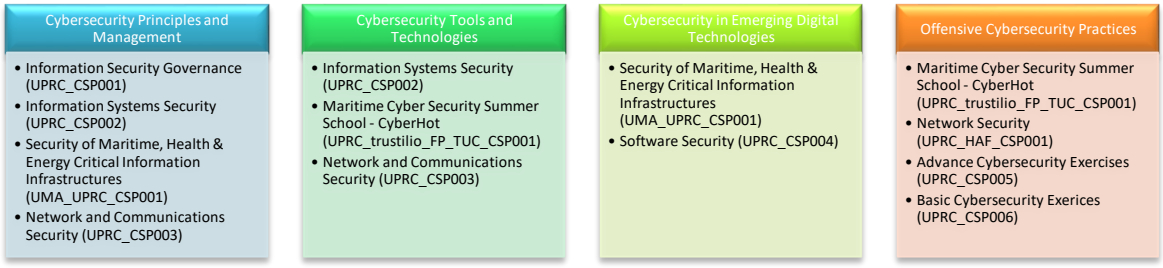

Figure 14. The full overview of UPRC's training modules per CSP capability categories

Figure 14 presents the full overview of UPRC's training modules per CSP capability categories. The following tables summarize the training modules that UPRC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	UPRC_CSP001
Module name	Information Security Governance
Module type	Course (C)
Training Provider	UPRC
Contact	Despoina Polemi (dpolemi@gmail.com)
Level	A (Advanced)
Year – semester – exact dates offered	October to February
Duration	
Training method and provision	Physical, partially virtual
Evaluation method(s)	
Module overview	The following topics are covered: Common vulnerabilities of systems and applications; Methods and tools to discover vulnerabilities of apps and systems; Exploitation & persistence Digital forensics Information risk analysis; Security plans, policies and processes Regulatory framework and security standards Continuity and recovery plans.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity, Policy, Process and Compliance 10. Human Aspects of Cybersecurity
Tools to be used	
Language	GR
ECTS	6
Certificate of Attendance (CoA)	

Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UPRC_CSP002
Module name	Information Systems Security
Module type	Course (C)
Training Provider	UPRC
Contact	Panagiotis Kotzanikolaou (pkotzani@unipi.gr)
Level	A (Advanced)
Year – semester – exact dates offered	February to June
Duration	
Training method and provision	Physical, partially virtual
Evaluation method(s)	Coursework examination
Module overview	The following topics are covered: Security Management Systems; Cryptographic systems; Public Key Infrastructure; Access control and Privacy Security in Technologies; Secure electronic and mobile services.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies
Tools to be used	CryptTool, OpenSSL, OpenLDAP
Language	GR
ECTS	5
Certificate of Attendance (CoA)	No
Module enrolment dates	6 Oct – 19 Jan
Other important dates	

Training Module fields	Training Module information
Code	UPRC_CSP003
Module name	Network and Communications Security
Module type	Course (C)
Training Provider	UPRC
Contact	Christos Douligeris (cdoulig@unipi.gr)
Level	Intermediate
Year – semester – exact dates offered	Winter semester
Duration	-
Training method and provision	Physical, partially virtual
Evaluation method(s)	Coursework examination
Module overview	The following topics are covered: Data-link layer security, Network layer security, Transport layer security, Designing network security policies, Cross-layer network security mechanisms, Application-layer firewalls and IDS. Network security includes the proactive study of all methods,

	techniques and tools aimed at designing, implementing and monitoring the implementation of a structured and documented network security policy. This course covers the basic principles and technologies of network security, such as the definition of network security policy, the identification and detection of network security incidents and the implementation of technologies and measures for the proper implementation of the security policy.
Module description	TBA
Knowledge area(s)	7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Snort, OSSEC
Language	GR
ECTS	6
Certificate of Attendance (CoA)	No
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UPRC_CSP004
Module name	Software Security
Module type	Course (C), Seminar (S)
Training Provider	UPRC
Contact	Panagiotis Kotzanikolaou (pkotzani@unipi.gr)
Level	A (Advanced)
Year – semester – exact dates offered	February to June
Duration	-
Training method and provision	Physical, partially virtual
Evaluation method(s)	Coursework examination
Module overview	The following topics are covered: Identification of security issues in open source and closed source software, Code Auditing, Demonstration and rating of a vulnerability and Implementation and maintenance phases of software projects. Through lectures, assignments and workshops students will find out how to identify security bugs both in software for which the source code has been made available (code review) but also in software where source code is not available (black box review). The vulnerabilities studied throughout this course come from a wide area of applications including: operating system software, embedded systems software, Internet services, desktop software, web applications and mobile applications.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies
Tools to be used	Code auditing tools
Language	Spoken: GR Material: GR / EN Assessment: GR / EN
ECTS	6
Certificate of Attendance (CoA)	No

Module enrolment dates	-
Other important dates	

Training Module fields	Training Module information
Code	UPRC_CSP005
Module name	Advance Cybersecurity exercises
Module type	Cybersecurity exercise (CS-E)
Training Provider	UPRC
Contact	Spyros Papageorgiou, Panagiotis Kotzanikolaou (pkotzani@unipi.gr)
Level	A (Advanced)
Year – semester – exact dates offered	Summer
Duration	-
Training method and provision	Physical, partially virtual
Evaluation method(s)	
Module overview	Two sectoral Cybersecurity exercises
Module description	TBA
Knowledge area(s)	1.Penetration Testing, 7.Cyber Incident Response
Tools to be used	
Language	Spoken: GR / EN
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	-
Other important dates	

Training Module fields	Training Module information
Code	UPRC_CSP006
Module name	Basic Cybersecurity exercises
Module type	Cybersecurity exercise (CS-E)
Training Provider	UPRC
Contact	Spyros Papageorgiou, Panagiotis Kotzanikolaou (pkotzani@unipi.gr)
Level	B
Year – semester – exact dates offered	Summer
Duration	-
Training method and provision	Physical, partially virtual
Evaluation method(s)	
Module overview	Two sectoral Cybersecurity exercises
Module description	TBA

Knowledge area(s)	1.Penetration Testing, 7.Cyber Incident Response
Tools to be used	
Language	Spoken: GR / EN
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	-
Other important dates	

Training Module fields	Training Module information
Code	UPRC_HAF_CSP001
Module name	Network Security (UPRC jointly with Hellenic Air Force)
Module type	Course (C)
Training Provider	Hellenic Air Force
Contact	Antonios Andreatos (antonios.andreatos@hafa.haf.gr)
Level	B (Basic)
Year – semester – exact dates offered	February to June
Duration	
Training method and provision	Physical, partially virtual
Evaluation method(s)	
Module overview	The following topics are covered: Introduction, Principles of Cryptography, Message Integrity, Digital Signatures, Hash Function, Digital Signatures, Key Management, End-Point Authentication, Secure E-Mail, SSL, Securing Wireless LANs, Operational Security, Firewalls and Intrusion Detection Systems, Malware.
Module description	TBA
Knowledge area(s)	2.Cybersecurity Tools and Technologies 8.Network and Communication Security
Tools to be used	
Language	Spoken: GR/EN
ECTS	2
Certificate of Attendance (CoA)	Yes (if partially attended)
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	UMA_UPRC_CSP001
Module name	Security of Maritime, Health & Energy Critical Information Infrastructures
Module type	Seminar (S)
Training Provider	UPRC (jointly with UMA)
Contact	Cristina Alcaraz (alcaraz@uma.es)
Level	B (Basic)

Year – semester – exact dates offered	Summer / annually
Duration	2h
Training method and provision	Virtual
Evaluation method(s)	Virtual tests and activities
Module overview	Hybrid and interconnected threats in maritime (e.g., ports), energy (e.g., LNG refueling stations at ports) and health (e.g., drug disposal, lack of access to immediate resources) infrastructures are analyzed, mitigating measures are presented and policy recommendations are made to reduce as much as possible the cascading effect between critical domains and sectors after threats.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	TBD
Language	English (spoken, material, evaluation)
ECTS	Not applicable
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	-

Training Module fields	Training Module information
Code	UPRC_Trustilio_FP_TUC_CSP001
Module name	Maritime Cyber Security Summer School - CyberHot
Module type	Summer School (SS)
Training Provider	UPRC jointly with trustilio, Focal Point, TUC
Contact	Despoina Polemi (dpolemi@gmail.com)
Level	A (Advanced)
Year – semester – exact dates offered	(Summer) 01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Physical
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The "Maritime Cyber Security Summer School - CyberHot" is an immersive and intensive programme designed to equip participants with essential knowledge and practical skills in safeguarding maritime systems and infrastructure against cyber threats. Throughout this comprehensive seminar, trainees will delve into the intricate realm of maritime cyber security, exploring the diverse spectrum of threats and attacks that can potentially compromise the safety and functionality of ships and ports. Through hands-on training, participants will learn to identify vulnerabilities, assess risks, and implement mitigation actions, ensuring the resilience of maritime operations in an increasingly digitalized world. Additionally, the programme will provide a thorough examination of the legal, standards, and regulatory frameworks governing the maritime industry, enabling trainees to navigate compliance challenges and foster a secure and compliant maritime cyber ecosystem. By the end of the seminar, participants will emerge with practical skills and a deep understanding of cyber security tailored specifically to the maritime domain, positioning them as capable guardians of maritime cyber infrastructure.

Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

3.1.14 APIROPLUS SOLUTIONS LTD (APIRO), Cyprus

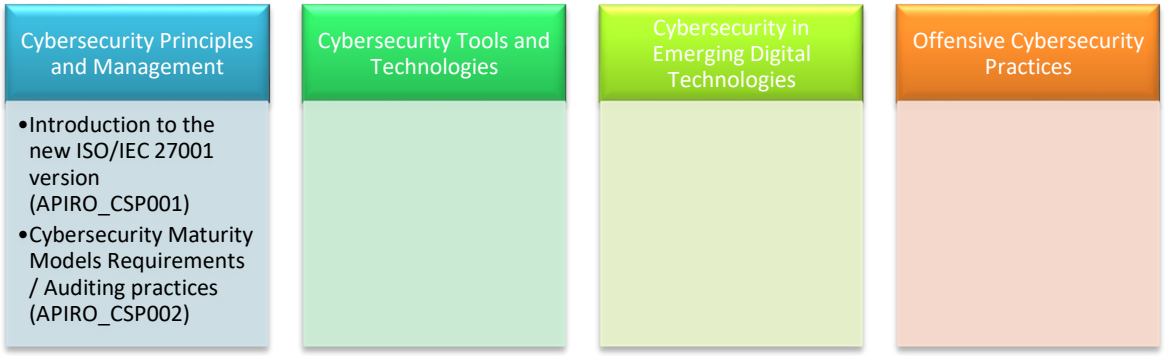

Figure 15. The full overview of APIRO's training modules per CSP capability categories

Figure 15 presents the full overview of APIROPLUS's training modules per CSP capability categories. The following tables summarize the training modules that APIROPLUS is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	APIRO_CSP001
Module name	Introduction to the new ISO/IEC 27001 version
Module type	Course (C)
Training Provider	APIROPLUS SOLUTIONS LTD.
Contact	Argyro Chatzopoulou (ac@apiroplus.solutions) Apostolis Karras (ak@apiroplus.solutions)
Level	B (Basic)
Year – semester – exact dates offered	September - July
Duration	8 hours
Training method and provision	Virtual
Evaluation method(s)	Participation and exercises
Module overview	The course has been created to introduce to the greater audience the requirements and operations of ISO/IEC 27001. Since the course has been

	created near the publication of the new ISO/IEC 27001 standard, the course also focuses on the changes between version 2013 and version 2022. The course covers • the importance and benefits of information security for the organisation and its customers • the basic structure and requirements of ISO/IEC 27001:2022 • the principles and methods prescribed related to information security risk management and the connection to Annex A • the mandatory minimum documentation related to an ISO/IEC 27001:2022 implementation • the transition period for certified ISO/IEC 27001:2013 systems based on the IAF Mandatory Document • the changes between version 2013 and version 2022 for the core requirements (4-10) and • the changes between version 2013 and version 2022 for the controls of Annex A and the way that ISO/IEC 27002:2022 is used.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	None
Language	Spoken: English or Greek Material: English
ECTS	
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	APIRO_CSP002
Module name	Cybersecurity Maturity Models Requirements / Auditing practices
Module type	Course (C)
Training Provider	APIROPLUS SOLUTIONS LTD.
Contact	Argyro Chatzopoulou (ac@apiroplus.solutions) Apostolis Karras (ak@apiroplus.solutions)
Level	A (Advanced)
Year – semester – exact dates offered	September - July
Duration	8 hours
Training method and provision	Virtual
Evaluation method(s)	Participation and exercises
Module overview	The last years, maturity models have been introduced also in the cybersecurity domain. Although the cybersecurity maturity models developed are still in their early stages and vary in type, scope and range, the market has already identified them as a valuable asset for organisations. The course covers • the concept of maturity models in general and in specific in cybersecurity, • the different types of maturity models and their scales, • well known examples of cybersecurity maturity models and

	• processes and methods utilised in order to assess the compliance of an organisation against the requirements of the levels of specific cybersecurity maturity models.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	None
Language	Spoken: English or Greek Material: English
ECTS	
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	

3.1.15 C2B CONSULTING (C2B), France

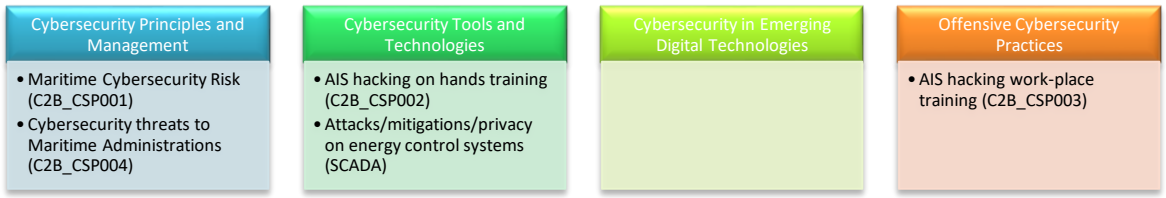

Figure 16. The full overview of C2B's training modules per CSP capability categories

Figure 16 presents the full overview of C2B's training modules per CSP capability categories. The following tables summarize the training modules that C2B is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	C2B_CSP001
Module name	Maritime Cybersecurity Risk
Module type	Course (C)
Training Provider	C2B
Contact	Bruno Bender (bruno.bender@ventura-associate.com)
Level	B (Basic)
Year – semester – exact dates offered	September to July
Duration	6hrs
Training method and provision	Physical and/or Distantly
Evaluation method(s)	Multiple choice Questionnaire
Module overview	The course aims at describing the maritime environment and specificities. A focus is done on the AIS standards and specificities as well as on international

	regulation. Common vulnerabilities of AIS/GNSS systems and applications are detailed; Methods and examples of hacking and spoofing of these systems are demonstrated during the course. Risk analysis, security plans, policies and processes, regulatory framework and security standards continuity and recovery measures are presented.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	No tool needed
Language	ENG / FRA / DEU
ECTS	5
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	C2B_CSP002
Module name	AIS hacking on hands training
Module type	Course (C)
Training Provider	C2B
Contact	Bruno Bender (bruno.bender@ventura-associate.com)
Level	B (Basic)
Year – semester – exact dates offered	January to July
Duration	6 hrs
Training method and provision	Physical
Evaluation method(s)	Test
Module overview	In continuation of Course C2B_CSP001, the course aims at providing a training on AIS devices. During the activity a group of trainees (6 – 12 Pax) will have the opportunity to practice simulated attacks. Most often observed attacks of AIS (including attacks via GNSS) are detailed and presented during the course.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	AIS transponder, RF Jammer
Language	ENG / FRA / DEU
ECTS	5 (TBA)
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	C2B_CSP003
Module name	AIS hacking work-place training
Module type	Course (C)
Training Provider	C2B
Contact	Bruno Bender (bruno.bender@ventura-associate.com)
Level	B (Basic)
Year – semester – exact dates offered	January to July
Duration	4 hrs
Training method and provision	Physical on the workplace
Evaluation method(s)	TBA
Module overview	Course C2B_CSP003 is a course that can be operated on a physical installation operated by an end-user. The course should be as reallistic as possible and aims at providing a training on AIS devices detained by an entity willing to improve the training of its personnel. It will help to identify spoofing or jamming of AIS and GNSS. During the activity a group of trainees (4 – 6 Pax) will have the opportunity to face the symptoms of attacks, simulated on the devices they are normally operating. Most often observed attacks of AIS (including attacks via GNSS) are simulated via a dedicated platform and presented to the audience during the course.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	AIS transponder
Language	ENG / FRA / DEU
ECTS	5 (TBA)
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	C2B_CSP004
Module name	Cybersecurity threats to Maritime Administrations
Module type	Workshop (W)
Training Provider	C2B
Contact	Bruno Bender (bruno.bender@ventura-associate.com)
Level	B (Basic)
Year – semester – exact dates offered	January to November
Duration	12 hrs
Training method and provision	Physical
Evaluation method(s)	Written / online test
Module overview	Course C2B_CSP004 is a 2 days workshop dedicated to the specific threats for administrations operating at sea.

	The course aims at providing an overview on threats and attacks that have been observed in the past year in the maritime. The activity can take place during an overall workshop on security and will detail several activities on the methodologies to assess risks, to reduce them and draft security operating procedures within a maritime entity. Several interactive modules will allow participants to face System Security issues as preemptive measures to reduce cybersecurity risks and reduce impacts of potential threats.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	No tools needed
Language	ENG / FRA / DEU
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	C2B_CSP005
Module name	Attacks/countermeasures/mitigations/privacy on energy control systems (SCADA)
Module type	Course (C)
Training Provider	C2B
Contact	Bruno Bender (bruno.bender@ventura-associate.com)
Level	B (Basic)
Year – semester – exact dates offered	January to June
Duration	4hrs
Training method and provision	Physical
Evaluation method(s)	Written test
Module overview	Industrial Control Systems also referred to as Supervisory Control and Data Acquisition (SCADA] systems, are essential component of critical infrastructure sectors. As so they are also representing an attractive target for cyberattacks. The couse aims at identify threats and risks on these systems and on how best to protect them from compromise via methods and courses of action that could include updates and patches. These operations can have catastrophic impact even on life. It also proposes to describe mitigations for better protection, in particular for data loss prevention. Course C2B_CSP005 is a generic course dedicated to industrial systems operating in the energy sector. The course aims also at providing an overview on threats and attacks that have been observed in the past year on energy control systems. The course could include the participation of a SCADA vendor (SCHNEIDER).
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 5. Cybersecurity Risk Management

	6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response
Tools to be used	No tools needed
Language	ENG / FRA
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

3.1.16 FOCAL POINT (FP), Belgium

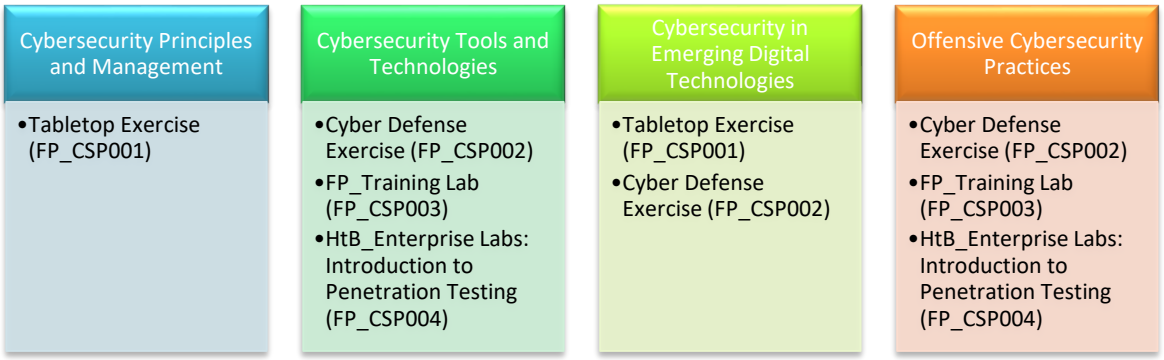

Figure 17. The full overview of FP's training modules per CSP capability categories

Figure 17 presents the full overview of FP's training modules per CSP capability categories. The following tables summarize the training modules that FP is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	FP_CSP001
Module name	Focal Point - Tabletop Exercise
Module type	Other – Tabletop Cybersecurity Game
Training Provider	Focal Point
Contact	Paris E. Laras plaras@focalpoint-sprl.be
Level	B
Year – semester – exact dates offered	Scheduled upon request, starting from February 2024,
Duration	30 – 60 minutes
Training method and provision	Both Physical and Digital or Hybrid, Location is open option, organized ad-hoc Digitally provided with a web or mobile application and complemented by communications over Zoom, MS Teams or Webex.
Evaluation method(s)	Participation-based, Gamified Evaluation
Module overview	Relevant topics: Network security control. Incident response. Risk management. An interactive, gamified experience or multiple participating persons. Participants are divided into groups with each group led by a

	moderator assisting in the distribution of relevant materials, educating the participants, moderating the exercise, and reporting on the outcomes of the game session. Participants gain increased cyber-awareness and are introduced to cyber hygiene concepts by interacting with the game and through exchanges with other participants.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	Proprietary game software (.apk, web app etc.)
Language	English
ECTS	-
Certificate of Attendance (CoA)	-
Module enrolment dates	Upon Demand
Other important dates	-

Training Module fields	Training Module information
Code	FP_CSP002
Module name	Focal Point – Cyber Defense Exercise
Module type	*CS-E*
Training Provider	Focal Point
Contact	Christos Grigoriadis cgrigor@focalpoint-sprl.be
Level	A
Year – semester – exact dates offered	Upon Demand
Duration	2 days
Training method and provision	Both Physical and Digital or Hybrid, Location is open option, organized ad-hoc Digitally provided over Zoom, Teams or Webex
Evaluation method(s)	Participation, Log analysis exercise, Threat identification exercise, Incident Response exercise
Module overview	Relevant topics: SIEM, Active Directory, Threat Identification & Management. Focal Point's cyber defence exercise is carried out through a SIEM and provides participants a complete view of an active directory environment through extensive monitoring. Detection Engineering querying is performed.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Azure Sentinel, Windows Servers, Linux & Windows terminals

Language	Spoken: English/Greek Material: English Assessment: English
ECTS	-
Certificate of Attendance (CoA)	-
Module enrolment dates	Upon Demand
Other important dates	-

Training Module fields	Training Module information
Code	FP_CSP003
Module name	FP_Training Lab
Module type	Cybersecurity exercise (CS-E)/ Hackathon (H)
Training Provider	Focal Point
Contact	Christos Grigoriadis cgrigor@focalpoint-sprl.be
Level	A
Year – semester – exact dates offered	Upon demand
Duration	2-4 days
Training method and provision	Physical/Virtual
Evaluation method(s)	Participation/questionnaires
Module overview	Relevant topics: Penetration Testing- Active Directory Attacks. The FP Training Lab offers a comprehensive course focused on red teaming, where students are not only taught but also actively engage in performing a variety of realistic attacks. The purpose of this course is to provide hands-on experience and in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber attacks and evaluate an organization's defensive capabilities.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies
Tools to be used	Nmap, bloodhound, hashcat,caldera
Language	Spoken: English Material: English Assessment: English
ECTS	-
Certificate of Attendance (CoA)	No
Module enrolment dates	Upon Demand
Other important dates	-

Training Module fields	Training Module information
Code	FP_CSP004
Module name	HtB_Enterprise_Labs: Introduction To Penetration Testing
Module type	C/W/H
Training Provider	Focal Point

Contact	Christos Grigoriadis cgrigor@focalpoint-sprl.be
Level	B
Year – semester – exact dates offered	Upon Demand
Duration	1-5 days
Training method and provision	Physical/Virtual
Evaluation method(s)	Flag submission system & Leaderboards
Module overview	Penetration Testing Introductory Course. The course covers a vast variety of introductory penetration testing scenarios so that the participants will be able to develop the proper vocabulary and understanding concerning existing attacks.The attacks taught include Injections, LFI/RFI, IDOR, CSRF, XSS, Command Injection, SUID,Priviledge escalation.
Module description	TBA
Knowledge area(s)	1, 2
Tools to be used	Nmap, gobuster, burpsuite, netcat, hydra, nikto, Metasploit,
Language	Spoken: English Material: English Assessment: English
ECTS	-
Certificate of Attendance (CoA)	-
Module enrolment dates	Upon Demand
Other important dates	-

Training Module fields	Training Module information
Code	UPRC_Trustilio_FP_TUC_CSP001
Module name	Maritime Cyber Security Summer School - CyberHot
Module type	Summer School (SS)
Training Provider	UPRC jointly with trustilio, Focal Point, TUC
Contact	Despoina Polemi (dpolemi@gmail.com)
Level	A (Advanced)
Year – semester – exact dates offered	(Summer) 01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Physical
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The "Maritime Cyber Security Summer School - CyberHot" is an immersive and intensive program designed to equip participants with essential knowledge and practical skills in safeguarding maritime systems and infrastructure against cyber threats. Throughout this comprehensive seminar, trainees will delve into the intricate realm of maritime cyber security, exploring the diverse spectrum of threats and attacks that can potentially compromise the safety and functionality of ships and ports. Through hands-on training, participants will learn to identify vulnerabilities, assess risks, and implement mitigation actions, ensuring the resilience of maritime operations in an increasingly digitalized world. Additionally, the program will provide a thorough examination of the legal, standards, and regulatory frameworks governing the maritime industry, enabling trainees to navigate compliance challenges and foster a secure and compliant maritime cyber ecosystem. By the end of the seminar, participants

	will emerge with practical skills and a deep understanding of cyber security tailored specifically to the maritime domain, positioning them as capable guardians of maritime cyber infrastructure.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

3.1.17 INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP (ITML), Greece

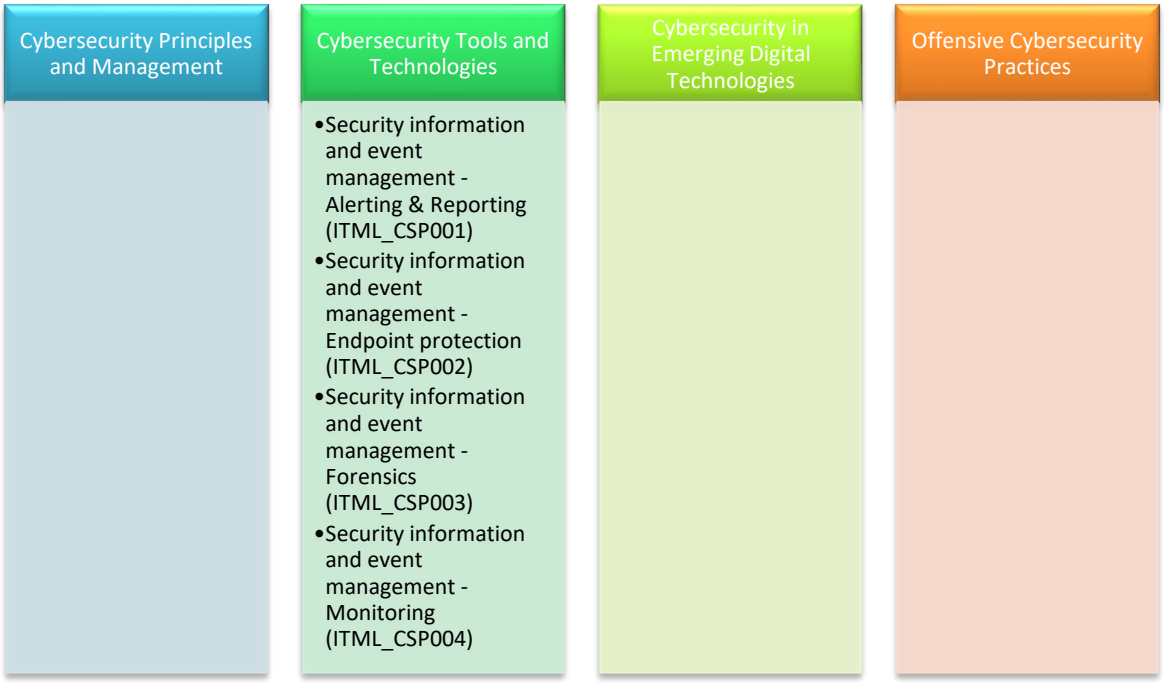

Figure 18. The full overview of ITML's training modules per CSP capability categories

Figure 18 presents the full overview of ITML's training modules per CSP capability categories. The following tables summarize the training modules that ITML is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	ITML_CSP001
Module name	Cybersecurity; Security information and event management - Alerting & Reporting

Module type	S and/or O – demonstration
Training Provider	ITML
Contact	Dimitra Siaili (disiaili@itml.gr)
Level	A
Year – semester – exact dates offered	Two (2) times; Schedule to be defined
Duration	3h
Training method and provision	Virtual
Evaluation method(s)	Virtual testing - Mock exercises and group work
Module overview	Demonstration on how the user (e.g IT service provider) will be notified (email and/or via a slack account) through a a cloud-based manager about malicious activity. In addition, reports will be reported for the systems' status identifying new vulnerabilities with actionable feedback.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Security Infusion
Language	Spoken: English, Greek Material: Slides available, YouTube videos Assessment: User's experimentation and exercises
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	ITML_CSP002
Module name	Cybersecurity; Security information and event management - Endpoint protection
Module type	S and/or O – demonstration
Training Provider	ITML
Contact	Dimitra Siaili (disiaili@itml.gr)
Level	B
Year – semester – exact dates offered	Two (2) times; Schedule to be defined
Duration	2h
Training method and provision	Virtual
Evaluation method(s)	Virtual testing - Mock exercises and group work
Module overview	Demonstration on how via the several Security Infusion agents, the initial data will be collected and evaluated on the edge device through a cloud-based manager.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 7. Cyber Incident Response 8. Network and Communication Security

Tools to be used	Security Infusion
Language	Spoken: English, Greek Material: Slides, YouTube videos Assessment: User's experimentation and exercises
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	ITML_CSP003
Module name	Cybersecurity; Security information and event management - Forensics
Module type	S and/or O – demonstration
Training Provider	ITML
Contact	Dimitra Siaili (disiaili@itml.gr)
Level	A
Year – semester – exact dates offered	Two (2) times; Schedule to be defined – One time Basic, one time Advanced
Duration	3h
Training method and provision	Virtual
Evaluation method(s)	Virtual testing - Mock exercises and group work
Module overview	Demonstration on how to deliver a detailed investigation into historical data in order to find the series of events that caused an incident. In addition, guidelines and methodology will be provided towards efficient activity to restore and secure infrastructure against the identified root cause.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Security Infusion
Language	Spoken: English, Greek Material: Slides, YouTube videos Assessment: User's experimentation and exercises
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	ITML_CSP004
Module name	Cybersecurity; Security information and event management – Monitoring
Module type	S and/or O – demonstration
Training Provider	ITML
Contact	Dimitra Siaili (disiaili@itml.gr)

Level	A
Year – semester – exact dates offered	Two (2) times; Schedule to be defined – One time *Basic*, one time *Advanced*
Duration	3h
Training method and provision	Virtual
Evaluation method(s)	Virtual testing - Mock exercises and group work
Module overview	Demonstration of how to use a cloud-based manager to monitor any critical infrastructure 24x7 through a single dashboard while examining any low-level historical event, if needed.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	Security Infusion
Language	Spoken: English, Greek Material: Slides, YouTube videos Assessment: User's experimentation and exercises
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

3.1.18 MAGGIOLI SPA (MAG), Italy

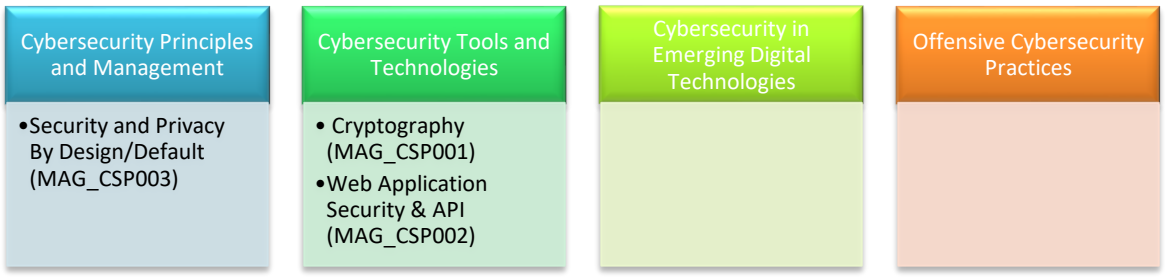

Figure 19. The full overview of MAG's training modules per CSP capability categories

Figure 19 presents the full overview of MAG's training modules per CSP capability categories. The following tables summarize the training modules that MAG is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	MAG_CSP001
Module name	Cryptography
Module type	Seminar (S)
Training Provider	MAG
Contact	Davide Luppoli, Spiros Borotis (spiros.borotis@maggioli.gr)
Level	B (Basic)

Year – semester – exact dates offered	2024 (no further information available)
Duration	3 days
Training method and provision	Physical (Italy, Santarcangelo di Romagna)
Evaluation method(s)	Participation
Module overview	This module introduces the learner to cryptography, presenting the fundamental concepts and illustrating the building blocks and protocols. It avoids mathematical language but puts the learner in a position to use the library BENE, avoiding common errors (such as non-state-of-the-art algorithms, use of ECB or errors in initialization vectors). At the end of the course the Security Champions should be able to validate and possibly optimize the choices already made on their product and use state-of-the-art libraries and methodologies. Additionally, they should be able to parameterize libraries and technologies for their company. Some topics are: • Definition • Kerckhoffs' Principle Avoid security through obscurity • Cryptography attacks • Hashing - MAC - HMAC • Password Hashing • Symmetric Crypt • RSA Asymmetric Critt and elliptic curve • Digital Signature • Key storage and ownership • Key management • Random Numbers (Evaluate) • Choosing a standard • Correct use of encryption - typical mistakes • Some examples of "What can go wrong" • Libraries
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 10. Human Aspects of Cybersecurity
Tools to be used	-
Language	Italian
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	-
Other important dates	-

Training Module fields	Training Module information
Code	MAG_CSP002
Module name	Web Application Security & API
Module type	Seminar (S)
Training Provider	MAG
Contact	Davide Luppoli, Spiros Borotis (spiros.borotis@maggioli.gr)
Level	B (Basic)
Year – semester – exact dates offered	2024 (no further information available)
Duration	5 days

Training method and provision	Physical (Italy, Santarcangelo di Romagna)
Evaluation method(s)	Participation
Module overview	This module introduces the learner to the writing of secure web applications, including both the development and the authentication sides. It also addresses the issue of security in the fundamental components of a web app, from the interface to the server part, with particular attention to microservices. Part 1 - For Dev and Delivery o Main web application vulnerabilities: introduction and testing methods ▪ Injections (sql, command, file…) ▪ Broken authentication & broken access control & session management ▪ Sensitive data exposure ▪ XML external entities ▪ Security misconfiguration ▪ Cross site scripting (XSS) - Reflected & stored ▪ Use of components with known vulnerabilities o Tools per test ▪ Burp ▪ SQL map ▪ Hydra ▪ Dirb/dirbuster/gobuster ▪ Nikto ▪ Wp Scan ▪ No Scan ▪ MonitorPA o Case studies and real tests ▪ On selected applications ▪ Exercises Part 2 - For Dev o Guidelines for developing secure applications ▪ Web applications ▪ Api Rest ▪ Web Services SOAP ▪ Security of authentication and authorization systems o Case studies and real tests ▪ Analysis of real vulnerabilities extracted from DefectDojo and/or SAST system ▪ Exercises
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies
Tools to be used	-
Language	Italian
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	-
Other important dates	-

Training Module fields	Training Module information
Code	MAG_CSP003
Module name	Security and Privacy By Design/Default
Module type	Seminar (S)

Training Provider	MAG
Contact	Davide Luppoli, Spiros Borotis (spiros.borotis@maggioli.gr)
Level	B (Basic)
Year – semester – exact dates offered	2024 (no further information available)
Duration	2 days
Training method and provision	Physical (Italy, Santarcangelo di Romagna)
Evaluation method(s)	Participation
Module overview	This module introduces the learner to the security by design principles. • GDPR regulation • Security by design principles • Data management • Cookies • Anonymisation/pseudonymisation techniques – differences between the two • Database encryption in compliance with the GDPR • DPIA - Need assessment (art.35) • Security in all phases of software development • Definition and basic principles of secure design (least privilege, defense in depth, fail-safe defaults, modularity, encapsulation…) • Definition and adoption of a framework (e.g. Microsoft SDL) • Notes on functional analysis • Threat modeling • Risk assessment • AGID guidelines
Module description	TBA
Knowledge area(s)	8. Network and Communication Security
Tools to be used	-
Language	Italian
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	-
Other important dates	-

3.1.19 PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA (PDMFC), Portugal

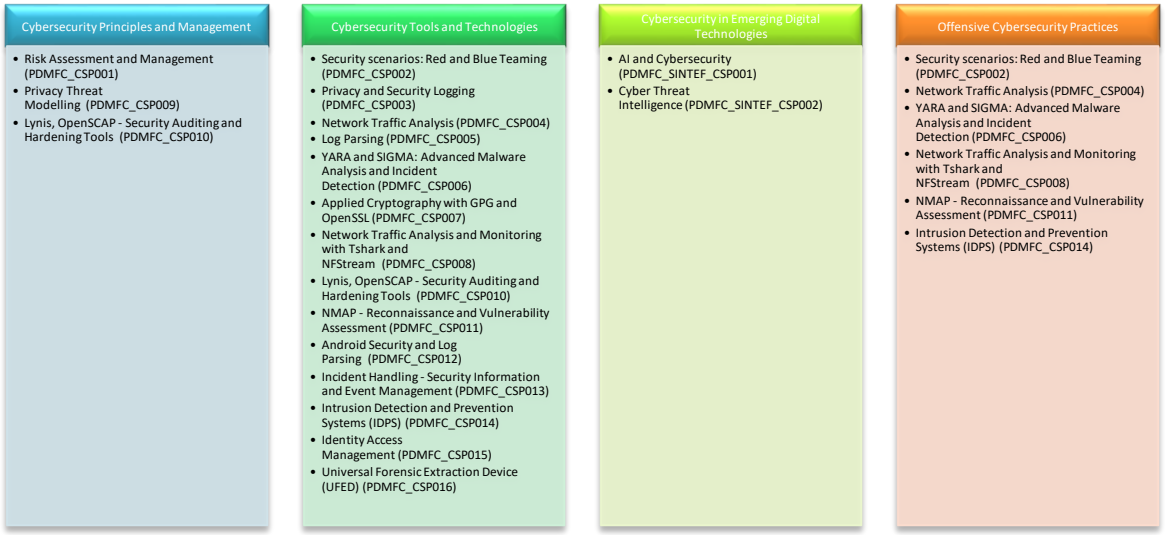

Figure 20. The full overview of PDMFC's training modules per CSP capability categories

Figure 20 presents the full overview of PDMFC's training modules per CSP capability categories. The following tables summarize the training modules that PDMFC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	PDMFC_CSP001
Module name	Risk Assessment and Management
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Provides comprehensive knowledge and practical skills for identifying, evaluating, and mitigating security risks. Through methodologies and frameworks, case studies, the course fosters an understanding of risk assessment methodologies, compliance requirements, and the development of robust security plans.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	eRamba, SimpleRisk
Language	English, Greek, Portuguese

ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP002
Module name	Security scenarios: Red and Blue Teaming
Module type	C, S, CS-E, and H
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	A
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours), H (1hr – 2 days)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Engage in Red and Blue Teaming roles, allowing them to act as both attackers and defenders to comprehensively grasp security vulnerabilities and mitigation strategies. On the Red Team side, students simulate cyberattacks, exploiting vulnerabilities ethically. Meanwhile, the Blue Team segment focuses on using Wazuh for real-time threat detection, analysis, and incident response. Hands-on exercises, case studies, and simulated scenarios enable practical learning.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	Wazuh, Suricata, Nmap, Hydra, hping, Metasploit
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP003
Module name	Privacy and Security Logging
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B

Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Privacy and security logging is the systematic recording and monitoring of events in information systems to protect sensitive data and uphold privacy regulations. It involves continuous monitoring of activities, data protection, incident response, compliance demonstration, alerting, secure log storage, and anonymization when necessary. These logs are vital for identifying and addressing security threats, ensuring data privacy, and complying with industry standards and regulations. They serve as forensic evidence during investigations and enable organizations to maintain robust cybersecurity and privacy practices while effectively managing and securing their digital assets. Log parser is provided by PDMFC for effective log analysis.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 9. Privacy and Data Protection
Tools to be used	Chimera, Metago, Chidroid
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP004
Module name	Network Traffic Analysis
Module type	C and S
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Wireshark is a versatile network analysis tool that enables professionals to inspect, capture, and analyze network traffic. It offers detailed packet inspection, protocol analysis, and is invaluable for security monitoring and threat detection.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 9. Privacy and Data Protection
Tools to be used	Wireshark, Tshark, Netcat

Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP005
Module name	Log Parsing
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	A
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Learn to extract valuable insights and critical information from log data generated by applications, systems, and networks. The course covers techniques for efficiently processing large volumes of logs, identifying anomalies, and detecting security incidents.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 6. Cybersecurity Policy, Process, and Compliance 7. Cyber Incident Response
Tools to be used	Metago, ELK Beats
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP006
Module name	YARA and SIGMA: Advanced Malware Analysis and Incident Detection
Module type	C and S, CS-E, H
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)

Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Master YARA, a robust approach for creating and refining custom rules to identify and classify malware effectively. Additionally, they will gain expertise in SIGMA, a versatile framework for developing detection rules to pinpoint security incidents proactively.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	YARA, SIGMA, VirusTotal
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP007
Module name	Applied Cryptography with GPG and OpenSSL
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Participants will learn the essential techniques of encryption, digital signatures, and secure communication, with a focus on hands-on experience. Key course components include configuring and utilizing GPG and OpenSSL for various encryption tasks, cryptographic key management, secure file sharing, email encryption, and web communication security.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	GPG, OpenSSL
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP008
Module name	Network Traffic Analysis and Monitoring with Tshark and NFStream
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	A
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Provides comprehensive training in network traffic analysis and monitoring techniques using Tshark and NFStream tools. Participants learn to capture, dissect, and analyze network packets and flow data, gaining insights into traffic patterns, security threat detection, and network performance optimization.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 7. Cyber Incident Response 8. Network and Communication Security
Tools to be used	NFStream, Wireshark, Tshark
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP009
Module name	Privacy Threat Modelling
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	A
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Offers a structured approach to understanding and mitigating risks to individual privacy within various systems and environments. Participants learn to identify sensitive data, assess data processing activities, and uncover potential threats that may compromise privacy.
Module description	TBA

Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 10. Human Aspects of Cybersecurity
Tools to be used	LINDDUN, MS Threat Modeling Tool
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP010
Module name	Lynis, OpenSCAP - Security Auditing and Hardening Tools
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	A
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Participants will learn to conduct thorough security audits using Lynis to assess vulnerabilities, security configurations, and compliance with best practices. Additionally, the course covers the utilization of OpenSCAP for automated security compliance checks and policy enforcement.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	Lynis, OpenSCAP, Wazuh
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP011
Module name	NMAP - Reconnaissance and Vulnerability Assessment
Module type	C and S, CS-E
Training Provider	PDMFC

Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Participants will learn to conduct network scans, discover devices and services, and assess potential vulnerabilities within target networks. Key components of the course include mastering NMAP for network discovery, service enumeration, and vulnerability assessment, along with advanced scanning techniques.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 5. Cybersecurity Risk Management 8. Network and Communication Security
Tools to be used	Nmap, OpenVAS, Nessus
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP012
Module name	Android Security and Log Parsing
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Participants gain knowledge and practical skills to assess and enhance the security of Android devices and applications. Key components include understanding Android security fundamentals, utilizing log parsing for threat detection, and implementing security best practices for app development and device management.
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 7. Cyber Incident Response 9. Privacy and Data Protection
Tools to be used	Chidroid, Android Debug Bridge, Mobile Security Framework (MobSF)
Language	English, Greek, Portuguese
ECTS	-

Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP013
Module name	Incident Handling - Security Information and Event Management
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Provides knowledge and practical skills to efficiently manage security incidents through SIEM tools. The course covers incident handling fundamentals, SIEM implementation for threat detection and log analysis, and incident response strategy development.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 7. Cyber Incident Response
Tools to be used	Metadon, Wazuh
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP014
Module name	Intrusion Detection and Prevention Systems (IDPS)
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Learn about network intrusion detection systems and prevention techniques. Participants learn to recognize and categorize security threats, operate and

	configure IDPS technologies, and monitor network traffic and system activities in real-time. They become proficient in configuring alert mechanisms, generating reports, and responding to security incidents, including incident investigation and mitigation.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 7. Cyber Incident Response
Tools to be used	Metadon, Wazuh
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP015
Module name	Identity Access Management
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Managing user identities and access control within an organization's digital environment. Topics include user identity management, access control principles, authentication, and authorization methods, as well as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) solutions. The course covers directory services, access policies, and governance, along with identity lifecycle management and federated identity.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	SPA (PDMFC), Keycloak
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_CSP016
Module name	Universal Forensic Extraction Device (UFED)
Module type	C and S, CS-E
Training Provider	PDMFC
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com)
Level	B
Year – semester – exact dates offered	TBD
Duration	C (3-6 Months), S (1-3 Hours)
Training method and provision	Both (Physical: Corfu Greece, Lisboa Portugal)
Evaluation method(s)	Participation and exercises
Module overview	Digital forensics within cybersecurity, emphasizing the pivotal role of UFED (Universal Forensic Extraction Device). Commercial tools like Cellebrite and open-source tools like Kuiper extend UFED's capabilities by introducing advanced data analysis and visualization, enhancing data interpretation and pattern recognition. A tool from PDM (Chimera/Metago), will be used for forensic data collection and distribution. Establish a strong foundation in digital forensics principles, encompassing ethical and legal considerations, evidence collection methodologies, and the critical importance of preserving evidence integrity.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 7. Cyber Incident Response
Tools to be used	Cellebrite, Kuiper, Sysmon, The Sleuth Kit
Language	English, Greek, Portuguese
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_SINTEF_CSP001
Module name	AI and Cybersecurity
Module type	Seminar (S)
Training Provider	PDMFC (jointly with SINTEF)
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com) Nektaria Kaloudi (nektaria.kaloudi@sintef.no)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Both

Evaluation method(s)	Participation and exercises
Module overview	The module explores the reciprocal influence of AI and cybersecurity. It will cover the three dimensions in which AI and cybersecurity intersect, covering both challenges and opportunities from the offensive and defensive aspects. Examples will include adversary penetration testing and emerging challenges of adversarial AI through a blend of theoretical and practical exercises. It covers various facets of this intersection, including adversary penetration testing, intrusion detection systems (IDS), Security Information and Event Management (SIEM) systems, and the emerging challenge of adversarial AI. Through a blend of theoretical knowledge and practical exercises, students gain a comprehensive understanding of how AI can be applied defensively and offensively in cybersecurity, with a focus on building expertise in AI-driven penetration testing, enhancing IDS and SIEM with AI, and defending against adversarial AI attacks.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 8. Network and Communication Security
Tools to be used	NFStream, Wireshark, Tshark, Python, Tensorflow, PySyft
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

Training Module fields	Training Module information
Code	PDMFC_SINTEF_CSP002
Module name	Cyber Threat Intelligence
Module type	Seminar (S)
Training Provider	PDMFC (jointly with SINTEF)
Contact	Stylianos Karagiannis (stylianos.karagiannis@pdmfc.com) Nektaria Kaloudi (nektaria.kaloudi@sintef.no)
Level	B
Year – semester – exact dates offered	TBD
Duration	TBD
Training method and provision	Both
Evaluation method(s)	Participation and exercises
Module overview	Comprehensive exploration of the core principles and practical applications of cyber threat intelligence. It equips students with a deep understanding of threat identification, threat actor analysis, and motives. The module emphasizes hands-on training with industry-standard tools, including STIX and TAXII for structured threat information sharing and security, OpenCTI for effective threat intelligence management and integration, and MISP for structured threat data sharing. Depending on scenarios within the sectors (e.g., health, energy, maritime), the module will show the integration of the TORC tool with cyber threat intelligence-based cybersecurity trainings and best practices in a way that

	enhances stakeholders' resilience and adaptability in the face of cyber threats.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 7. Cyber Incident Response
Tools to be used	STIX, TAXII, OpenCTI, and MISP, Digital TORC
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	TBD
Other important dates	TBD

3.1.20 SOCIAL ENGINEERING ACADEMY (SEA), Germany

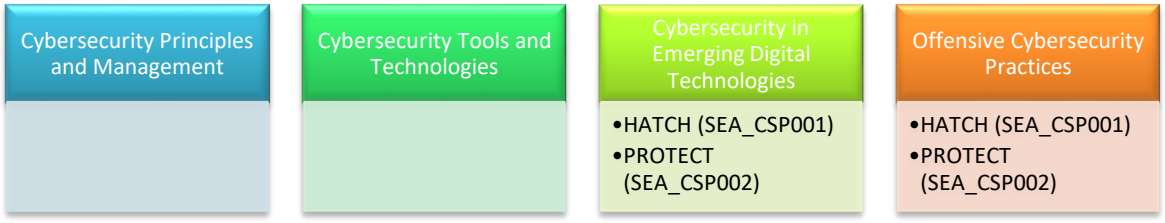

Figure 21. The full overview of SEA's training modules per CSP capability categories

Figure 21 presents the full overview of SEA's training modules per CSP capability categories. The following tables summarize the training modules that SEA is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	SEA_CSP001
Module name	HATCH
Module type	Seminar (S) or Cybersecurity exercise (CS-E)
Training Provider	SEA
Contact	sebastian.pape@social-engineering.academy
Level	B
Year – semester – exact dates offered	Not yet aligned. We are not offering the training on a regular schedule but on demand by customers.
Duration	Needs to be aligned. A minimum of 2 hours is needed. 3 to 4 hours would be optimal.
Training method and provision	Physical
Evaluation method(s)	Participation
Module overview	Social Engineering. A serious game where players will be in the role of an attacker and apply social engineering attacks in a virtual scenario. The game offers the most common social engineering attacks, psychological principles and a game plan with virtual personas. Based on the social engineering attack

	cards and the social principle cards the player drew, players need to come of with attacks on the personas in the game. If needed (depending on the knowledge of the players), an introduction to social engineering can be given before. According to our work plan, the scenario will be from the energy sector. Other scenarios (e.g. maritime) would be available as well or are under development (health) if needed.
Module description	TBA
Knowledge area(s)	10. Human Aspects of Cybersecurity
Tools to be used	HATCH, the serious card/board game developed by us
Language	Spoken: English or German Material: English or German Assessment:%
ECTS	%
Certificate of Attendance (CoA)	Yes
Module enrolment dates	Needs to be aligned
Other important dates	

Training Module fields	Training Module information
Code	SEA_CSP002
Module name	PROTECT
Module type	Cybersecurity exercise (CS-E)
Training Provider	SEA
Contact	sebastian.pape@social-engineering.academy
Level	B
Year – semester – exact dates offered	Not yet aligned. We are not offering the game on a regular schedule but on demand by customers.
Duration	Depends on player, for the first game around 20 minutes should be planned. Follow-up games can be done in a shorter time since the player will be familiar with the rules
Training method and provision	Virtual
Evaluation method(s)	Participation in the virtual game
Module overview	Social Engineering. A serious game where players will be need to defend against social engineering attacks in a virtual card game. A demo with only limited cards can be found here: https://demo.protect.social-engineering.academy/en/ The cards can be customized and adapted to a certain training as long as they follow the pattern that they come in attack/defense pairs. According to our work plan, the scenario will be from the energy sector. Other scenarios (e.g. maritime) would be available as well or are under development (health) if needed.
Module description	TBA
Knowledge area(s)	10. Human Aspects of Cybersecurity
Tools to be used	PROTECT, a virtual serious card game developed by us
Language	Material: English or German Assessment:%
ECTS	%
Certificate of Attendance (CoA)	Yes
Module enrolment dates	Needs to be aligned

Other important dates	

3.1.21 SERIOUS GAMES INTERACTIVE APS (SGI), Denmark

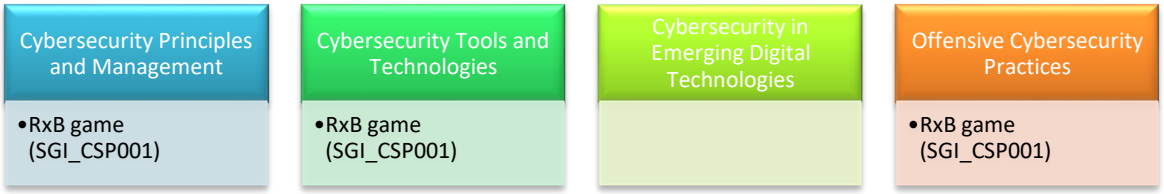

Figure 22. The full overview of SGI's training modules per CSP capability categories

Figure 22 presents the full overview of SGI's training modules per CSP capability categories. The following tables summarize the training modules that SGI is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	SGI_CSP001
Module name	RxB game
Module type	C, W, SS
Training Provider	Serious Games Interactive A/S
Contact	mba@seriousgames.net
Level	B
Year – semester – exact dates offered	All year available online game
Duration	45min
Training method and provision	Physical & virtual
Evaluation method(s)	Multiple choice Questionnaire
Module overview	As the manager of a team of tech savvy individuals your aim is to assess, identify and manipulate a networked systems security in order to win over an opponent who is directly trying to prevent you in this. Red can train hackers and use an arsenal of offensive tools to complete their objectives. Blue on the other hand has to balance resources, employee training, and close vulnerability gaps before red discovers them. No practical technical skill is required to play, however, it helps to know about cybersecurity terminology and concepts - if not, you will learn by failing. Main learning objectives: • Risk assessment, prioritisation and resource management • Recognize the many different types of vulnerabilities • Various attack vectors and strategies • Various defensive mitigations and strategies RxB aims to deliver more awareness within the following areas: • Cyber security defences require regular adjustment • Promote Situation awareness by navigating through an active attack • Familiarisation with Hacker- and Cyber-Defence-terminology
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management

	4. Cybersecurity Threat Management 10. Human Aspects of Cybersecurity
Tools to be used	No special tools apart from an internet browser with an internet connection
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

3.1.22 SECURITY LABS CONSULTING LIMITED (SLC), Ireland

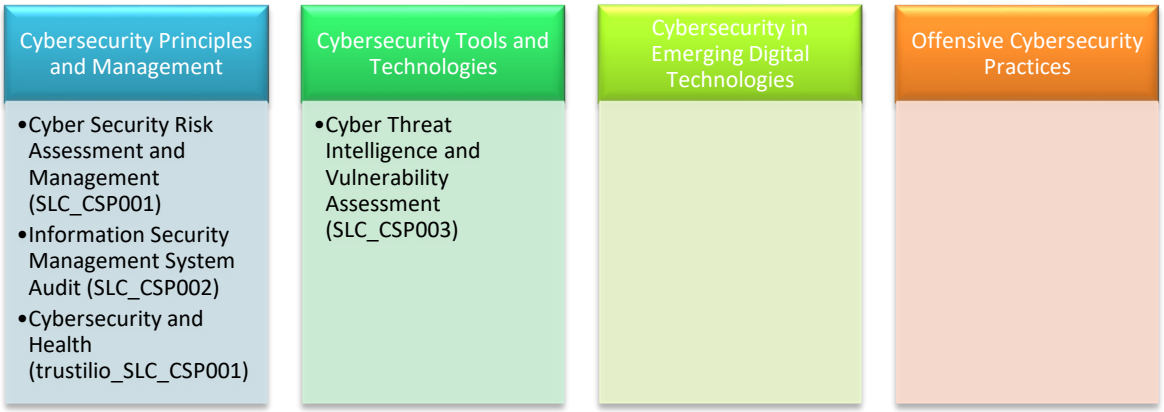

Figure 23. The full overview of SLC's training modules per CSP capability categories

Figure 23 presents the full overview of SLC's training modules per CSP capability categories. The following tables summarize the training modules that SLC is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	SLC_CSP001
Module name	Cyber Security Risk Assessment and Management
Module type	Course (C), Workshop (W), Cybersecurity exercise (CS-E)
Training Provider	SLC
Contact	Shareeful Islam shareeful.islam@securitylabs.ie Athina Labropoulou athina.labropoulou@securitylabs.ie
Level	B (Basic), / A (Advanced) Dependent on learner requirements
Year – semester – exact dates offered	September to December or April to June
Duration	
Training method and provision	Both
Evaluation method(s)	Summative assessment with multiple choice question and risk management scenario-based exercise.
Module overview	The module aims to provide an understanding of the underlying principles associated with the cyber security risk assessment and management. It facilitates the learner with the ability to identify the assets and their

	dependencies within cyber system and critically evaluate the protection mechanisms used to enhance the security and resilience of context. It also offers an automated tool to implement the risk assessment and management activities for improving overall security. This course covers a number of topics to provide learners understanding about the cybersecurity risk management • Security concept • Asset and system modelling • Vulnerability and threat identification • Risk management frameworks, qualitative and quantitative risk assessment • Risk treatment, monitoring and risk evolution • Business continuity and contingency planning Key functionalities of the tools to support the course • Asset identification and visual representation • Cyber threat management and attack scenario generation • Individual and cascading risk assessment and reporting
Module description	TBA
Knowledge area(s)	5. Cybersecurity Risk Management
Tools to be used	SLC's Risk Assessment and Management Platform
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	SLC_CSP002
Module name	Information Security Management System Audit
Module type	Course (C)
Training Provider	SLC
Contact	Shareeful Islam shareeful.islam@securitylabs.ie
Level	B (Basic), / A (Advanced) Dependent on learner requirements
Year – semester – exact dates offered	September to December or April to June
Duration	
Training method and provision	Both
Evaluation method(s)	Summative assessment based on internal audit by following ISO 27001.
Module overview	The module aims to practical experience of auditing information systems for adequate information security based on industry specific standards. It facilitates understanding ISO 27001 key objectives and related audit check list. This course covers a number of topics to provide learners understanding about the information security management system audit • Information security objective • Information security management system standard ISO 27001 • Information security management system audit process

	• Audit report and checklist
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 6. Cybersecurity Policy, Process, and Compliance
Tools to be used	ISO 27001 audit check list
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	SLC_CSP003
Module name	Cyber Threat intelligence and vulnerability assessment
Module type	Workshop
Training Provider	SLC
Contact	Shareeful Islam shareeful.islam@securitylabs.ie
Level	B (Basic)
Year – semester – exact dates offered	September to December or April to June
Duration	
Training method and provision	Both
Evaluation method(s)	Summative assessment based on assessing vulnerability and threat intelligence extraction
Module overview	The module aims to provide learners with an overview of the threat intelligence and vulnerabilities assessment relating with the threats. It allows the learners to carry on a vulnerability assessment and capability for writing a technical report of the vulnerability and threat intelligence. This course covers a number of topics to provide learners understanding about the threat intelligence and vulnerability assessment • Cyber threat taxonomies and threat intelligence information • Threat modelling • Threat feed • Vulnerabilities database • Common vulnerabilities scoring system • Threat intelligence reporting
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management
Tools to be used	Virustotal, Phishtank, Threatminer, Mozilla observatory, Threatfeeds, Malware bazaar, CVSS v4.0 calculator
Language	English
ECTS	
Certificate of Attendance (CoA)	
Module enrolment dates	

Other important dates	

Training Module fields	Training Module information
Code	Trustilio_SLC_CSP001
Module name	Cybersecurity and Health
Module type	Seminar
Training Provider	Trustilio jointly with SLC
Contact	Kitty Kioskli (kitty.kioskli@trustilio.com) Shareeful Islam (shareeful.islam@securitylabs.ie)
Level	Basic
Year – semester – exact dates offered	01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Virtual
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	In" Cybersecurity and Health" seminar where we will delve into the critical intersection of cybersecurity and healthcare. We will cover essential topics such as the evolving threat landscape, vulnerabilities in medical devices, regulatory compliance, practical strategies for healthcare institutions, and the human element in cybersecurity. Through informative sessions, real-world case studies, and expert insights, attendees will gain a comprehensive understanding of the challenges and opportunities in securing health data and infrastructure, ensuring they leave with practical knowledge to enhance cybersecurity in the healthcare sector.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

3.1.23 TRUSTILIO BV (TRUSTILIO), Netherlands

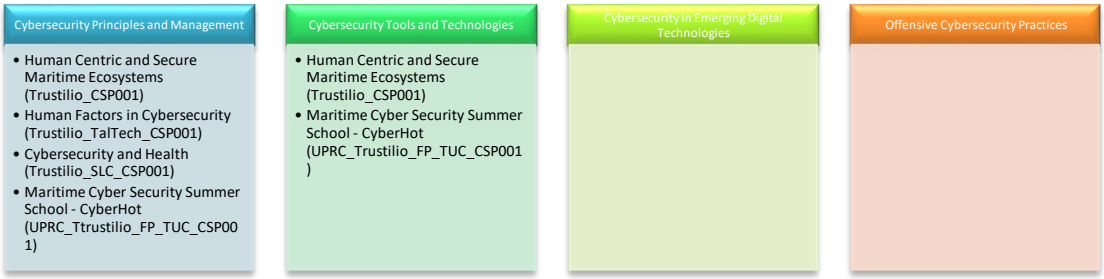

Figure 24. The full overview of Trustilio's training modules per CSP capability categories

Figure 24 presents the full overview of Trustilio's training modules per CSP capability categories. The following tables summarize the training modules that Trustilio is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	Trustilio_CSP001
Module name	Human Centric and Secure Maritime Ecosystems
Module type	Seminar
Training Provider	Trustilio
Contact	Maria Lambrou (mariaatlambrou@gmail.com)
Level	Advanced
Year – semester – exact dates offered	01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Virtual
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The seminar "Human-Centric and Secure Maritime Ecosystems" offers a comprehensive exploration of the multifaceted dynamics within the maritime industry, emphasizing a human-centric approach to maritime operations and security. This interdisciplinary seminar delves into the complexities of maritime ecosystems, addressing the unique challenges posed by technological advancements, environmental concerns, and global security issues. Trainees will gain a deep understanding of the critical role played by human factors, maritime technologies, and regulatory frameworks in shaping the industry. Moreover, the seminar equips learners with the knowledge and skills necessary to design and implement secure, resilient, and sustainable maritime systems, ensuring the safety and well-being of both maritime professionals and the environment. Through a blend of theoretical insights and practical applications, trainees will be prepared to navigate the evolving landscape of maritime operations, security, and sustainability.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A

Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

Training Module fields	Training Module information
Code	Trustilio_SLC_CSP001
Module name	Cybersecurity and Health
Module type	Seminar
Training Provider	Trustilio jointly with SLC
Contact	Kitty Kioskli (kitty.kioskli@trustilio.com) Shareeful Islam (shareeful.islam@securitylabs.ie)
Level	Basic
Year – semester – exact dates offered	01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Virtual
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	In" Cybersecurity and Health" seminar where we will delve into the critical intersection of cybersecurity and healthcare. We will cover essential topics such as the evolving threat landscape, vulnerabilities in medical devices, regulatory compliance, practical strategies for healthcare institutions, and the human element in cybersecurity. Through informative sessions, real-world case studies, and expert insights, attendees will gain a comprehensive understanding of the challenges and opportunities in securing health data and infrastructure, ensuring they leave with practical knowledge to enhance cybersecurity in the healthcare sector.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

Training Module fields	Training Module information
Code	Trustilio_TalTech_CSP001
Module name	Human Factors in Cybersecurity
Module type	Seminar
Training Provider	Trustilio jointly with TalTech
Contact	Kitty Kioskli (kitty.kioskli@trustilio.com) Ricardo Gregorio Lugo (ricardo.lugo@taltech.ee)
Level	Basic

Year – semester – exact dates offered	01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Virtual
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The seminar on Human Factors in Cybersecurity offers a comprehensive exploration of the intricate relationship between human cognitive and behavioral dynamics and the realm of cybersecurity. This seminar provides an in-depth analysis of the psychological, sociological, and cognitive factors that underpin individuals' interactions with digital systems, and subsequently shape the efficacy of cybersecurity protocols. Through a meticulous examination of empirical research and pertinent case studies, attendees will scrutinize the psychological mechanisms that underlie susceptibility to phishing attacks, the challenges posed by user authentication processes, and the cognitive decision-making paradigms during cyber incidents. By fostering a nuanced comprehension of human factors, participants will acquire the expertise necessary to engineer user-centric interfaces, formulate targeted training regimens, and deploy strategies tailored to enhance user compliance and overall cybersecurity robustness. The seminar offers a platform to navigate the intricate terrain of human-centric cybersecurity, contributing to the fortification of the digital domain.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

Training Module fields	Training Module information
Code	UPRC_Trustilio_FP_TUC_CSP001
Module name	Maritime Cyber Security Summer School - CyberHot
Module type	Summer School (SS)
Training Provider	UPRC jointly with Trustilio, Focal Point, TUC
Contact	Despoina Polemi (dpolemi@gmail.com)
Level	A (Advanced)
Year – semester – exact dates offered	(Summer) 01.02.2024-31.07.2024
Duration	1 day
Training method and provision	Physical
Evaluation method(s)	Virtual tests, participation, workshops, bonus tasks, assignments
Module overview	The "Maritime Cyber Security Summer School - CyberHot" is an immersive and intensive program designed to equip participants with essential knowledge and practical skills in safeguarding maritime systems and infrastructure against cyber threats. Throughout this comprehensive seminar, trainees will delve into the intricate realm of maritime cyber security, exploring the diverse spectrum of threats and attacks that can potentially compromise the safety and

	functionality of ships and ports. Through hands-on training, participants will learn to identify vulnerabilities, assess risks, and implement mitigation actions, ensuring the resilience of maritime operations in an increasingly digitalized world. Additionally, the program will provide a thorough examination of the legal, standards, and regulatory frameworks governing the maritime industry, enabling trainees to navigate compliance challenges and foster a secure and compliant maritime cyber ecosystem. By the end of the seminar, participants will emerge with practical skills and a deep understanding of cyber security tailored specifically to the maritime domain, positioning them as capable guardians of maritime cyber infrastructure.
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	English
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	N/A
Other important dates	N/A

3.1.24 ZELUS IKE (ZELUS), Greece

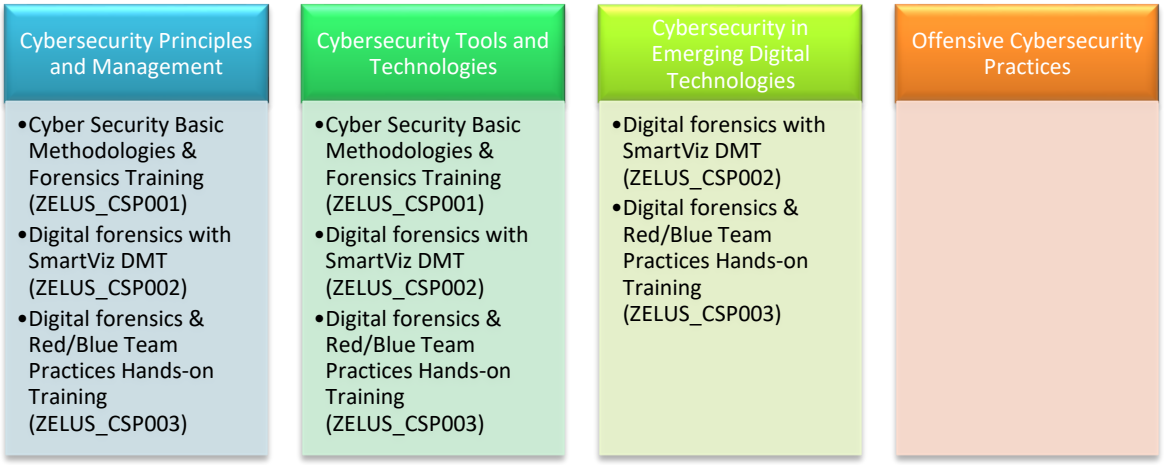

Figure 25. The full overview of Zelus's training modules per CSP capability categories

Figure 25 presents the full overview of Zelus's training modules per CSP capability categories. The following tables summarize the training modules that Zelus is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	ZELUS_CSP001
Module name	Cyber Security Basic Methodologies & Forensics Training

Module type	Course (C), Workshop (W), Cybersecurity exercise (CS-E)
Training Provider	Zelus P.C
Contact	Stella Markopoulou s.markopoulou@zelus.gr Christos Kargatzis c.kargatzis@zelus.gr
Level	B (Basic)
Year – semester – exact dates offered	-
Duration	4hrs
Training method and provision	Physical and/or Distantly
Evaluation method(s)	participation
Module overview	Course ZELUS_CSP001 is designed to immerse participants in a practical cybersecurity environment through a straightforward cybersecurity training program. The training employs a Red Team/Blue Team exercise, where the Red Team, consisting of offensive security experts, attempts to breach an organization's cybersecurity defenses, while the Blue Team defends against and counteracts these attacks. The focus of this training is on the Blue Team perspective, emphasizing digital forensics methodologies to enhance defense strategies. (https://www.zelus.gr/training-modules/)
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security 10. Human Aspects of Cybersecurity
Tools to be used	Nmap, elasticsearch , HTML5, CSS3, JavaScript
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	ZELUS_CSP002
Module name	Digital forensics with SmartViz DMT
Module type	Course (C), Seminar (S)
Training Provider	Zelus P.C
Contact	Stella Markopoulou s.markopoulou@zelus.gr Christos Kargatzis c.kargatzis@zelus.gr
Level	B(Basic)
Year – semester – exact dates offered	-
Duration	2h
Training method and provision	Physical and/or Distantly
Evaluation method(s)	-
Module overview	This course endeavors to provide users with a practical demonstration of SmartViz DMT, showcasing its functionalities in crucial cybersecurity domains including endpoint security, security training, reporting, security-focused design, and the detection of data manipulation. Additionally, it offers an in-depth exploration of SIEM (Security Information and Event

	Management) and its operational methods through digital forensics analysis. In terms of design, the tool adopts a security-centric approach, prioritizing principles like confidentiality, integrity, and availability. This approach ensures that the tool is resilient against potential attacks, promoting secure design practices throughout its implementation. (https://www.zelus.gr/training-modules/)
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security
Tools to be used	Nmap, elasticsearch , HTML5, CSS3, JavaScript
Language	English
ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	
Other important dates	

Training Module fields	Training Module information
Code	ZELUS_CSP003
Module name	Digital forensics & Red/Blue Team Practices Hands-on Training
Module type	Workshop (W), Summer School (SS), Cybersecurity exercise (CS-E)
Training Provider	Zelus P.C
Contact	Stella Markopoulou s.markopoulou@zelus.gr Christos Kargatzis c.kargatzis@zelus.gr
Level	A (Advanced)
Year – semester – exact dates offered	-
Duration	5h
Training method and provision	Physical and/or Distantly
Evaluation method(s)	exercises
Module overview	This course offers a practical encounter with a Red Team/Blue Team exercise, wherein the Red Team consists of offensive security experts endeavoring to breach the cybersecurity defenses of a given subject. Simultaneously, the Blue Team is responsible for defending against and responding to the attacks launched by the Red Team. The primary objective of this exercise is to tackle key issues, including identifying misconfigurations and coverage gaps in existing security products, enhancing network security to detect targeted attacks and reduce response time, raising awareness among participants about human vulnerabilities that could compromise system security, and developing the skills and maturity of the training group's security capabilities within a secure, low-risk training environment. (https://www.zelus.gr/training-modules/)
Module description	TBA
Knowledge area(s)	1.Penetration Testing 2.Cybersecurity Tools and Technologies 3.Cybersecurity Management 4.Cybersecurity Threat Management 8.Network and Communication Security
Tools to be used	TBA
Language	English

ECTS	-
Certificate of Attendance (CoA)	TBD
Module enrolment dates	
Other important dates	

3.1.25 UNIVERSIDADE NOVA DE LISBOA (FCT), Portugal

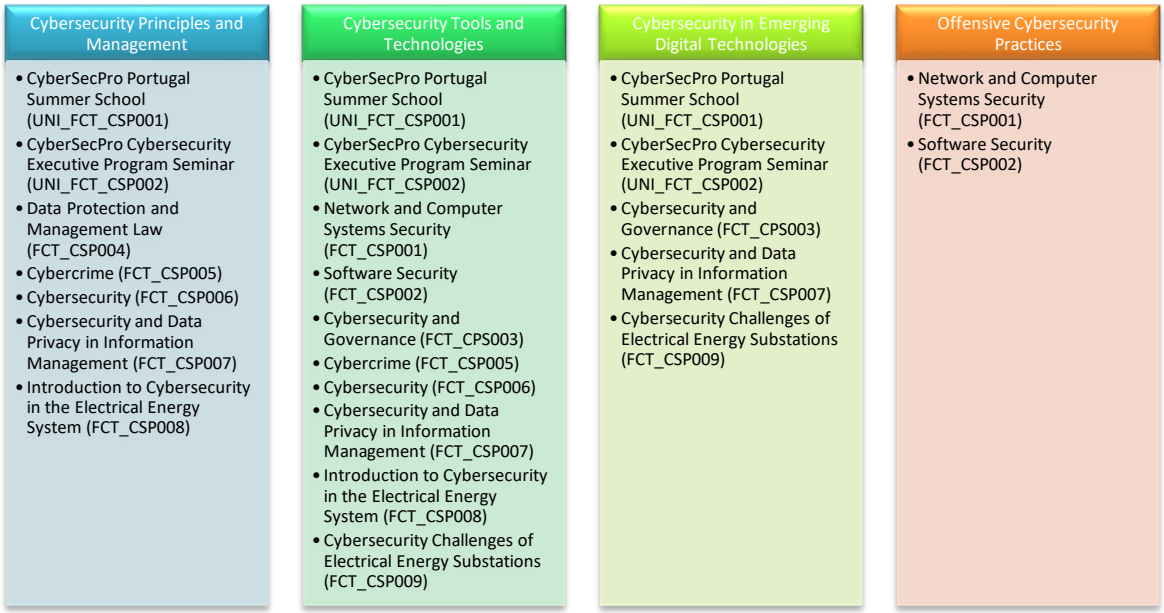

Figure 26. The full overview of FCT's training modules per CSP capability categories

Figure 26 presents the full overview of FCT's training modules per CSP capability categories. The following tables summarize the training modules that FCT is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	FCT_CSP001
Module name	Network and Computer Systems Security
Module type	C – Course
Training Provider	FCT (Department of Informatics)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	Every first semester
Duration	3-4 months
Training method and provision	Physical at FCT campus (NOVA School of Science and Technology, 2829-516 Caparica, Portugal)
Evaluation method(s)	Physical written examination, course frequency, and exercises (mini-projects)
Module overview	Networks and Computer Systems Security Fundamentals Applied Computational Cryptography and Cryptographic Tools Authentication and Access Control TCP/IP Stack Security

	Systems Security (https://guia.unl.pt/en/2019/fct/program/935/course/11619)
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the first semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP002
Module name	Software Security
Module type	C – Course
Training Provider	FCT (Department of Informatics)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	Every first semester
Duration	3-4 months
Training method and provision	Physical at FCT campus (NOVA School of Science and Technology, 2829-516 Caparica, Portugal)
Evaluation method(s)	Physical written examination, course frequency, and exercises
Module overview	1. Software Security Concepts. Security Properties. Threat and Attacker Modelling. How to express security properties and policies. Security Properties as System Invariants. 2. Principles of Secure Software Design. Basic principles (Least Privilege; Fail-Safe Defaults; Economy of Mechanism; Complete Mediation; Separation of Duties; Least Common Mechanism), and how they map into programming / architectural concepts. Preserving security across modules and trust maintenance: some basic techniques. 3. Authorization. Authorization and Access control models. Access control policies and rules. General languages and frameworks for expressing and enforcing authorization. Signatures and certificates. Language-Based authorization security: Authorization in runtime support systems, Stack inspection, Proof carrying code, signed code (Java). Permissions and object-capability models (Google Caja). 4. Information Flow. Security Lattices. Non-interference. Declassification. Covert Channels and indirect flows. (Sand)boxing and Tainting. Reference Monitors. Language-based information flow security: Data Flow analysis. Type-based analysis. Tainting. Paragon - Java, JSFlow - JavaScript. 5. Domain Specific Security Threats. Two sample scenarios: Web Applications (code injection, cross-site scripting, cross-site request forgery,

	and session hijacking). Unsafe Languages (exploiting unsafety to violate integrity – buffer overruns, stack smashing). Countermeasures to sample threats using general principles and techniques (information flow, capabilities, tanting, monitors). 6. Data Security and Provenance. Schema oriented security and row oriented security. Access Control in Data Models. Database inference. Balancing privacy and utility; statistical database security; k-anonymity; differential privacy, privacy languages. Provenance models and languages. (https://guia.unl.pt/pt/2019/fct/program/935/course/11553)
Module description	TBA
Knowledge area(s)	1. Penetration Testing 2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the first semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP003
Module name	Cybersecurity and Governance
Module type	C – Course
Training Provider	FCT (NOVA School of Law)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	First semester
Duration	3-4 months
Training method and provision	Physical at NOVA School of Law (NOVA School of Law, Campus de Campolide. 1099-032 Lisboa, Portugal)
Evaluation method(s)	Physical written examination and course frequency
Module overview	1. Introduction: Information, Information 2. Hackers, Crackers e other outlaws in Cyberspace 3. Cyberspace Regulation 4. Fight against Cybercrime 5. Incident response and Cybersecurity crisis management 6. Other public policies 7. Algorithms and future technologies (https://guia.unl.pt/en/2023/fd/program/M863/course/36121)
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management

	6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the first semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP004
Module name	Data Protection and Management Law
Module type	C – Course
Training Provider	FCT (NOVA School of Law)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	Second semester
Duration	3-4 months
Training method and provision	Physical at NOVA School of Law (NOVA School of Law, Campus de Campolide. 1099-032 Lisboa, Portugal)
Evaluation method(s)	Physical written examination, course frequency, and report
Module overview	1. The rights to privacy and data protection: Contextualization of these rights in European law 2. The GDPR: legal background and practical application 3. Critical assessment of the GDPR (https://guia.unl.pt/en/2022/fd/program/M863/course/37035)
Module description	TBA
Knowledge area(s)	9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the second semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP005
Module name	Cybercrime

Module type	O – Other (Postgraduate program)
Training Provider	FCT (NOVA School of Law)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	Second semester
Duration	3-4 months
Training method and provision	Physical at NOVA School of Law (NOVA School of Law, Campus de Campolide. 1099-032 Lisboa, Portugal)
Evaluation method(s)	Course frequency, mid-term exercise, and essay
Module overview	• Threats in the online environment • Cybercrime typologies • Cyber-criminology: Why cybercrime occurs; why people are victimized by criminals in the cyberspace • Financial crime in online settings (e.g., cyber extortion; online fraud; money laundering by means of cryptocurrency) • Cyber-terrorism (with an emphasis of terrorist financing) • Attacks against information systems • The transition from electronic to AI-generated evidence • Automation in law enforcement settings • Algorithmic criminal justice • Cyber-security: technical solutions • Cyber-security: EU policies and plans (https://guia.unl.pt/en/2022/fd/program/M364/course/33241)
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 6. Cybersecurity Policy, Process, and Compliance 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the second semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP006
Module name	Cybersecurity
Module type	C – Course
Training Provider	FCT (NOVA Information Management School)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B – Basic
Year – semester – exact dates offered	Second semester
Duration	3-4 months
Training method and provision	Physical at NOVA Information Management School (NOVA IMS, Campus de Campolide. 1099-032 Lisboa, Portugal)

Evaluation method(s)	Physical written examination, course frequency, and practical exercises
Module overview	Information Security in the context of organizations. Legal and normative framework for Information Security and Cybersecurity. Cyberspace Actors and Threats Risk Assessment and Management Information Security Technologies Information Security Policies Information Security Organization Management and Governance Compliance and Reporting (https://guia.unl.pt/en/2020/novaims/program/5381/course/200135)
Module description	TBA
Knowledge area(s)	4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	7.5
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the second semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP007
Module name	Cybersecurity and Data Privacy in Information Management
Module type	S - Seminar
Training Provider	FCT (NOVA Information Management School)
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	Every academic semester
Duration	3-4 months
Training method and provision	Physical at NOVA Information Management School (NOVA IMS, Campus de Campolide. 1099-032 Lisboa, Portugal)
Evaluation method(s)	Physical written examination, course frequency
Module overview	1. Digital Transformation in a Cybersecurity context 2. Cybersecurity, IT Asset Management, and Governance 3. GDPR: Governance, Implementation, Maintenance and Control 4. The Legal Framework of the Digital Ecosystem - Telecommunications, Media and Information Technology (TMT) 5. How to implement an Information Security Management System with ISO/IEC 27001 6. Cybercrime - Prevention and Forensic Techniques 7. Competitive and Counter Intelligence

Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 3. Cybersecurity Management 4. Cybersecurity Threat Management 5. Cybersecurity Risk Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	6
Certificate of Attendance (CoA)	Yes
Module enrolment dates	One month before the academic semester
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP008
Module name	Introduction to Cybersecurity in the Electrical Energy System
Module type	C - Course
Training Provider	FCT
Contact	José Fonseca jmrf@fct.unl.pt
Level	B - Basic
Year – semester – exact dates offered	2024 (exact dates TBA)
Duration	1-2 months
Training method and provision	Physical at Lisbon, Portugal
Evaluation method(s)	Physical written examination and module frequency
Module overview	1. The electrical energy system. 2. The criticality of the electrical energy infrastructure. 3. Overview of key cybersecurity threats specific to the sector. 4. SCADA systems and their cybersecurity weaknesses and challenges. 5. Emerging threats and trends in the sector. 6. Case studies.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	TBD
Certificate of Attendance (CoA)	Yes

Module enrolment dates	2024 (exact dates TBA)
Other important dates	

Training Module fields	Training Module information
Code	FCT_CSP009
Module name	Cybersecurity Challenges of Electrical Energy Substations
Module type	C - Course
Training Provider	FCT
Contact	José Fonseca jmrf@fct.unl.pt
Level	A - Advanced
Year – semester – exact dates offered	2024 (exact dates TBA)
Duration	1-2 months
Training method and provision	Physical at Lisbon, Portugal
Evaluation method(s)	Physical written examination and module frequency
Module overview	1. The electrical energy substation. 2. Cyber threats and attack vectors. 3. Countermeasures and best practices. 4. Mitigation of cyber threats. 5. Privacy and data management. 6. Regulations and standards. 7. Case studies.
Module description	TBA
Knowledge area(s)	3. Cybersecurity Management 4. Cybersecurity Threat Management 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	TBD
Certificate of Attendance (CoA)	Yes
Module enrolment dates	2024 (exact dates TBA)
Other important dates	

Training Module fields	Training Module information
Code	UNI_FCT_CSP001
Module name	CyberSecPro Portugal Summer School
Module type	SS – Summer School
Training Provider	UNINOVA and FCT
Contact	Vasco Delgado-Gomes vmdg@uninova.pt José Fonseca jmrf@fct.unl.pt
Level	B - Basic

Year – semester – exact dates offered	TBD (expected between 24-28 June 2024)
Duration	2 days
Training method and provision	Physical – Madeira, Portugal (hotel will be informed later)
Evaluation method(s)	Summer School participation and engagement
Module overview	The CSP Summer School 2024 will focus on basic Cyber Security training for SMEs based in Portugal and other European countries, and in the domains of Health, Energy, and Maritime. It will provide a general comprehensive view on the threats and issues associated with insufficient security and privacy measures and how to tackle such threats in the context of SMEs.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

Training Module fields	Training Module information
Code	UNI_FCT_CSP002
Module name	CyberSecPro Cybersecurity Executive Program Seminar
Module type	S -Seminar
Training Provider	UNINOVA and FCT
Contact	Vasco Delgado-Gomes vmdg@uninova.pt José Fonseca jmrf@fct.unl.pt
Level	A - Advanced
Year – semester – exact dates offered	TBD (expected June 2025)
Duration	3-4 days
Training method and provision	Physical – Lisbon, Portugal
Evaluation method(s)	Seminar participation and engagement
Module overview	The Cybersecurity Executive Program will be composed by 3 different and independent modules: **1 - Strategic Leadership and Governance:** This module will focus on providing executives with a strategic understanding of cybersecurity, enabling them to lead cybersecurity initiatives, make informed decisions, and effectively communicate cybersecurity risks and investments to stakeholders. **2- Incident Response and Risk Management:** This module will emphasize the preparedness and response aspects of cybersecurity. Executives will learn how to effectively respond to incidents,

	manage crises, mitigate risks associated with vendors and third parties, and integrate cybersecurity into business continuity planning. **3 - Emerging Trends and Collaboration:** This module will explore emerging trends, technologies, and collaboration in the cybersecurity landscape. Executives will gain insights into ethical and legal implications, international cooperation, cyber threat intelligence, security operations, and the impact of emerging technologies on cybersecurity. This seminar will focus on executives and leaders from SMEs in the domains of Health, Energy, and Maritime.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management 6. Cybersecurity Policy, Process, and Compliance 8. Network and Communication Security 9. Privacy and Data Protection 10. Human Aspects of Cybersecurity
Tools to be used	TBD
Language	Spoken: English/Portuguese Material: English/Portuguese Assessment: English/Portuguese
ECTS	N/A
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBD
Other important dates	

3.1.26 UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES (UNSPMF), Serbia

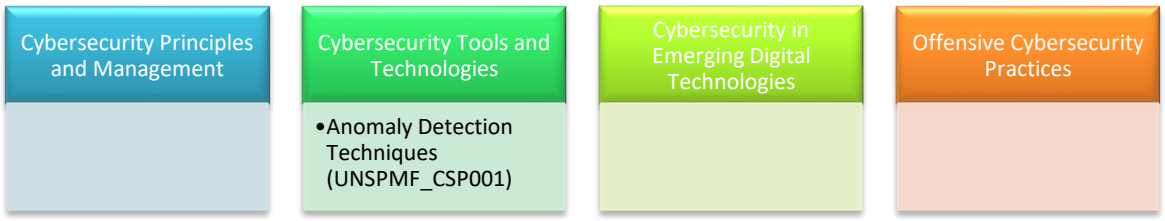

Figure 27. The full overview of UNSPMF's training modules per CSP capability categories

Figure 27 presents the full overview of UNSPMF's training modules per CSP capability categories. The following table summarizes the training module that UNSPMF is planning to offer as part of the operationalization of the CSP programme.

Training Module fields	Training Module information
Code	UNSPMF_CSP001
Module name	Anomaly Detection Techniques
Module type	S/W
Training Provider	UNSPMF
Contact	Danijela Boberić Krstićev (dboberic@uns.ac.rs)
Level	B (Basic)

Year – semester – exact dates offered	Summer semester starting from 2024
Duration	3-4 Sessions (Each session is up to 1.5 hours)
Training method and provision	Both, in the premises of UNSPMF and via Webex, meeting link will be announced
Evaluation method(s)	• Seminar/Workshop participation and engagement • Final project on a selected topic within anomaly detection
Module overview	This seminar provides a comprehensive overview of anomaly detection techniques using advanced machine learning algorithms. Participants will gain practical skills and insights into applying these techniques to real-world problems.
Module description	TBA
Knowledge area(s)	2. Cybersecurity Tools and Technologies 4. Cybersecurity Threat Management
Tools to be used	• Behavioral Analysis and Cognitive Security component (BACS) – https://zenodo.org/record/6557696 • Tensorflow 2 - https://www.tensorflow.org/ • Scikit-learn - https://scikit-learn.org/ • PyOD - https://pyod.readthedocs.io/en/latest/
Language	Spoken: Serbian/English Material: Serbian/English Assessment: Serbian/English
ECTS	-
Certificate of Attendance (CoA)	Yes
Module enrolment dates	TBA
Other important dates	

3.2 Descriptive analysis of the Training Modules

Below are some statistics based on the training modules on CSP knowledge areas that CSP partners are willing to offer:

- LAU: 19 modules
- UPRC: 6 modules and 3 joint modules with Trustilio, FP, TUC, HAF, UMA
- UMA: 8 modules and 3 joint modules with UCY, UPRC, CNR
- GUF: 3 modules
- PDMFC: 16 modules and 2 joint modules with SINTEF
- TalTech: 4 modules and 1 joint module with Trustilio
- TUBS: 1 joint module with TUC
- SINTEF: 2 joint modules with PDMFC
- TUC: 2 joint modules with TUBS, Trustilio, FP, UPRC
- UCY: 3 modules and 1 joint module with UMA
- AIT: 6 modules
- COFAC: 14 modules
- CNR: 1 joint module with UMA
- MAG: 3 modules
- UNINOVA: 2 joint modules with FCT
- APIRO: 2 modules
- C2B: 5 modules
- FP: 4 modules and 1 joint module with TUC, Trustilio, UPRC
- ITML: 4 modules

- SEA: 2 modules
- SGI: 1 module
- SLC: 3 modules and 1 joint module with Trustilio
- TRUSTILIO: 1 module and 3 joint modules with TalTech, SLC, FP, TUC, UPRC
- ZELUS: 3 modules
- FCT: 9 modules and 2 joint modules with UNINOVA
- UNSPMF: 1 module

Individual training modules: **117**
Joint training modules: **12**
Total training modules: **129**

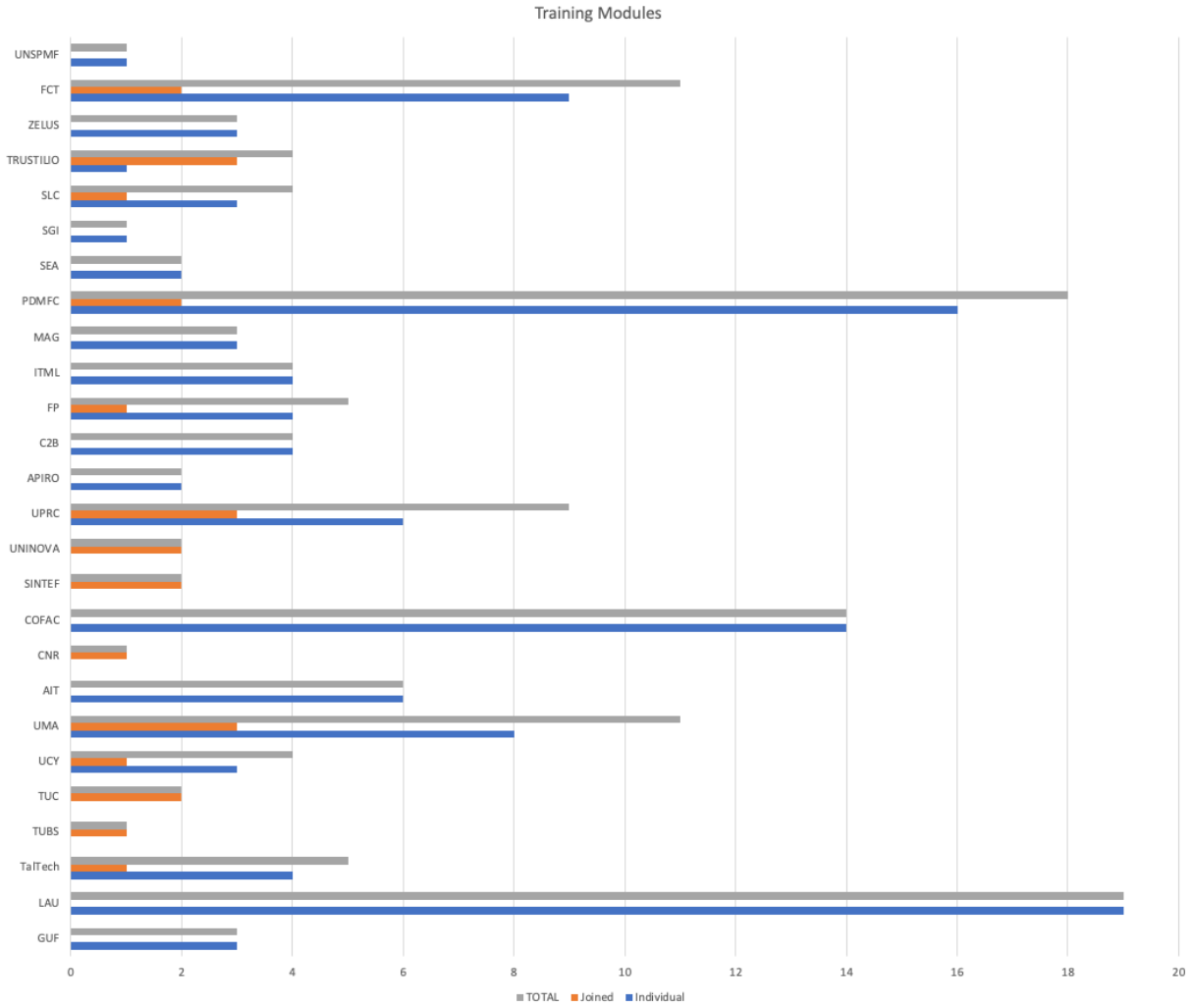

Figure 28. A descriptivee analysis of joint and individual training modules per CSP partner

3.3 Initial Design of the CSP Programme

The initial draft schedule of the CSP programme was developed through a more detailed analysis of the information gathered above. This analysis was conducted on the CSP training modules to ensure the CSP programme covers all the CSP knowledge areas and offers market-oriented capabilities. The CSP programme addresses the following aspects:

- CSP programme schedule per CSP knowledge area: Detailed planning of the trainings is done based on knowledge areas. The prioritised CyberSecPro knowledge areas considered in this deliverable are part of the outcome of a comprehensive analysis result provided in [CSP D2.3]
- CSP programme schedule per training module type,

CSP programme schedule per capability category: The planning includes the scalable offering for the CSP training modules which capture the four categories of capabilities reflected in Tasks 4.3 – Task 4.6 of CyberSecPro (cf. Section 2.1, Step 6).

The creation of the CSP programme is based on the *type and number of training modules*, as described in the CyberSecPro GA:

- "Cybersecurity Principles and Management" (Task 4.3)
  - Quantity of CSP training modules: **12 general and sector-specific** in two different levels (basic and advanced)
- "Cybersecurity Tools and Technologies" (Task 4.4)
  - Quantity of CSP training modules: **14 general and sector-specific** in two different levels (basic and advanced)
- "Cybersecurity in Emerging Digital Technologies" (Task 4.5)
  - Quantity of CSP training modules: **10 general and sector-specific** in two different levels (basic and advanced)
- "Offensive Cybersecurity Practices" (Task 4.6)
  - Quantity of CSP training modules: **12 general and sector-specific** in two different levels (basic and advanced)

Sections 3.3.1 – 3.3.10 present an initial clustering of the training modules provided by CSP partners based on the ten CSP knowledge areas defined in WP2. Later in Section 3.4 the modules will be described in more detail.

3.3.1 CSP Knowledge Area 1 – Cybersecurity Management

The following table shows the clustering of training modules under the knowledge area of Cybersecurity Management.

Table 2: Clustering of training modules under the knowledge area of Cybersecurity Management

CSP Knowledge Area 1 – Cybersecurity Management	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	TalTech_CSP001 "Introduction to Cyber Security (Maritime)" (C)
	Trustilio_SLC_CSP001 "Cybersecurity and Health" (S)
	UMA_UPRC_CSP001 "Security of Maritime, Health & Energy Critical Information Infrastructures" (S)
	UMA_CSP007 "Information Security" (C)
	UPRC_CSP002 "Information Systems Security" (C)
	LAU_CSP001 "Information and Cyber Security Management" (C)
	LAU_CSP002 "Introduction to Information Security" (C)
	LAU_CSP003 "Information Security Management" (C)
	LAU_CSP004 "Cybersecurity Management" (C)
	TUC_TUBS_CSP001 "Energy Security Fundamentals" (S)
	FCT_CSP008 "Introduction to Cybersecurity in the Electrical Energy System" (C)
	LAU_CSP011 "Enterprise Security and Practitioners" (C)
	FCT_CSP006 "Cybersecurity" (C)
	GUF_CSP003 "Information & Communication Security" (C)
	APIRO_CSP001 "Introduction to the new ISO/IEC 27001 version" (C)
Proposed CSP training modules on "**Cybersecurity Essentials and Management**" Tentative Quantity: 4	**1 general course** (basic and/or advance) • APIRO_CSP001 • GUF_CSP003 • UMA_CSP007 • UPRC_CSP002

	• LAU_CSP001 • LAU_CSP002 • LAU_CSP003 • LAU_CSP004 • FCT_CSP006 • FCT_CSP008 • LAU_CSP011 **3 sector-specific seminars** • TalTech_CSP001 (maritime) • Trustilio_SLC_CSP001 (health) • UMA_UPRC_CSP001 (maritime, health, energy) • TUC_TUBS_CSP001 (energy)
CSP capability categories:	Cybersecurity Principles and Management

3.3.2 CSP Knowledge Area 2 – Human Aspects of Cybersecurity

The following table shows the clustering of training modules under the knowledge area of Human Aspects of Cybersecurity.

Table 3: Clustering of training modules under the knowledge area of Human Aspects of Cybersecurity

CSP Knowledge Area 2 – Human Aspects of Cybersecurity	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	Trustilio_CSP001 "Human Centric and Secure Maritime Ecosystems" (S)
	Trustilio_TalTech_CSP001 "Human Factors in Cybersecurity" (S)
Proposed CSP training modules on "**Human Factors and Cybersecurity**" Tentative Quantity: 2	**1 general seminar** • Trustilio_TalTech_CSP001 **1 sector-specific seminar** • Trustilio_CSP001 (maritime)
CSP capability categories:	Cybersecurity Principles and Management

3.3.3 CSP Knowledge Area 3 – Cybersecurity Risk Management

The following table shows the clustering of training modules under the knowledge area of Cybersecurity Risk Management.

Table 4: Clustering of training modules under the knowledge area of Cybersecurity Risk Management

CSP Knowledge Area 3 – Cybersecurity Risk Management	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	AIT_CSP001 "Advanced Risk Assessment" (C)
	SLC_CSP001 "Cyber Security Risk Assessment and Management" (C), (W), (CS-E)
	C2B_CSP001 "Maritime Cybersecurity Risk" (C)
	PDMFC_CSP001 "Risk Assessment and Management" (C and S, CS-E)
	COFAC_CSP001 "Cybersecurity Management in SMEs" (C)
	CNR_UMA_CSP001 "SATRA for energy" (O)
	LAU_CSP005 "Risk Manager" (C,W)

Proposed CSP training modules on "**Risk Management**" Tentative Quantity: 3	**1 general course** (basic and/or advance) • AIT_CSP001 • SLC_CSP001 • COFAC_CSP001 • LAU_CSP005 **2 sector-specific seminars** • C2B_CSP001 (maritime) • PDMFC_CSP001 • CNR_UMA_CSP001 (energy)
CSP capability categories:	Cybersecurity Tools and Technologies

3.3.4 CSP Knowledge Area 4 – Cybersecurity Policy, Process, and Compliance

The following table shows the clustering of training modules under the knowledge area of Cybersecurity Policy, Process, and Compliance.

Table 5: Custering of training modules under the knowledge area of Cybersecurity Policy, Process, and Compliance

CSP Knowledge Area 4 – Cybersecurity Policy, Process, and Compliance	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	TalTech_CSP002 "Strategic Communications and Cybersecurity" (C)
	FCT_CSP003 "Cybersecurity and Governance" (C)
	LAU_CSP014 "Business Continuity" (C)
	APIRO_CSP002 "Cybersecurity Maturity Models Requirements / Auditing practices" (C)
	LAU_CSP017 "Cybersecurity Working Life Practices" (C,W,CS-E)
	UPRC_CSP001 "Information Security Governance" (C)
Proposed CSP training modules on "**Cybersecurity Governance**" Tentative Quantity: 1	**1 general course** (basic and/or advance) • FCT_CSP003 • LAU_CSP014 • LAU_CSP017 • UPRC_CSP001 • TalTech_CSP002 • APIRO_CSP002
CSP capability categories:	Cybersecurity Principles and Management

3.3.5 CSP Knowledge Area 5 – Network and Communication Security

The following table shows the clustering of training modules under the knowledge area of Network and Communication Security.

Table 6: Clustering of training modules under the knowledge area of Network and Communication Security

CSP Knowledge Area 5 – Network and Communication Security	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	ITML_CSP002 "Cybersecurity; Security information and event management - Endpoint protection" (S and/or O – demonstration)
	AIT_CSP002 "System and Network Security" (C)
	UMA_CSP001 "Design and Configuration of Secure Network Systems" (C)
	PDMFC_CSP004 "Network Traffic Analysis" (C and S)

	PDMFC_CSP005 "Log Parsing" (C and S, CS-E)
	PDMFC_CSP008 "Network Traffic Analysis and Monitoring with Tshark and NFStream" (C and S, CS-E)
	PDMFC_CSP011 "NMAP - Reconnaissance and Vulnerability Assessment" (C and S, CS-E)
	LAU_CSP006 "Internet Infrastructure and Security" (C)
	UPRC_CSP003 "Network and Communications Security" (C)
	UPRC_HAF_CSP001 "Network Security" (C)
	LAU_CSP007 "Data Networks and Information Security" (C)
	LAU_CSP016 "Network and Applications Security" (C)
	LAU_CSP008 "Network Applications" (C)
	GUF_CSP001 "Mobile Business I–Technology, Markets, Platforms, and Business Models" (C)
	LAU_CSP015 "Cybersecurity Analyst" (C)
	FCT_CSP001 "Network and Computer Systems Security" (C)
Proposed CSP training modules on "**Network Security**" Tentative Quantity: 3	**2 general courses** (basic and/or advance) • AIT_CSP002 • UMA_CSP001 • FCT_CSP001 • LAU_CSP016 • LAU_CSP007 • UPRC_HAF_CSP001 • UPRC_CSP003 • LAU_CSP006 • GUF_CSP001 **1 general/sector-specific seminar** • ITML_CSP002 • LAU_CSP008
Proposed CSP training modules on "**Network Traffic Analysis**" Tentative Quantity: 1	**1 general/sector-specific seminar** (basic and/or advance) • PDMFC_CSP011 • PDMFC_CSP008 • PDMFC_CSP004 • LAU_CSP015 • PDMFC_CSP005
CSP capability categories:	Cybersecurity Tools and Technologies

3.3.6 CSP Knowledge Area 6 – Privacy and Data Protection

The following table shows the clustering of training modules under the knowledge area of Privacy and Data Protection.

Table 7: Clustering of training modules under the knowledge area of Privacy and Data Protection

CSP Knowledge Area 6 – Privacy and Data Protection	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	COFAC_CSP002 "Data Protection and Cyber Crime Law" (C)
	UCY_CSP003 "Data Security" (C)
	UMA_CSP002 "Security and Privacy in Application Environments" (C)

	PDMFC_CSP003 "Privacy and Security Logging" (C and S, CS-E)
	PDMFC_CSP009 "Privacy Threat Modelling" (C and S, CS-E)
	FCT_CSP004 "Data Protection and Management Law" (C)
	GUF_CSP002 "Mobile Business II−Application Design, Applications, Infrastructures and Security" (C)
	MAG_CSP003 "Security and Privacy By Design/Default" (S)
	FCT_CSP007 "Cybersecurity and Data Privacy in Information Management" (S)
Proposed CSP training modules on "**Data Protection"** Tentative Quantity: 1	**1 general/sector-specific course or seminar** (basic and/or advance) • COFAC_CSP002 • UCY_CSP003 • FCT_CSP004
Proposed CSP training modules on "**Privacy**" Tentative Quantity: 1	**1 general/sector-specific course or seminar** (basic and/or advance) • PDMFC_CSP009 • UMA_CSP002 • PDMFC_CSP003 • FCT_CSP007 • MAG_CSP003 • GUF_CSP002
CSP capability categories:	Cybersecurity Principles and Management

3.3.7 CSP Knowledge Area 7 – Cybersecurity Threat Management

The following table shows the clustering of training modules under the knowledge area of Cybersecurity Threat Management.

Table 8: Clustering of training modules under the knowledge area of Cybersecurity Threat Management

CSP Knowledge Area 7 – Cybersecurity Threat Management	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	PDMFC_SINTEF_CSP002 "Cyber Threat Intelligence" (S)
	SLC_CSP003 "Cyber Threat intelligence and vulnerability assessment" (W)
	AIT_CSP003 "Cyber Security Threat Hunting" (C)
	C2B_CSP004 "Cybersecurity threats to Maritime Administrations" (W)
	FCT_CSP009 "Cybersecurity Challenges of Electrical Energy Substations" (C)
	LAU_CSP019 "The Landscape of Hybrid Threats" (C)
Proposed CSP training modules on "**Cyber Threat Intelligence**" Tentative Quantity: 2	**1 general or sector-specific course** (basic and/or advance) • AIT_CSP003 • FCT_CSP009 (energy) • LAU_CSP019 **1 general or sector-specific seminar/workshop** (basic and/or advance) • PDMFC_SINTEF_CSP002 • SLC_CSP003 • C2B_CSP004 (maritime)
CSP capability categories:	Cybersecurity Tools and Technologies

3.3.8 CSP Knowledge Area 8 – Cybersecurity Tools and Technologies

The following table shows the clustering of training modules under the Cybersecurity Tools and Technologies knowledge area.

Table 9: Clustering of training modules under the Cybersecurity Tools and Technologies knowledge area

CSP Knowledge Area 8 – Cybersecurity Tools and Technologies	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	AIT_CSP006 "Industrial Control Systems Security" (C)
	AIT_CSP005 "Next Generation Energy Systems Security" (C)
	UMA_UCY_CSP001 "Security in charging stations and their control systems" (S)
	LAU_CSP012 "Critical Infrastructure Protection" (C)
	C2B_CSP005 "Attacks/countermeasures/mitigations/privacy on energy control systems (SCADA)" (C)
	UMA_CSP006 "Security in Industrial and Cyber-Physical Systems" (C)
	COFAC_CSP009 "Critical Infrastructures Security" (C)
	UMA_CSP004 "Secure Coding" (C)
	COFAC_CSP008 "Secure Software Development" (C)
	LAU_CSP009 "Information Management and Databases" (C)
	UCY_CSP002 "Software Analysis" (C)
	FCT_CSP002 "Software Security" (C)
	UNSPMF_CSP001 "Anomaly Detection Techniques" (S/W)
	PDMFC_CSP007 "Applied Cryptography with GPG and OpenSSL" (C and S, CS-E)
	PDMFC_CSP010 "Lynis, OpenSCAP - Security Auditing and Hardening Tools" (C and S, CS-E)
	LAU_CSP010 "Systems Security" (C)
	PDMFC_CSP012 "Android Security and Log Parsing" (C and S, CS-E)
	PDMFC_CSP015 "Identity Access Management" (C and S, CS-E)
	UCY_CSP001 "Systems Security" (C)
	COFAC_CSP003 "Systems Security Auditing" (C)
	COFAC_CSP004 "Cloud Security" (C)
	COFAC_CSP007 "Cryptography" (C)
	PDMFC_SINTEF_CSP001 "AI and Cybersecurity" (S)
	COFAC_CSP006 "Data Analysis for Cybersecurity" (C)
	COFAC_CSP010 "AI in Cybersecurity" (C)
	UPRC_Trustilio_FP_TUC_CSP001 "Maritime Cyber Security Summer School - CyberHot" (SS)
	UPRC_CSP004 "Software Security" (C,S)
	MAG_CSP001 "Cryptography" (S)
	MAG_CSP002 "Web Application Security & API" (S)
	UNI_FCT_CSP002 "CyberSecPro Cybersecurity Executive Program Seminar" (S)
	UNI_FCT_CSP001 "CyberSecPro Portugal Summer School" (SS)
	COFAC_CSP005 "Network & IoT Security" (C)
Proposed CSP training modules on "**Cybersecurity in Emerging Technologies**"	**2 general courses or seminars** (basic and/or advance) • COFAC_CSP006

Tentative Quantity: 4	• COFAC_CSP010 • COFAC_CSP004 • COFAC_CSP005 • PDMFC_SINTEF_CSP001 • UNSPMF_CSP001 **2 general / sector-specific summer schools** • UPRC_Trustilio_FP_TUC_CSP001 (maritime) • UNI_FCT_CSP001
Proposed CSP training modules on "**CPS Security**" Tentative Quantity: 2	**1 general course** (basic and/or advance) • AIT_CSP006 • LAU_CSP012 • UMA_CSP006 • COFAC_CSP009 **1 sector-specific course** • AIT_CSP005 (energy) • UNI_FCT_CSP002 • UMA_UCY_CSP001 • C2B_CSP005 (energy)
Proposed CSP training modules on "**Software Security**" Tentative Quantity: 2	**2 general / sector-specific courses** (basic and/or advance) • UMA_CSP004 • COFAC_CSP008 • UCY_CSP002 • FCT_CSP002 • PDMFC_CSP012 • UPRC_CSP004 • MAG_CSP002
Proposed CSP training modules on "**System Security**" Tentative Quantity: 2	**2 general / sector-specific courses** (basic and/or advance) • PDMFC_CSP007 • PDMFC_CSP010 • PDMFC_CSP015 • UCY_CSP001 • COFAC_CSP003 • COFAC_CSP007 • LAU_CSP009 • LAU_CSP010 • MAG_CSP001
CSP capability categories:	Cybersecurity in Emerging Digital Technologies

3.3.9 CSP Knowledge Area 9 – Penetration Testing

The following table shows the clustering of training modules under the knowledge area of Penetration Testing.

Table 10: Clustering of training modules under the knowledge area of Penetration Testing

CSP Knowledge Area 9 – Penetration Testing	
	SGI_CSP001 "RxB game" (C, W, SS)

Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	PDMFC_CSP002 "Security scenarios: Red and Blue Teaming" (C, S, CS-E, and H)
	COFAC_CSP012 "Hacking and Pentesting Lab" (C)
	COFAC_CSP013 "Catch the Flag (CTF) Workshop" (W)
	C2B_CSP002 "AIS hacking on hands training" (C)
	C2B_CSP003 "AIS hacking work-place training" (C)
	FP_CSP001 "Focal Point - Tabletop Exercise" (Other – Tabletop Cybersecurity Game)
	FP_CSP002 "Focal Point – Cyber Defense Exercise" (CS-E)
	FP_CSP003 "FP_Training Lab" (Cybersecurity exercise (CS-E / H)
	SEA_CSP001 "HATCH" (S or CS-E)
	SEA_CSP002 "PROTECT" (CS-E)
	COFAC_CSP014 "Hacking and Defence Games Summer School" (SS)
	UPRC_CSP005 "Advance Cybersecurity Exercises" (CS-E)
	UPRC_CSP006 "Basic Cybersecurity Exercises" (CS-E)
	LAU_CSP018 "Cybersecurity Hackathon Project" (C,W,CS-E)
	LAU_CSP013 "Cybersecurity Project" (C)
	FP_CSP004 "HtB_Enterprise_Labs: Introduction To Penetration Testing" (C/W/H)
Proposed CSP training modules on "**Penetration Testing**" Tentative Quantity: 3	**3 general/sector-specific courses or seminars** (basic and/or advance) • COFAC_CSP012 • COFAC_CSP013 • FP_CSP004 • LAU_CSP018 • C2B_CSP002 (maritime) • C2B_CSP003 (maritime)
Proposed CSP training modules on "**Cyber Ranges**" Tentative Quantity: 3	**3 general/sector-specific seminars or cybersecurity exercises** (basic and/or advance) • SGI_CSP001 • PDMFC_CSP002 • FP_CSP001 • FP_CSP002 • FP_CSP003 • SEA_CSP001 • SEA_CSP002 • UPRC_CSP005 • UPRC_CSP006 • LAU_CSP013 • COFAC_CSP014
CSP capability categories:	Offensive Cybersecurity Practices

3.3.10 CSP Knowledge Area 10 – Cyber Incident Response

The following table shows the clustering of training modules under the knowledge area of Cyber Incident Response.

Table 11: Clustering of training modules under the knowledge area of Cyber Incident Response

CSP Knowledge Area 10 – Cyber Incident Response	
Relevant training modules on CSP knowledge areas that CSP partners are willing to offer:	TalTech_CSP003 "Cyber Incident handling" (C)
	AIT_CSP004 "Security Incident and Event Management" (C)
	TalTech_CSP004 "Cyber Defense Monitoring Solutions" (C)
	ITML_CSP004 "Cybersecurity; Security information and event management – Monitoring" (S and/or O – demonstration)
	PDMFC_CSP013 "Incident Handling - Security Information and Event Management" (C and S, CS-E)
	PDMFC_CSP014 "Intrusion Detection and Prevention Systems (IDPS)" (C and S, CS-E)
	ITML_CSP001 "Cybersecurity; Security information and event management - Alerting & Reporting" (S and/or O – demonstration)
	SLC_CSP002 "Information Security Management System Audit" (C)
	UMA_CSP003 "Malware Analysis" (C)
	UMA_CSP005 "Computer Forensics" (C)
	UMA_CSP008 "Information Security and Computer Forensics" (C)
	PDMFC_CSP016 "Universal Forensic Extraction Device (UFED)" (C and S, CS-E)
	COFAC_CSP011 "Forensic Analysis Lab" (C)
	ZELUS_CSP002 "Digital forensics with SmartViz DMT" (C), (S)
	ZELUS_CSP001 "Cyber Security Basic Methodologies & Forensics Training" (C), (W), (CS-E)
	ZELUS_CSP003 "Digital forensics & Red/Blue Team Practices Hands-on Training" (W), (SS), (CS-E)
	ITML_CSP003 "Cybersecurity; Security information and event management - Forensics" (S and/or O – demonstration)
	FCT_CSP005 "Cybercrime" (O)
	PDMFC_CSP006 "YARA and SIGMA: Advanced Malware Analysis and Incident Detection" (C and S, CS-E, H)
Proposed CSP training modules on "**Cyber Operations**" Tentative Quantity: 3	**1 general course** (basic and/or advance) • UMA_CSP003 • SLC_CSP002 • TalTech_CSP004 • AIT_CSP004 • TalTech_CSP003 **2 general/sector-specific seminars** • PDMFC_CSP006 • PDMFC_CSP014 • PDMFC_CSP013 • ITML_CSP004 • ITML_CSP001
Proposed CSP training modules on "**Digital Forensics**" Tentative Quantity: 3	**1 general course** (basic and/or advance) • COFAC_CSP011 • UMA_CSP008 • UMA_CSP005 **2 general/sector-specific seminars** • FCT_CSP005 • ITML_CSP003

	• ZELUS_CSP003 • ZELUS_CSP002 • ZELUS_CSP001 • PDMFC_CSP016
CSP capability categories:	Offensive Cybersecurity Practices

3.4 CSP Training Modules' Catalogue and Schedule

This section introduces an initial proposed CSP training modules catalogue, offering an overview of twelve proposed general CSP modules. These twelve general CSP modules result from further clustering to account for any potential overlaps. This represents a starting point toward building synergies to create the syllabi for these CSP modules.

Figure 29 presents an overview of the proposed clustering of CSP modules.

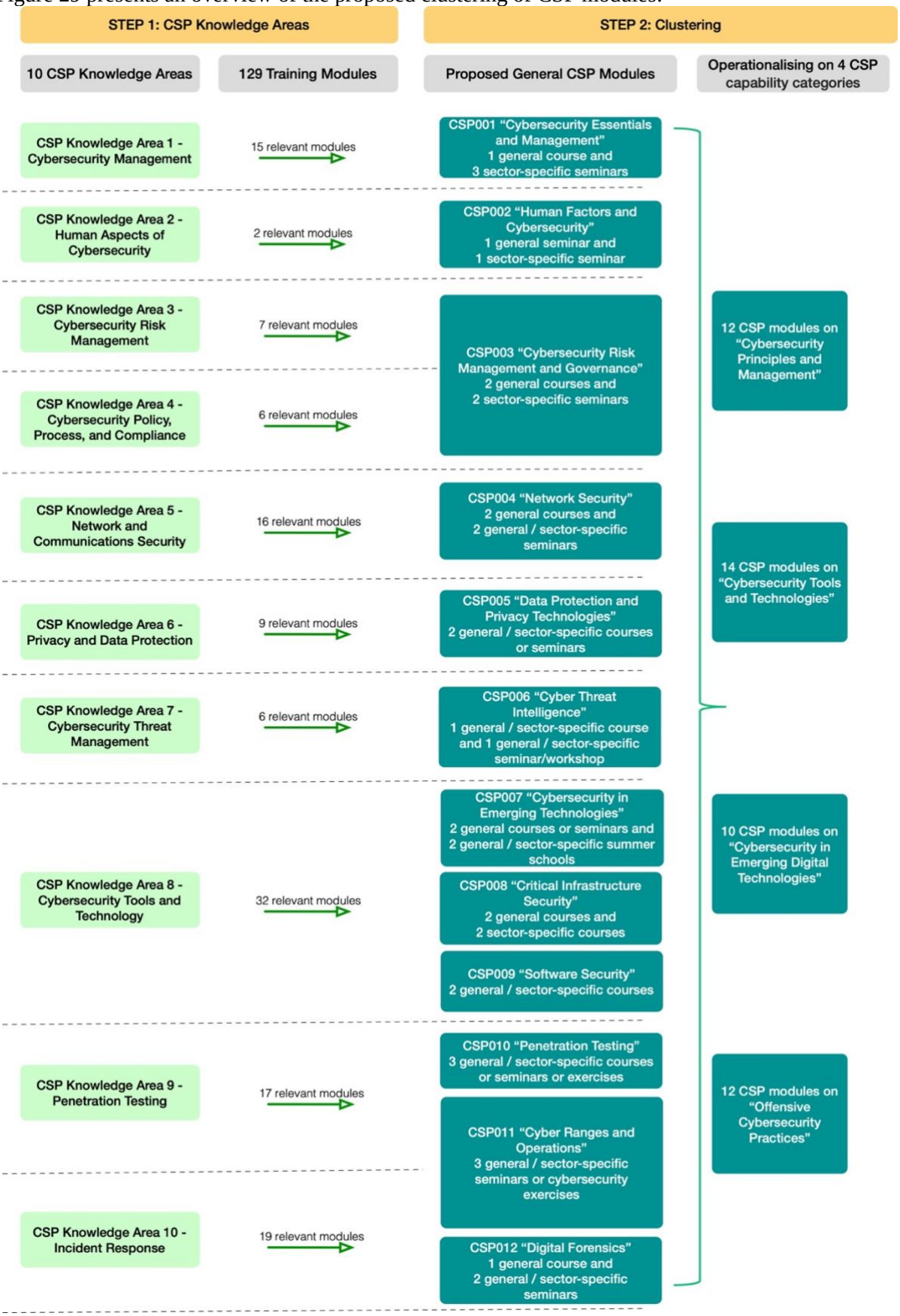

Figure 29. Overview of the proposed CSP training modules' catalogue

Below, we further analyze the 12 proposed general CSP modules and their relation to the training offerings and expertise of our CSP partners. This will lay the groundwork for fostering synergies among CSP partners and initiate their syllabus development.

CSP001 "Cybersecurity Essentials and Management"

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

15 relevant training modules for creating synergies with CSP partners:

TalTech_CSP001 "Introduction to Cyber Security (Maritime)" (C)
Trustilio_SLC_CSP001 "Cybersecurity and Health" (S)
UMA_UPRC_CSP001 "Security of Maritime, Health & Energy Critical Information Infrastructures" (S)
UMA_CSP007 "Information Security" (C)
UPRC_CSP002 "Information Systems Security" (C)
LAU_CSP001 "Information and Cyber Security Management" (C)
LAU_CSP002 "Introduction to Information Security" (C)
LAU_CSP003 "Information Security Management" (C)
LAU_CSP004 "Cybersecurity Management" (C)
TUC_TUBS_CSP001 "Energy Security Fundamentals" (S)
FCT_CSP008 "Introduction to Cybersecurity in the Electrical Energy System" (C)
LAU_CSP011 "Enterprise Security and Practitioners" (C)
FCT_CSP006 "Cybersecurity" (C)
GUF_CSP003 "Information & Communication Security" (C)
APIRO_CSP001 "Introduction to the new ISO/IEC 27001 version" (C)

CSP002 "Human Factors and Cybersecurity"

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

2 relevant training modules for creating synergies with CSP partners:

Trustilio_CSP001 "Human Centric and Secure Maritime Ecosystems" (S)
Trustilio_TalTech_CSP001 "Human Factors in Cybersecurity" (S)

CSP003 "Cybersecurity Risk Management and Governance"

This general module can be related to the CSP KA3: Cybersecurity Risk Management and CSP KA4: Cybersecurity Policy, Process and Compliance, among others. These areas involve recognising, evaluating, and mitigating cybersecurity risks, as well as encompass the creation and implementation of cybersecurity policies and procedures and the management of cybersecurity compliance, respectively. Additionally, this general module can be related to the market analysis identified knowledge areas: Cybersecurity Risk Assessment and Management, Cybersecurity Regulations and Compliance, Legal and Auditing Training, among others.

13 relevant training modules for creating synergies with CSP partners:

AIT_CSP001 "Advanced Risk Assessment" (C)
SLC_CSP001 "Cyber Security Risk Assessment and Management" (C), (W), (CS-E)
C2B_CSP001 "Maritime Cybersecurity Risk" (C)
PDMFC_CSP001 "Risk Assessment and Management" (C and S, CS-E)
COFAC_CSP001 "Cybersecurity Management in SMEs" (C)
CNR_UMA_CSP001 "SATRA for energy" (O)
LAU_CSP005 "Risk Manager" (C,W)
TalTech_CSP002 "Strategic Communications and Cybersecurity" (C)
FCT_CSP003 "Cybersecurity and Governance" (C)

LAU_CSP014 "Business Continuity" (C)
APIRO_CSP002 "Cybersecurity Maturity Models Requirements / Auditing practices" (C)
LAU_CSP017 "Cybersecurity Working Life Practices" (C,W,CS-E)
UPRC_CSP001 "Information Security Governance" (C)

CSP004 "Network Security"

This general module can be related to the CSP KA5: Network and Communication Security, among others. This area encompasses the principles and methodologies for safeguarding networks and communication channels. Additionally, this general module can be related to the market analysis identified knowledge areas: Communications and Network Security: Network Security Controls, Network and System Administration, among others.

14 relevant training modules for creating synergies with CSP partners:

ITML_CSP002 "Cybersecurity; Security information and event management - Endpoint protection" (S and/or O – demonstration)
AIT_CSP002 "System and Network Security" (C)
UMA_CSP001 "Design and Configuration of Secure Network Systems" (C)
PDMFC_CSP004 "Network Traffic Analysis" (C and S)
PDMFC_CSP005 "Log Parsing" (C and S, CS-E)
PDMFC_CSP008 "Network Traffic Analysis and Monitoring with Tshark and NFStream" (C and S, CS-E)
PDMFC_CSP011 "NMAP - Reconnaissance and Vulnerability Assessment" (C and S, CS-E)
LAU_CSP006 "Internet Infrastructure and Security" (C)
UPRC_CSP003 "Network and Communications Security" (C)
UPRC_HAF_CSP001 "Network Security" (C)
LAU_CSP007 "Data Networks and Information Security" (C)
LAU_CSP016 "Network and Applications Security" (C)
LAU_CSP008 "Network Applications" (C)
GUF_CSP001 "Mobile Business I−Technology, Markets, Platforms, and Business Models" (C)
LAU_CSP015 "Cybersecurity Analyst" (C)
FCT_CSP001 "Network and Computer Systems Security" (C)

CSP005 "Data Protection and Privacy Technologies"

This general module can be related to the CSP KA6: Privacy and Data Protection, among others. This area addresses the principles and strategies aimed at preserving the privacy and confidentiality of data. Additionally, this general module can be related to the market analysis identified knowledge area: Data Protection and Security, among others.

9 relevant training modules for creating synergies with CSP partners:

COFAC_CSP002 "Data Protection and Cyber Crime Law" (C)
UCY_CSP003 "Data Security" (C)
UMA_CSP002 "Security and Privacy in Application Environments" (C)
PDMFC_CSP003 "Privacy and Security Logging" (C and S, CS-E)
PDMFC_CSP009 "Privacy Threat Modelling" (C and S, CS-E)
FCT_CSP004 "Data Protection and Management Law" (C)
GUF_CSP002 "Mobile Business II−Application Design, Applications, Infrastructures and Security" (C)
MAG_CSP003 "Security and Privacy By Design/Default" (S)
FCT_CSP007 "Cybersecurity and Data Privacy in Information Management" (S)

CSP006 "Cyber Threat Intelligence"

This general module can be related to the CSP KA7: Cybersecurity Threat Management, among others. This area involves the procedures for identifying, assessing, and mitigating cybersecurity threats.Additionally, this general module can be related to the market analysis identified knowledge areas: Cybersecurity Threat Management: threat awareness, threat knowledge, and threat intelligence, among others.

6 relevant training modules for creating synergies with CSP partners:

PDMFC_SINTEF_CSP002 "Cyber Threat Intelligence" (S)
SLC_CSP003 "Cyber Threat intelligence and vulnerability assessment" (W)
AIT_CSP003 "Cyber Security Threat Hunting" (C)
C2B_CSP004 "Cybersecurity threats to Maritime Administrations" (W)
FCT_CSP009 "Cybersecurity Challenges of Electrical Energy Substations" (C)
LAU_CSP019 "The Landscape of Hybrid Threats" (C)

CSP007 "Cybersecurity in Emerging Technologies"

This general module can be related to the CSP KA8: Cybersecurity Tools and Technologies, among others. This area covers the utilisation of cybersecurity tools and technologies to detect and counter cybersecurity threats. Additionally, this general module can be related to the market analysis identified knowledge areas: Emerging Technologies, Cybersecurity for Artificial Intelligence and Machine Learning, Cloud Security, Cybersecurity Tools and Technlogies, among others.

8 relevant training modules for creating synergies with CSP partners:

UNSPMF_CSP001 "Anomaly Detection Techniques" (S/W)
PDMFC_SINTEF_CSP001 "AI and Cybersecurity" (S)
COFAC_CSP006 "Data Analysis for Cybersecurity" (C)
COFAC_CSP010 "AI in Cybersecurity" (C)
UPRC_Trustilio_FP_TUC_CSP001 "Maritime Cyber Security Summer School - CyberHot" (SS)
COFAC_CSP005 "Network & IoT Security" (C)
COFAC_CSP004 "Cloud Security" (C)
UNI_FCT_CSP001 "CyberSecPro Portugal Summer School" (SS)

CSP008 "Critical Infrastructure Security"

This general module can be related to the CSP KA8: Cybersecurity Tools and Technologies, among others. This area covers the utilisation of cybersecurity tools and technologies to detect and counter cybersecurity threats. Additionally, this general module can be related to the market analysis identified knowledge areas: Cybersecurity Architecture and Engineering, among others.

11 relevant training modules for creating synergies with CSP partners:

AIT_CSP006 "Industrial Control Systems Security" (C)
AIT_CSP005 "Next Generation Energy Systems Security" (C)
UMA_UCY_CSP001 "Security in charging stations and their control systems" (S)
LAU_CSP012 "Critical Infrastructure Protection" (C)
C2B_CSP005 "Attacks/countermeasures/mitigations/privacy on energy control systems (SCADA)" (C)
UMA_CSP006 "Security in Industrial and Cyber-Physical Systems" (C)
COFAC_CSP009 "Critical Infrastructures Security" (C)
UNI_FCT_CSP002 "CyberSecPro Cybersecurity Executive Program Seminar" (S)
LAU_CSP010 "Systems Security" (C)
COFAC_CSP003 "Systems Security Auditing" (C)
UCY_CSP001 "Systems Security" (C)

CSP009 "Software Security"

This general module can be related to the CSP KA8: Cybersecurity Tools and Technologies, among others. This area covers the utilisation of cybersecurity tools and technologies to detect and counter cybersecurity threats. Additionally, this general module can be related to the market analysis identified knowledge areas: Software Security, Programming Skills, Operating Systems, and Software Design Skills, among others.

13 relevant training modules for creating synergies with CSP partners:

UMA_CSP004 "Secure Coding" (C)
COFAC_CSP008 "Secure Software Development" (C)
LAU_CSP009 "Information Management and Databases" (C)

UCY_CSP002 "Software Analysis" (C)
FCT_CSP002 "Software Security" (C)
PDMFC_CSP007 "Applied Cryptography with GPG and OpenSSL" (C and S, CS-E)
PDMFC_CSP010 "Lynis, OpenSCAP - Security Auditing and Hardening Tools" (C and S, CS-E)
UPRC_CSP004 "Software Security" (C,S)
MAG_CSP001 "Cryptography" (S)
MAG_CSP002 "Web Application Security & API" (S)
PDMFC_CSP012 "Android Security and Log Parsing" (C and S, CS-E)
PDMFC_CSP015 "Identity Access Management" (C and S, CS-E)
COFAC_CSP007 "Cryptography" (C)

CSP010 "Penetration Testing"

This general module can be related to the CSP KA9: Penetration Testing, among others. This area is focused on simulating cyber-attacks to uncover and rectify security vulnerabilities. Additionally, this general module can be related to the market analysis identified knowledge area: Ethical Hacking and Penetration Testing, among others.

6 relevant training modules for creating synergies with CSP partners:

COFAC_CSP012 "Hacking and Pentesting Lab" (C)
COFAC_CSP013 "Catch the Flag (CTF) Workshop" (W)
C2B_CSP002 "AIS hacking on hands training" (C)
C2B_CSP003 "AIS hacking work-place training" (C)
LAU_CSP018 "Cybersecurity Hackathon Project" (C,W,CS-E)
FP_CSP004 "HtB_Enterprise_Labs: Introduction To Penetration Testing" (C/W/H)

CSP011 "Cyber Ranges and Operations"

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

21 relevant training modules for creating synergies with CSP partners:

SGI_CSP001 "RxB game" (C, W, SS)
PDMFC_CSP002 "Security scenarios: Red and Blue Teaming" (C, S, CS-E, and H)
FP_CSP001 "Focal Point - Tabletop Exercise" (Other – Tabletop Cybersecurity Game)
FP_CSP002 "Focal Point – Cyber Defense Exercise" (CS-E)
FP_CSP003 "FP_Training Lab" (Cybersecurity exercise (CS-E / H)
SEA_CSP001 "HATCH" (S or CS-E)
SEA_CSP002 "PROTECT" (CS-E)
UPRC_CSP005 "Advance Cybersecurity Exercises" (CS-E)
UPRC_CSP006 "Basic Cybersecurity Exercises" (CS-E)
LAU_CSP013 "Cybersecurity Project" (C)
COFAC_CSP014 "Hacking and Defence Games Summer School" (SS)
PDMFC_CSP006 "YARA and SIGMA: Advanced Malware Analysis and Incident Detection" (C and S, CS-E, H)
TalTech_CSP003 "Cyber Incident handling" (C)
AIT_CSP004 "Security Incident and Event Management" (C)
TalTech_CSP004 "Cyber Defense Monitoring Solutions" (C)
ITML_CSP004 "Cybersecurity; Security information and event management – Monitoring" (S and/or O – demonstration)
PDMFC_CSP013 "Incident Handling - Security Information and Event Management" (C and S, CS-E)
PDMFC_CSP014 "Intrusion Detection and Prevention Systems (IDPS)" (C and S, CS-E)
ITML_CSP001 "Cybersecurity; Security information and event management - Alerting & Reporting" (S and/or O – demonstration)
SLC_CSP002 "Information Security Management System Audit" (C)

UMA_CSP003 "Malware Analysis" (C)

CSP012 “Digital Forensics”

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

9 relevant training modules for creating synergies with CSP partners:

UMA_CSP005 "Computer Forensics" (C)
UMA_CSP008 "Information Security and Computer Forensics" (C)
PDMFC_CSP016 "Universal Forensic Extraction Device (UFED)" (C and S, CS-E)
COFAC_CSP011 "Forensic Analysis Lab" (C)
ZELUS_CSP002 "Digital forensics with SmartViz DMT" (C), (S)
ZELUS_CSP001 "Cyber Security Basic Methodologies & Forensics Training" (C), (W), (CS-E)
ZELUS_CSP003 "Digital forensics & Red/Blue Team Practices Hands-on Training" (W), (SS), (CS-E)
ITML_CSP003 "Cybersecurity; Security information and event management - Forensics" (S and/or O – demonstration)
FCT_CSP005 "Cybercrime" (O)

Based on the clustering, Figure 30 presents an overview of the proposed synergies for the 12 general CSP modules. This Figure 30 serves as an initial foundation for partners to establish clusters of synergies and start working on the syllabi. However, it is important to take into consideration the following aspects:

- Cross-module collaboration might be expected and necessary, depending on the partners’ efforts in WP3 and WP4. Additionally, there would be flexibility if, during the syllabus development process, some CSP partners realize that a move of the training offerings across general CSP modules is needed.
- Modules may naturally cover more than one CSP knowledge area and may be given more than once throughout the project period. The final decisions that will be made are up to each cluster of CSP partners to decide.
- The synergies of partners are expected to address their modules in multiple levels (basic and advanced), multiple types (e.g., course, seminar, workshop) and to be adjusted to different sectors.

	CSP001 "Cybersecurity Essentials and Management"	CSP002 "Human Factors and Cybersecurity"	CSP003 "Cybersecurity Risk Management and Governance"	CSP004 "Network Security"	CSP005 "Data Protection and Privacy Technologies"	CSP006 "Cyber Threat Intelligence "	CSP007 "Cybersecurity in Emerging Technologies"	CSP008 "Critical Infrastructure Security"	CSP009 "Software Security"	CSP010 "Penetration Testing"	CSP011 "Cyber Ranges and Operations"	CSP012 "Digital Forensics"
GUF	X			X	X							
LAU	X		X	X		X		X	X	X	X	
TalTech	X	X	X								X	
TUBS	X											
TUC	X						X					
UCY					X			X	X			
UMA	X		X	X	X			X	X		X	X
AIT			X	X		X		X			X	
CNR			X									
COFAC			X		X		X	X	X	X	X	X
SINTEF						X	X					
UNINOVA							X	X				
UPRC	X		X	X			X		X		X	
APIRO	X		X									
C2B			X			X		X		X		
FP							X			X	X	
ITML				X							X	X
MAG					X				X			
PDMFC			X	X	X	X	X		X		X	X
SEA											X	
SGI											X	
SLC	X		X			X					X	
TRUSTILIO	X	X					X					
ZELUS												X
FCT	X		X	X	X	X	X	X	X			X
UNSPMF							X					

Figure 30. An overview of the proposed synergies for the CSP modules

Figure 31 presents an initial plan of the trainings. A more detailed planning of the trainings will be provided later, once clusters of partners collaborate to finalize the specific timing offerings.

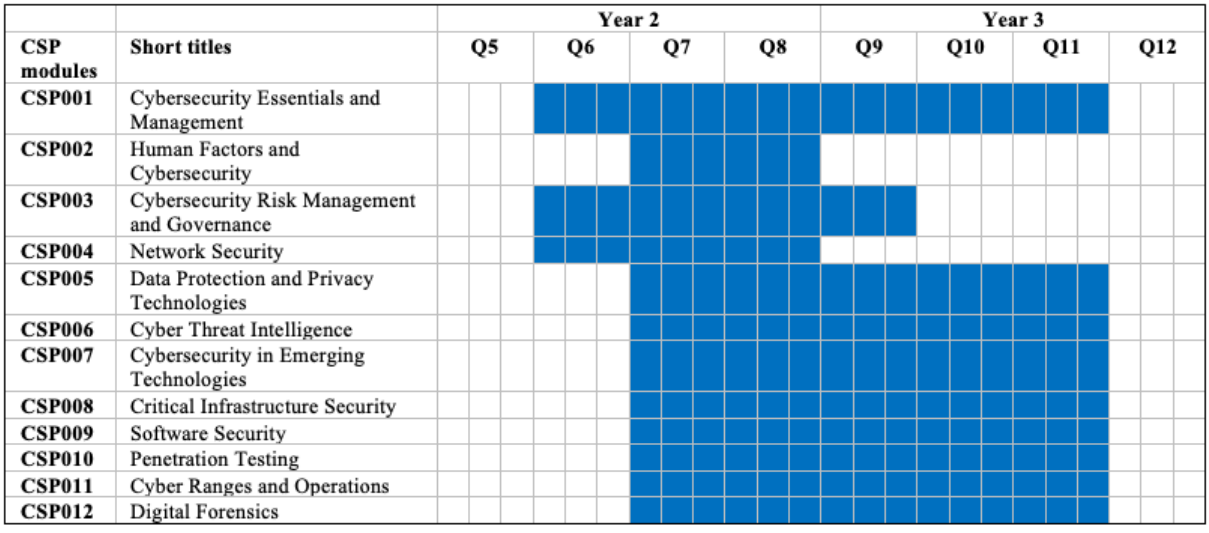

Figure 31. An initial scheduling of the CSP modules

3.5 Evaluation Templates

This section presents templates for evaluation forms for both trainers and trainees based on [1, 2]. The following evaluation templates are designed to guide you through a reflection on the training module that was just finished. They are intended to help clarify what changes could be made in the training module in the future and what should not be changed. For the trainers, filling out the evaluation report after the trainees have turned in their module evaluations would be helpful.

CyberSecPro Training Programme Analysis
Training Module – Evaluation report

Training Module Code: _____

Training Module Name: _____ Date: _____

Training Module Offered by: _____

Provider (Trainers) Evaluation Report

First Impressions

1. What do you think worked particularly well in this training module?

_____
_____

Content

2. How well do you think your trainees learned:

	1 Not at all	2 A little	3 Some	4 Much	5 Very much
Learning Objective 1	☐	☐	☐	☐	☐
Learning Objective 2	☐	☐	☐	☐	☐
Learning Objective 3	☐	☐	☐	☐	☐
Learning Objective 4	☐	☐	☐	☐	☐

Note: (Learning Objectives) will be defined by the trainers based on the module syllabus.

3. Is it your impression that the trainees had sufficient support to learn the topics in this module? Do you have any ideas of how to improve this?

_____
_____

4. Learning any topic also gives trainees the chance to learn 'transferable skills' such as writing, oral presentation, experimental design, etc. Do you think this module particularly helped your trainees improve in any of these?

_____
_____

Trainees' effort and preparedness

5. Do you think your trainees put in sufficient time and effort in this module to succeed?

	1 Few trainees	2 Some trainees	3 About half of them	4 Many trainees	5 Most trainees
Sufficient effort	☐	☐	☐	☐	☐
Sufficient time	☐	☐	☐	☐	☐

6. Do you have the impression the trainees had sufficient knowledge from previous modules to succeed in this module? (Yes/No)

Do you think the trainees saw the relevance of past knowledge/modules for your subject? (Yes/No)
How do you think we could improve the trainees' preparedness?

_____
_____

TEACHING

7. Was it your impression that these tools/teaching methods worked well to support your students learning?

	Not relevant	1 Not at all	2 A little	3 Some	4 Much	5 Very much
Lectures	☐	☐	☐	☐	☐	☐
Labs	☐	☐	☐	☐	☐	☐
Literature	☐	☐	☐	☐	☐	☐
Trainee activities	☐	☐	☐	☐	☐	☐
Seminars	☐	☐	☐	☐	☐	☐
Real life examples	☐	☐	☐	☐	☐	☐
Exercise sessions	☐	☐	☐	☐	☐	☐
Case studies (sector-specific)	☐	☐	☐	☐	☐	☐
Project work	☐	☐	☐	☐	☐	☐

Tools	☐	☐	☐	☐	☐	☐
Other: ……..	☐	☐	☐	☐	☐	☐

8. Are you satisfied with how the different parts (moments) of the module were distributed? (for example, should there have been more lab or lecture?) (Yes/No) If no, how would you change this next time?

_____
_____

9. 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? _____
_____

10. Did the examination (all aspects) correspond well with the learning objectives?
_____

Would you consider other ways of examination perhaps in the future (e.g. computer-assisted, quizzes, oral, group exams, written papers)?

_____
_____

Organisation

11. Was it your impression that trainees found it easy to find information about the course (e.g. schedule, literature lists, etc.)? Would you change anything to improve this?

_____
_____

Overall Impression

12. What challenges or problems did you face in this training module (if any)?

_____
_____

13. What would you change in this training module next time it runs? And why?

_____
_____

14. What kinds of teaching methods do you use in your module?

_____
_____

Would you like to use any new teaching methods in the future? Yes/No
What kind of support would you like to make this easy?

_____
_____

15. Other reflections?

_____
_____

Demographics

Total number of persons:

Nationalities: List ALL.

Level of education [undergraduate student (e.g. 10% or number of persons), BSc, postgraduate student, MSc, PhD student, PhD

Group ages [18-29 (e.g. 10% or number of persons), 30-39, 40-49, 50-59, 60-…]

Gender groups [% Male, % Female]

Audience (Trainees) Evaluation Report

1.How well did you achieve this learning objective in this module?

	1 To no extent	2 To little extent	3 To some extent	4 To a large extent	5 To a very large extent
Learning Objective 1	☐	☐	☐	☐	☐
Learning Objective 2	☐	☐	☐	☐	☐
Learning Objective 3	☐	☐	☐	☐	☐
Learning Objective 4	☐	☐	☐	☐	☐

Note: (Learning Objectives) will be defined by the trainers based on the module syllabus.

2.How useful to you was this module element?

	1 To no extent	2 To little extent	3 To some extent	4 To a large extent	5 To a very large extent
Learning Element 1	☐	☐	☐	☐	☐
Learning Element 2	☐	☐	☐	☐	☐
Learning Element 3	☐	☐	☐	☐	☐
Learning Element 4	☐	☐	☐	☐	☐

Note: (Learning Element) will be defined by the trainers based on the module syllabus. Examples of learning elements to evaluate can be lectures, group project, exercises etc.

3.How much did you learn from this module?

1 To no extent	2 To little extent	3 To some extent	4 To a large extent	5 To a very large extent
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐

4.Overall, how would you describe the quality of the instruction in this module?

1 Very poor	2 Poor	3 Fair	4 Good	5 Excellent
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐

5.What skills or knowledge did you learn or improve?

_____
_____

6.How many hours per week on average did you spend on this module?

[Drop-down options may make the evaluation easier e.g., 5 to 10, 11 to 20, 20 to 30. This will be assessed, when the from will be put online]

_____
_____

7.How organized was this module?

1 Not organized at all	2 Slightly organized	3 Moderately organized	4 Very organized	5 Extremely organized
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐
☐	☐	☐	☐	☐

8. would you like to recommend this module to your friends or colleagues?

_____
_____

9.What would you like to say about this module to a trainee who is considering taking it in the future?

_____
_____

10.Would you like to provide any other comments about this module?

_____
_____

4 Trainees and Trainers Mobilization

In order to broaden its reach and impact in the realm of cybersecurity education, the project is considering various strategies. One approach involves tapping into existing summer schools that offer cybersecurity courses. These established programs provide a valuable platform for engagement, offering participants structured educational experiences and access to seasoned instructors and industry professionals. By affiliating with such summer schools, the project can extend its influence and potentially create synergistic partnerships that enhance its visibility.
Moreover, the project envisions the creation of its own workshops, hackathons, or summer schools. This proactive step not only affords better visibility but also grants the project greater control over curriculum design and content delivery. Crafting customized educational experiences tailored to the project's objectives ensures a more focused and impactful engagement with participants.
Additionally, the project intends to explore opportunities at technical conferences. These conferences can serve as ideal venues to connect with a wider audience interested in cybersecurity. By presenting structured educational programs, the project can provide attendees with a pathway leading to certification, fostering their growth as cybersecurity professionals.
A key aspect of these educational initiatives is the emphasis on practical application over theoretical knowledge. The cybersecurity courses offered aim to equip participants with hands-on experiences, focusing on the development of practical skills and real-world problem-solving. This approach allows individuals to gain tangible experience and confidence in tackling cybersecurity challenges.
Furthermore, the project envisions tailoring its courses to accommodate varying skill levels, from introductory to advanced. This inclusivity ensures that diverse learners can benefit from the educational programs, fostering a community of cybersecurity practitioners at different stages of their careers.
In response to the growing demand for skilled cybersecurity professionals, the project is committed to offering comprehensive cybersecurity certification programs when possible. This involves equipping participants with the knowledge, skills, and practical experience required to excel in the field of cybersecurity and obtain recognized certifications. Below is an outline of the key components and stages of this structured learning path:

Objectives and Methodology Plan: The project can investigate initiated collaborative efforts with prominent cybersecurity associations and organizations such as (ISC)², ISACA, and CompTIA. These entities boast extensive networks comprising experienced cybersecurity professionals. By forging partnerships with these organizations, the project aims to tap into this reservoir of expertise. The passive voice is employed to emphasize the ongoing nature of these collaborative endeavours.
Another avenue being explored is the utilization of alumni networks from cybersecurity programs and universities. The project team is actively reaching out to alumni who may possess both the technical proficiency and the inclination to engage in teaching roles. The passive voice underscores the proactive nature of these outreach activities.
As part of the networking strategy, the project is considering attendance at local cybersecurity meetups and conferences. Sponsorship opportunities are also being investigated. These events serve as valuable platforms for connecting with potential trainers and partners within the cybersecurity community.
To promote project awareness and identify potential trainers, the team is contemplating the organization of webinars, workshops, and training sessions aligned with the project's objectives. This approach not only disseminates information but also creates a platform for identifying individuals who could contribute to the project's success.
A strategic collaboration is in progress with universities and colleges offering cybersecurity programs. This partnership is expected to provide access to a pool of students and professors with specialized knowledge in the cybersecurity field. The passive voice highlights the deliberate nature of this collaborative effort.
The project has embarked on initiatives to engage policymakers within relevant sectors. This engagement seeks to establish the project's relevance and alignment with governmental objectives. The passive voice underscores the importance of these ongoing efforts in securing support and endorsement from key stakeholders.

4.1 Mobilization Approach of Trainees

The Table 12 below includes event dates and locations, target audiences, participating organizations, presentation durations, and attendees. For instance, "Chania Event" was scheduled for September 26, 2023, and was open to both students and the public on registration. The event featured presentations by UPRC, PDMFC, FP, ZELUS, with presentations lasting 20-60 minutes. The event was atteneded by representatives from PDMFC, UPRC, ZELUS, SLC, and GUF, showcasing the collaborative nature of the event. The "Winterschool" event, set for 2024 in Lisbon, Portugal, is open to students and industry partners and will consist of workshops, seminars, or a hackathon, with PDMFC taking a leading role in both presenting and attending. UMA will also contribute to the Winterschool by providing seminars. As for Financial Opportunities, UMA mainly depend on the fundings provided by this project and looking additionally at a program provided by ERASMUS+. However, this requires a pre-agreement with the host university where the event will be held.

Table 12. Mobilization approach of trainees

Event	Event Date/ Place	Audience	Presenting Duration	Presenting	Attending
CyberHOT	9/29/2023	Registered	All day	UPRC, FP	PDMFC, TRUSTILLIO, TUC, FORTH, THALES, UNISEA, PROTON,
Chania Event	9/26/2023	Open	20-60 minutes	UMA, UPRC, FP, UCY, ITML, C2B, SLC, ZELUS, SGI, TRUSTILIO, COFAC, PDMFC	Consortium, TUC students
Winterschool (2 Weeks)	Planned for 2024 (Lisbon, Portugal)	Registered	1-3hrs Workshops, Seminars or Hackathon	PDMFC, COFAC, UNINOVA, UMA	PDMFC, UMA, COFAC, UNINOVA
IPICS 2024	2024 Summer	Open upon registration, mostly students	PDMFC, UMA	1-3 Hour Workshops, Seminars or Hackathon	PDMFC, UMA

The table will be further extended during Task 4.2

Knowing which organizations have already established connections with the project is valuable. These established connections may lead to opportunities for collaboration, resource sharing, and knowledge exchange. Maintaining these connections can be essential for the long-term sustainability and growth of the project. This information is vital for event planning and execution. It ensures that the project team can organize events efficiently, target the right audience, and coordinate with partner organizations to ensure successful events. Building synergy with partners is critical for aligning goals, avoiding duplication of efforts, and maximizing the impact of the project. This data helps project managers to focus their efforts on strategic partnerships that can enhance the project's effectiveness.

Mobilization Programs from Universities: Although it is possible to carry out many of the actions of the CSP project through Erasmus+ programs, it is also required to explore the individual conditions of each HEI. For example, if the Universidade Lusofona and the University of Malaga want to establish a mobility alliance between them, there must first be an inter-institutional agreement. After this, each of these two institutions must continue to comply with the conditions established by their respective institutions. In the case of the University of Malaga, their staff members have to take into account the Erasmus+ KA131 model to establish the individual mobility agreement with the destination university and for both teaching and training periods. Teaching periods allow the mobility of teaching staff to teach in another academic institution, while training periods allow trainers (either Professors or staff members at HEIs) to carry out training activities.

4.2 Mobilization Approach of Trainers

Achievements: In conjunction with Universidade Lusofona, the project is excited to announce the commencement of Bachelor (180 ECTS) and Masters (120 ECTS) degree programs in Cybersecurity. These programs have received official recognition from the Portuguese Ministry of Education and are scheduled to launch in the academic year 2023-2024. PDMFC has already compiled a comprehensive list of courses, and these academic programs will be delivered exclusively in English. The curriculum will encompass a diverse range of courses, with many drawing upon the extensive research and development undertaken by the CyberSecPro team.
In addition to the degree programs, the project is also introducing a one-year Professional Masters programme, comprising 60 ECTS credits. This initiative, spearheaded by colleague Nuno Mateus, is set to commence in the upcoming academic year. It is essential to note that this particular program will be conducted exclusively in the Portuguese language, catering to a specific linguistic demographic.
In summary, the project is actively engaged in various initiatives to identify and engage potential trainers and partners within the cybersecurity community. Moreover, the forthcoming academic programs in collaboration with Universidade Lusofona mark a significant milestone in the project's development, promising a comprehensive and specialized approach to cybersecurity education.
The following Table 13 offers a detailed overview of the project's partnerships, planned events, established connections, efforts toward synergy, and module information from partners. The first column of the table lists the project's partner organizations. These partners include PDMFC, COFAC, UNINOVA, University Lusofona, and Ionian University. These partnerships are vital for the project's success as they contribute to knowledge sharing, resource pooling, and collaborative efforts in the field of cybersecurity.

Table 13. Mobilization approach of trainers

Partner	Events (Planned)	Established Connections	Working for Synergy with	Module information provided by the partner (Main Topics - Majority)
PDMFC	CyberHOT, Chania Event, Lisbon Winterschool	**COFAC UNINOVA,** Ionian University	September 2023: SINTEF October 2023: FP, UPRC, SGI, UMA	SIEM, N/HIDS, Privacy, Identity Management, Ethical Hacking
UPRC	CyberHOT, Chania Event	**FP**	October 2023: PDMFC, SGI	Red Tearming, Blue Teaming
FP	CyberHOT, Chania Event	**UPRC**	October 2023: PDMFC, UPRC, FP	Risk Assessment
SINTEF	CyberHOT	To be established	September 2023: PDMFC	Gamification, Table top, Methodology
SGI	Chania Event	None specific	October 2023: PDMFC, UPRC, FP	Gamification, Game-Based Learning

The second column outlines the events planned as part of the project's activities. Two significant events are listed: "CyberHOT" and "Winterschool (Lisbon, Portugal)." These events are essential components of the project's engagement strategy and provide opportunities for knowledge dissemination and networking.
The third column, "Established Connections," highlights the partners with which the project has already established connections. These connections are essential for fostering collaboration and synergy. The organizations listed include COFAC, UNINOVA, University Lusofona, and Ionian University. These connections signify the project's commitment to building a strong network within the cybersecurity community.
The fourth column, "Working for Synergy with," elaborates on the efforts made by the project to work collaboratively with specific organizations. This includes efforts to establish synergy with SINTEF, FP,

and UPRC. Such synergy is crucial for aligning goals, sharing expertise, and achieving collective success in cybersecurity endeavours.
The final column provides valuable information about the specific cybersecurity modules or topics offered by the project's partners. These modules are integral to the project's educational objectives. The topics include SIEM (Security Information and Event Management), N/HIDS (Network and Host Intrusion Detection Systems), Privacy, Identity Management, and Ethical Hacking. These modules reflect the diverse and comprehensive nature of the cybersecurity curriculum offered by the project.
Mobilization Programs from Universities: Beyond the Erasmus+ programs, the structure of which has already been mentioned in Section 4.1, other national and international programmes will be explored. For example, the Marie Skłodowska-Curie staff exchanges programme (https://marie-sklodowska-curie-actions.ec.europa.eu/calls/msca-staff-exchanges-2023) can be a vehicle for allowing trainers to move between various countries. Other programmes that will be explored relate to the funding through the Recovery and Sustainability Fund (RFF) (https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en). As an example, the Greek government has announced a call for covering the cost of moving and teaching and doing research in Greece for a period of 6 months to 2 years (https://www.minedu.gov.gr/news/55202-prosklisi-episkeptes-kathigites). It is worth noting that some of these programmes include the mobilization of companies, a requirement that fits perfectly with the synthesis of the CyberSecPro consortium and the objectives of the project.
As some events may be useful to mobilize both Trainers and Trainees the consortium decided to create a new uninfied table template to collect all the relevant events identified by the partners. The template and an example are shown in Figure 32.

Event	Partner	Public?	Type	CSPro/Other Partners	Scheduled/Forseen	Date Start	Date End	Place	Language	Local/Remote
IPCS	PDMFC	Yes	Summer School	UMA, UPRC	Scheduled	09/07/2024	21/07/2024	Mytilene, Lesvos, Greece	English	Local

Description	URL	ECTS (Number/No)	Fees	Funding?	Dissemination Plan	Forseen Trainees	Forseen Trainers
The summer school will include lectures, practical work, and excursions. The participants will have the opportunity to broaden their knowledge in cybersecurity through challenges, workshops, and lectures provided by cybersecurity experts. Part of the activities will be the participation of the students in	https://summerschool.eitdigital.eu/cyber-security-business-and-technical-perspectives	3	1 350 €	EIC Sponsored	Among the existing network of partners	?	20+

Figure 32. Template and example for Mobilization Events

The file can be found at:
https://svn.m-chair.de/svn/CSPro/WP4/Training Events and Funding/CSPro_TrainingEvents.xlsx

4.3 Financial Opportunities

As part of its strategic planning and partnership development, the project recognizes the critical need to investigate funding opportunities for mobilization. This section outlines the key considerations and actions related to securing financial support for the project's activities and objectives, taking into account the previously mentioned aspects:
Collaborating organizations and participating institutions may have access to funding options or scholarships that can support these events, thereby reducing the financial burden on the project itself. Government agencies and relevant authorities may have grants available for projects aligned with national cybersecurity priorities. Engaging policymakers promotes project relevance and provides a pathway to securing financial support.
Leveraging alumni networks can be a valuable strategy for mobilizing funds. Alumni who have benefited from cybersecurity programs and are now industry professionals may be willing to contribute to the project through endowments or scholarships, thus supporting future generations of cybersecurity experts.

Collaborating with industry partners, particularly those interested in cybersecurity education and workforce development, can open doors to corporate sponsorships and contributions. Companies often invest in educational initiatives aligned with their industry interests.

By strategically aligning funding efforts with the project's partnerships, events, curriculum development, and engagement strategies, the project can discover the financial opportunities needed to extend cybersecurity education further.
To collect information about these financial opportunities a template document was prepared to organize possible interesting funding programmes. This template was added to the SVN repository and presented to all the partners so everyone could collaborate in gathering information. The template and an example are presented in Figure 33.

Partner	Country / International	Funding program available (one per row)	URL	Deadline	Target Audience (Trainers/Trainees)	Short summary of conditions
PDMFC	*Portugal*	*Portugal 2030*	https://www.pt2030.org	*2027*	*Both*	***People 2030*** ***Dedicated to demography, qualifications and inclusion, this programme has an allocation of around 5.7 billion euros funded by the ESI Fund+ and is aimed at the least developed regions of the portuguese continent, although some of its measures may cover the Lisbon and Algarve Regions.*** ***It has interventions in the fields of active employment policies, vocational and higher education.***

Figure 33. Funding opportunities template

The file can be found at:
https://svn.m-chair.de/svn/CSPro/WP4/Training Events and Funding/CSPro_FundingPrograms.xlsx

5 Aspects of Massive Open Online Courses (MOOCs)

Massive Open Online Courses (MOOCs) have organisational aspects that go beyond those of other courses. Hence additional information needs to be provided in module descriptions describing such courses. This section is added to describe the respective additional fields for a course/module template covering MOOCs.
To find the additional aspects, the experience from MOOC design and implementation at LAU as well as D2.3 Section 5.5 on Moodle: An extensive reference of its capabilities is used. The results from experience (a 3-phase model and some additional practical tips) are described in Section 5.1. The resulting additional fields for a course/module template covering MOOCs are described in Section 5.2.

5.1 Methodology for MOOC Planning and Implementation

This section describes a 3-phase model and some additional practical tips to plan and implement MOOCs. The first three subsections describe three phases:

(1) Plan and design
(2) Develop and implement in practice
(3) Continue improvement and consolidation.

The subsection 5.1.4 adds more general practical hints.

5.1.1 Phase-1: Plan and Design CSP MOOCs

Planning and designing MOOCs includes the following activities: Identifying needs, selecting a platform, developing content, aligning with objectives, designing assessments, engaging learners, deciding on instructor involvement, scheduling and choosing cohorts, providing support and integrating with other training components.

They can be performed via three steps:

1. MOOC training module requirements and needs assessment: Identify training needs and learning objectives for the CSP MOOC training module.
2. Select a MOOC platform or Learning Management System (LMS).
3. Plan the MOOC structure: This includes the schedule, course content with learning objectives, tutoring plan, assessment policy, and other practical considerations.

5.1.2 Phase-2: Develop and Implement MOOCs in Practice

Developing and implementing MOOCs in practice includes the following activities: Developing content, assessments, and engagement strategies; deciding on instructor involvement, scheduling and choosing a cohort model; providing support and integrating with other training components; monitoring progress, gathering feedback; deciding on certification and recognition, utilising analytics, making iterative improvements, ensuring compliance, and communicating and market effectively.

They can be performed in twelve steps:

1. Develop or curate relevant course content.
2. Develop assessments and evaluation methods.
3. Develop engagement strategies.
4. Decide on the level of instructor involvement.
5. Schedule the MOOC and choose a cohort model.
6. Provide support resources and integrate with other training components.
7. Monitor participant progress and gather feedback.
8. Decide on certification and recognition.
9. Utilise analytics to track learner engagement and completion rates.
10. Make iterative improvements to the MOOC content and structure.
11. Ensure compliance with any relevant regulations or standards.

12. Communicate and market the MOOCs effectively.

5.1.3 Phase-3: Continue Improvement and Consolidate MOOCs

Continuing to improve and consolidate MOOCs includes the following activities: Evaluating learning outcomes, gathering feedback, using feedback to inform future planning, considering scalability and sustainability, and keeping detailed records.

They can be performed via five steps:

1. Evaluate learning outcomes and gather feedback from participants and supervisors.
2. Use feedback to inform future training programme planning and MOOC refinement.
3. Consider the long-term scalability and sustainability of MOOC-based training.
4. Keep detailed records of the MOOC design, implementation, and outcomes.
5. Continue improvement in future implementations.

5.1.4 Additional Practical Tips for Successful MOOCs Offerings:

It is evident that many MOOCs implementations did not succeed due to some common mistakes and errors. Therefore the following additional tips for success are recommended:

- Be clear and concise in your writing. Avoid using jargon or acronyms that your learners may not be familiar with.
- Use a variety of teaching methods and activities to keep your learners engaged. This could include video lectures, readings, quizzes, assignments, and discussion forums.
- Provide opportunities for learners to collaborate and interact with each other. This can help to create a more supportive and engaging learning environment.
- Give learners regular feedback on their work. This will help them to identify areas where they need to improve and to track their progress over time.
- Be responsive to learner feedback. Use feedback to improve your MOOCs and to make sure that they are meeting the needs of your learners.
- Consider that MOOC learners may come from a different location with a different legal environment.

5.2 Templates for the CSP MOOCs

Following the description of MOOC design experience in Section 5.1 the additional fields for a course/module template covering MOOCs are described in this section. The original templates from Section 2.2 are reproduced, and the additional fields are added in ***bold face and italics***.

Table 14: Template for CSP MOOCs

Training Module fields	Training Module information
Code (mandatory field) *Code format: PROVIDER NAME(S)_CSP001 (for example, LAU_CSP001). The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*	
Module name (mandatory field) *The title of the training module.*	
Module type (mandatory field) *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	
Training Provider (mandatory field) *Name(s) of training providers.*	
Contact (mandatory field) *Name(s) of the main contact person and their email address.*	

Level (mandatory field) *Training level: B (Basic), A (Advanced)*	
Year – semester – exact dates offered (mandatory field) *Indicates the year / semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	
Duration (mandatory field) *Duration of the training.* ***Duration of prefabricated teaching videos*** ***Estimated duration for students online-interaction during the module***	
Training method and provision (mandatory field) *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	
Types of assignments*:** ***Programming task, essay, presentation, test-exam. Mutual peer-review among students	
Evaluation method(s) (mandatory field) *Indicates physical and/or virtual tests, participation, exercises, etc.*	
Module overview (mandatory field) *The topics that the training module covers.*	
Module description *Please note that this field will be defined later. More information will be provided with syllabus /.ppt/ video teaser, registration procedures, developed in WP3.*	TBA
Knowledge area(s) (mandatory field) *Mapping to the 10 selected CSP knowledge areas.* *1. Penetration Testing* *2. Cybersecurity Tools and Technologies* *3. Cybersecurity Management* *4. Cybersecurity Threat Management* *5. Cybersecurity Risk Management* *6. Cybersecurity Policy, Process, and Compliance* *7. Cyber Incident Response* *8. Network and Communication Security* *9. Privacy and Data Protection* *10. Human Aspects of Cybersecurity* ***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)*** ***Frequency and rhythm of assignments if applicable***	
Tools to be used (mandatory field) *A list of tools that will be used for the operation of this training module.* ***MOOC platform Learning Management System (LMS) used, including the link to the platform or system*** ***Features and platforms for communication among students*** ***Dates and times for scheduled maintenance and updates of the MOOC platform and infrastructure*** ***Course materials, self-testing-tools and other resources made available and their location***	
Language (mandatory field) *Indicates the spoken **and if applicable subtitle** languages and the languages for the material and the assessment/evaluation.*	Spoken: Material: Assessment:
ECTS (optional field) *If applicable, the number of ECTS.*	
Certificate of Attendance (CoA) (optional field) *Indicates Yes or No (even in case of partial attendance)*	
Module enrolment dates (optional field) *Indicates the enrolment dates for the operation of this training module.*	
Other important dates (optional field) *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	

Technology that is required on the learner's side to utilise the MOOC course successfully, e.g. • ***minimum screen size and/or resolution,*** • ***minimum number of screens,*** • ***microphone needed or not*** • ***camera needed or not*** • ***minimum bandwidth*** • ***specification of device needed, e.g. operating system, browser type and version*** • ***specification of specific software (e.g. z-Tree client software) to be downloaded by participants for participation, including source and location of the software, conditions of use (e.g. licensing fees, prices and reductions), manuals, user guides, tutorials and other support materials*** ***Information, which requirements are essential and which are nice to have*** ***Conditions and requirements for remote group work of learners in e.g. cohorts*** ***Conditions of data collection and processing by the module provider, e.g. wrt GDPR compliance, purpose of collection (e.g. monitoring progress or gathering feedback), processing (analytics) tools, receiver of data, duration of storage, protection tools*** ***Further relevant regulation***	

6 Conclusions

This CyberSecPro deliverable D4.1 reflects the outcomes of tasks T4.1 and T4.2 at Month 11. Therefore it lists all the training modules each partner intends to develop and offer. These modules are then grouped into a list of 12 CyberSecPro modules, with various synergies proposed to assist in crafting their syllabi and facilitating their operation. Consequently, the deliverable presents a catalogue of CyberSecPro training modules. Moreover the deliverable provides mobilization mechanisms to attract and engage internal and external trainees and trainers. In this way, the deliverable lays the ground for the collaboration in designing and implementing the CSP programme and its modules.

References

1. https://medarbetarportalen.gu.se/digitalAssets/1747/1747007_teacher-course-evaluation.pdf
2. https://evals.stanford.edu/end-term-feedback/course-feedback-form