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

Project start: 2022-12-01
Project duration: 36 months

CyberSecPro

D3.5
CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Maritime

Document Identification	
Due date	2024-03-31
Submission date	2024-06-04
Version	1.0

Related WP	WP3	Dissemination Level	PU – Public
Lead Participant	UPRC	Lead Author	Dimitrios Kallergis, Nineta Polemi, Christos Douligeris (UPRC)
Contributing Participants	UPRC, LAU, AIT, Trustilio, FP, MAG, TUC, TalTech, SLC	Related Deliverables	D2.1, D2.3, D3.1, D4.1

Abstract: Maritime stakeholders are relying on specific systems, namely VMS (vessel monitoring systems), AIS (Automatic Identification Systems) and GNSS (Global Navigations by Satellite Systems) to ensure their movements at sea. They use specific professional tools as port control (PCS) and cargo controls (CCS) systems to monitor their activity and are largely integrated in the overall supply chains with highly interconnected systems that are as many potential sources as possible for threats.
The education of maritime stakeholders is broad in addition to the specialists that are operating directly the incident event management and incident response, mostly in close coordination with national administrations (customs, border security forces and port authorities). From the crew of a ship to the CIS information security officer of a company or a harbour, a broad area of training is needed adapted to their needs and skills. Crews of ships must be trained on their specific systems to maintain an ad-hoc security level of their navigation. Shipping companies must ensure that their systems are operating, avoiding major shutdowns as the ones observed on MAERSK in 2017 and CMA CGMin 2021 (the attacks on these companies impacted them with losses estimated at more than 100M€ for each). At least, the security of ships and their navigations systems are crucial to the security of crews that are navigating on them.
The following modules described hereafter are proposing seminars, courses and workshop aiming at developing a cybersecurity culture to maritime stakeholders, developing skills to avoid incidents and attacks and reducing risks for the sector.

The deliverable reflects the Task 3.6 outcomes.

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 (CSP) portfolio comprises a series of cybersecurity curricula tailored specifically for the maritime industry and its professionals. This report serves as a compilation of CSP training courses aimed at bolstering the cybersecurity skills of maritime professionals. The curriculum is strategically crafted to address critical areas and topics identified during the CSP development process, incorporating insights gleaned from market analysis and meeting the training supply from CSP partners. It represents a comprehensive assortment of CSP modules and their syllabi tailored specifically for the maritime sector.

Encompassing a broad spectrum of CSP module syllabi, including but not limited to human factors of cybersecurity, data security and privacy, as well as network and communication security, the content of these syllabi integrates both generic CSP elements and sector-specific nuances. The overarching objective is to equip maritime providers with the requisite tools and expertise to safeguard sensitive data and ensure the integrity of maritime systems. With a strong emphasis on hands-on training and practical learning, the CSP curriculum affords maritime professionals the opportunity to apply their skills in real-world scenarios. Through the CSP portfolio, maritime providers are empowered to make informed decisions and implement proactive measures to safeguard their maritime organizations against cyber-threats.

Document information

Contributors

Name	Beneficiary
Dimitrios Kallergis, Nineta Polemi, Christos Douligeris	UPRC
Paresh Rathod	LAU
Stefan Schauer	AIT
Kitty Kioskli	Trustilio
Christos Grigoriadis	FP
George Kliafas, Spiros Borotis	MAG
Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis	TUC
Ricardo Lugo	TalTech
Shareeful Islam	SLC

Reviewers

Name	Beneficiary
Cristina Alcaraz	UMA
Iro Chatzopoulou	APIRO

History

Version	Date	Contributor(s)	Comment(s)
0.1	2023-09-06	Nineta Polemi, Christos Douligeris, Dimitrios Kallergis	1st Draft of ToC
0.2	2023-11-03	Nineta Polemi, Christos Douligeris, Dimitrios Kallergis	2nd Draft of ToC
0.3	2023-12-13	Nineta Polemi, Christos Douligeris, Dimitrios Kallergis	Major changes in ToC
0.4	2024-02-01	Dimitrios Kallergis, Nineta Polemi, Christos Douligeris, Paresh Rathod, Stefan Schauer, Christos Grigoriadis, Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis, Kitty Kioskli, George Kliafas, Spiros Borotis	Modules 1, 3, 6, and 11 added
0.5	2024-02-02	Ricardo Lugo	Module 2 and 8 added
0.6	2024-02-09	Ricardo Lugo	Module added
0.7	2024-02-10	Pinelopi Kyranoudi, Markos Kimionis, Evripidis Sotiriadis	Modules 1 and 9 added
0.8	2024-02-13	Stefan Schauer	Module 4 added
0.9	2024-02-14	Shareeful Islam	Module 3 and 6 added
0.91	2024-02-28	Cristina Alcaraz, Iro Chatzopoulou, Dimitrios Kallergis, Nineta Polemi, Christos Douligeris	1st review and contribution
0.92	2024-03-14	Iro Chatzopoulou, Cristina Alcaraz, Dimitrios Kallergis, Nineta Polemi, Christos Douligeris	2nd review and contribution
0.93	2024-03-25	Dimitrios Kallergis, Nineta Polemi, Christos Douligeris	Review
0.94	2024-04-02	Jeldo Arno Meppen	Review by the QM
0.95	2024-05-30	Johanna Herz	Check and Layout
0.96	2024-05-31	Dimitrios Kallergis	Check and Layout
0.97	2024-05-31	Johanna Herz	Check and Layout
1.0	2024-06-04	Atiyeh Sadeghi	Final check, layout refinement and submission process

Table of Contents

List of Tables

List of Acronyms

	2FA	Two Factor Authentication
A	**ACM**	Association for Computing Machinery
	AI	Artificial Intelligence
	AIA	Artificial Intelligence Act
	API	Application Programming Interface
	APT	Advanced Persistent Threat
	AR	Augmented Reality
C	**CA**	Contract Agent
	CC	Computing Curricula
	CCN	Competence Centres Network, Cyber Competence Network
	CCPA	California Consumer Privacy Act
	CDO	Chief Data Officer
	CE	Computer Engineering
	CERT	Computer Emergency Response Team
	CI	Critical Infrastructures
	CIA	Confidentiality Integrity Availability
	CISO	Chief Information Security Officer
	CISSP	Certified Information Systems Security Professional
	CMMC	Cybersecurity Maturity Model Certification
	CNI	Critical National Infrastructure
	CNN	Convolutional Neural Network
	CoA	Certificate of Attendance
	COTS	Commercial Off-the-shelf
	CR	Cyber Range
	CS	Computer Science
	CSCL	Computer-Supported Collaborative Learning

	CSIRT	Computer Security Incident Response Team
	CSO	Chief Security Officer
	CSP	Cloud Service Provider
	CSR	Corporate Social Responsibility
	CTI	Cyber Threat Intelligence
	CVE	Common Vulnerabilities and Exposures
	CVSS	Common Vulnerability Scoring System
	CWE	Common Weakness Enumeration
	CyBoK	Cyber Security Body of Knowledge
	CyPR	Cybersecurity Professional Register
D	**D**	Deliverable
	DCM	Dynamic Curriculum Management
	DCMS	Dynamic Curriculum Management System
	DMZ	Demilitarised Zone
	DNS	Domain Name System
	DPIA	Data Protection Impact Assessment
	DTLS	Datagram Transport Layer Security
E	**E2EE**	End-to-end encryption
	EAP	Extensible Authentication Protocol
	EC	European Commission
	E-CCS	ECHO Cybersecurity Certification Scheme
	ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
	ECSF	European Cybersecurity Skills Framework
	ECTS	European Credit Transfer and Accumulation System
	EDR	Endpoint Detection and Response
	E-MAF	ECHO Multi-Sector Assessment Framework (previously E-MSAF)

	EMEA	Europe, Middle East, and Africa
	ENISA	European Union Agency for Cybersecurity
	EU	European Union
G	**GDPR**	General Data Protection Regulation
	GSM	Global System for Mobile Communication
H	**HEIs**	Higher Education Institutions
	HTTPS	Hypertext Transfer Protocol Secure
I	**ICTs**	Information and Communication Technologies
	IDS	Intrusion Detection System
	IEEE	Institute of Electrical and Electronics Engineers
	IoT	Internet of Things
	IPS	Intrusion Prevention System
	ISO	International Organization for Standardization
	ISRM	Information Security Risk Management
	IT	Information Technology
K	**KA**	Knowledge Area
	KPI	Key Performance Indicator
	KSA	Knowledge, Skills, Abilities
	KU	Knowledge Unit
L	**LAN**	Local Area Network
	LMS	Learning Management System
	LSTM	Long Short-Term Memory
M	**MAN**	Metropolitan Area Network

	MOOC	Massive Open Online Courses
N	**NAT**	Network Address Translation
	NIST	National Institute of Standards and Technology
O	**OSI**	Open System Interconnection
	OSINT	Open-Source Intelligence
	OT	Operational Technology
P	**PC**	Project Coordinator
	PETs	Privacy Enhancing Techniques
	PGP	Pretty Good Privacy
	PPT	Power Point Presentation
Q	**QUIC**	Quick UDP Internet Connections
R	**RBAC**	Role-Based Access Control
S	**SDLC**	Software Development Life Cycle
	SDN	Software-Defined Networks
	SIEM	Security Information and Event Management
	SMIME	Secure Multipurpose Internet Mail Extensions
	SSH	Secure Shell
T	**T**	Task
	TCP	Transmission Control Protocol
	TCP/IP	Transmission Control Protocol / Internet Protocol
	TLS	Transport Layer Security
	ToC	Table of Contents

U	**UDP**	User Datagram Protocol
V	**VLAN**	Virtual Local Area Network
	VPN	Virtual Private Network
	VR	Virtual Reality
W	**WAN**	Wide Area Network
	WLAN	Wireless Local Area Network
	WMAN	Wireless Metropolitan Area Network
	WP	Work Package
	WPA	Wi-Fi Protected Access
	WPA2	Wi-Fi Protected Access 2
X	**XSS**	Cross-Site Scripting

Glossary of Terms

C

CSP competence

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it.”

CSP Dynamic Curriculum Management System (DCMS)

Includes all the procedures and processes that CyberSecPro will use to manage the curriculum portfolio. The open-source learning platforms Moodle and/or e-class will be used (since the academic partners already use it in the academic programmes) for the CyberSecPro Dynamic Curriculum Management (DCM) integration. It will entail the entire curriculum creation, evaluation, review, approval, promotion processes, and regulation compliance (e.g., General Data Protection Regulation (GDPR)).

The main requirements of the CyberSecPro online DCM will be flexibility and responsiveness to the continuously changing needs of the cybersecurity market. The online DCM tool will be integrated by parametrising the Moodle or e-class open-source learning platform where the cybersecurity market needs will be monitored, and curricula will be managed.

CSP Knowledge Areas (KAs)

The Knowledge Areas (KAs) derived from D2.3 listed were based on the CyBoK Skills Framework, JRC recommendation and mainly from the European Cybersecurity Organisation report based on industry-academia cooperation and development work. However, the project will be further aligned with the ECSF and the market analyses' outcomes.

CSP practical skill

The initial studies confirmed the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results”.

CSP sector-specific training modules

CSP training modules will concentrate on the maritime, maritime, and energy sectors. The modules will be shaped around real-life challenges in collaboration with the HEIs, companies and industries, adapting their content and approach to the specific knowledge areas and parametrizing the training tools and practical exercises accordingly.

CSP syllabus

All training modules are accompanied by a syllabus that include information like learning outcomes, who should attend, relative conventions and standards, prerequisite competencies (skills & knowledge), training module outline, list tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training, training tools that will be used, assessment methods, exams, study time (physical and online learning) and so on.

A standard template for a CSP syllabus is available in this deliverable and it will be used in all CSP training modules.

CSP Trainees

CSP Trainees refer to prospective IT professionals or individuals who enrol in CyberSecPro training programme.

CSP Trainers

CSP Trainers refer to CyberSecPro partners who provide training in each cybersecurity domain.

CSP training format

CSP training format describes the way how modules will be provided, i.e., “OnDemand,” “Web-based,” “Live Online,” “Live in Person,” “Hybrid/mix” etc.

CSP training material

Corresponds to all material that will be used by the educator/trainer to provide the CSP training module.

CSP training modules

Comprises courses, mini-courses, lectures, cyber hands-on exercises, cyber hackathons, cyber mornings & events, cybersecurity games, red/blue team exercises, summer schools, workshops, ad-hoc sector-specific seminars, on-demand mini-technological courses, and crisis management training.

CSP training programme

The programme consists of training modules that can be offered individually or as a package of modules; it will not lead to any certification, degree, or career paths; it will be used to enhance existing training offers to close the gaps between academic training supply and marketing professional demands.

CSP training tools

Training tools that will be used in the training of the CSP modules (the assessment of the various tools, selection and portfolio occurs in T2.3).Introduction

1 Introduction

The maritime sector faces escalating cyber threats, necessitating robust cybersecurity training and awareness efforts. The CyberSecPro (CSP) project has conducted thorough research and analysis, identifying a deficiency in current cybersecurity training offerings for maritime professionals. This gap highlights the necessity for a specialized education and training program addressing the unique challenges and vulnerabilities within the maritime sector. In response, the CSP project has developed a series of key deliverables, with a focus on D2.1, D2.2, and D2.3. These foundational deliverables have established the groundwork for a targeted cybersecurity training approach tailored to the maritime sector, resulting in the creation of 12 core training modules. These modules are specifically crafted to provide maritime professionals with the requisite skills and knowledge to effectively navigate and mitigate daily cybersecurity threats. This deliverable aims to delineate the structure, requirements, and specifications of these training modules, presenting a comprehensive framework for the CyberSecPro education and training program customized for the maritime sector.

1.1 Background

Professional training on cybersecurity is essential for the maritime sector to safeguard its operations, protect critical infrastructure, ensure regulatory compliance, manage risks effectively, and mitigate the impact of cyber-attacks on global maritime activities. In detail, the maritime sector needs professional training on cybersecurity for several reasons:

1. **Vulnerability to Cyber Attacks**: Maritime infrastructure, including ships, ports, and logistics systems, are increasingly reliant on digital technologies and interconnected systems. This makes them vulnerable to cyber-attacks from various threat actors, including hackers, state-sponsored entities, and cybercriminals.
2. **Potential Impact of Attacks**: A cyber-attack on maritime systems can have severe consequences, including disruptions to global trade, environmental damage from accidents caused by compromised systems, financial losses, and threats to human safety.
3. **Complexity of Systems**: Modern vessels and port facilities are equipped with sophisticated onboard systems, navigation equipment, cargo management systems, and communication networks, all of which are potential targets for cyber-attacks. Understanding the complexities of these systems and how they interconnect is crucial for effectively securing them against cyber threats.
4. **Regulatory Compliance**: The maritime industry is subject to international regulations and standards related to cybersecurity, such as the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code and guidelines on maritime cybersecurity. Compliance with these regulations requires personnel with specialised training and knowledge in cybersecurity best practices.
5. **Risk Management**: Training in cybersecurity enables maritime professionals to identify, assess, and mitigate cybersecurity risks effectively. This includes implementing security controls, conducting risk assessments, developing incident response plans, and staying abreast of emerging threats and vulnerabilities.
6. **Protection of Sensitive Data**: The maritime sector handles sensitive information, including vessel schedules, cargo manifests, crew details, and financial transactions. Proper training ensures that personnel understand the importance of safeguarding this information from unauthorized access, theft, or manipulation.
7. **Emerging Threat Landscape**: Cyber threats are constantly evolving, with attackers developing new techniques and tactics to exploit vulnerabilities in maritime systems. Professional training equips personnel with the skills and knowledge needed to adapt to these evolving threats and implement proactive security measures.

The necessity for specialized training in the maritime sector was highlighted in deliverables D2.1 and D2.3, which pointed out the sector's need for further education across 10 Key Areas (KA). Based on this critical analysis, the deliverable D2.3 proposed the development of 12 modules specifically designed to

address these needs. This deliverable aims to present the programme developed to enhance the cybersecurity professional skills in the maritime sector.

1.2 Relation to Other Work Packages and Deliverables

This document offers details about the integration and the relationships between this deliverable and other components of the CyberSecPro project. It highlights how this deliverable complements and extends the work done in other packages, illustrating the cohesive effort to bolster cybersecurity in the maritime sector.

1.3 Structure of the Deliverable

Utilizing the templates from D3.1, this deliverable provides a detailed composition and guidance of CSP modules (courses, seminars, workshops, summer-schools, etc.) for readers through the sections and subsections. Chapter 2 describes the details about the mapping from the generic to the sector-specific modules, while Chapter 3 thourougly presents different module offerings for the maritime sector. Chapter 4 concludes this deliverable.

2 Mapping From Generic to Specific Training Modules

2.1 Value Proposition for Maritime

The maritime sector stands at the forefront of critical infrastructure, holding vast amounts of sensitive data and operating under the constant threat of cyberattacks. The value proposition for addressing cybersecurity specifically within the maritime sector cannot be overstated, given the potential risks and real-world consequences of cyber incidents. The justification for this targeted focus on maritime cybersecurity arises from several key considerations:

- **Real Cyberattacks and Vulnerabilities:** The maritime sector has witnessed numerous cyber incidents, ranging from ransomware attacks that cripple maritime systems to data breaches that expose passenger or staff information. Such events not only disrupt maritime services but also erode passenger or staff trust and can lead to direct harm. Analyzing these incidents reveals patterns and common vulnerabilities that training can address, making cybersecurity not just an IT concern but a passenger or staff safety issue.
- **Needs from D2.1:** The findings from deliverable D2.1 highlight specific cybersecurity knowledge gaps and training needs within the maritime sector. By connecting these identified needs with the real-world implications of cyberattacks, the rationale for bespoke cybersecurity training modules becomes clear. Training programs that address these gaps can significantly enhance the sector's resilience, ensuring maritime professionals are prepared to protect against and respond to cyber threats effectively.

The integration of these considerations into the CyberSecPro (CSP) programme underscores the critical nature of cybersecurity training tailored for maritime professionals. By focusing on actual incidents and the specific needs identified in D2.1, the CSP Maritime Modules aim to equip maritime professionals with the knowledge and skills necessary to safeguard their digital and physical environments against cyber threats, ensuring the continuity and integrity of maritime services.

2.2 Development methodology for CSP Maritime Modules

The development of the CSP Maritime Modules follows a structured methodology designed to ensure that each training module is relevant, comprehensive, and directly applicable to the maritime sector. This process involves several key steps:

1. **Construction of the Syllabus for Each Training Module:**
    a. **Considering Templates of D3.1 and the Cybok Framework:** Each syllabus is constructed with reference to the general description and structure provided in D3.1 templates, ensuring a consistent approach across all CSP Modules. The Cybok (Cyber Knowledge) framework further guides the content, ensuring it encompasses a broad spectrum of cybersecurity knowledge areas relevant to maritime.
2. **Parametrization and Adaptation to the Application Context:** The syllabus for each module is then tailored to the specific application context of the maritime sector, incorporating insights from D3.1 and D3.2. This step ensures that the training is not only grounded in theoretical knowledge but is also highly relevant to the practical challenges faced by maritime professionals. The adaptation process involves customizing examples, case studies, and exercises to reflect real-world maritime scenarios, enhancing the applicability and effectiveness of the training.

The methodology behind the development of CSP Maritime Modules is iterative and collaborative, involving feedback from cybersecurity experts, maritime professionals, and educators. This approach ensures that the modules are not only pedagogically sound but also technically accurate and directly

aligned with the needs of the maritime sector. By leveraging the foundational templates and adapting them to the specific context of maritime, the CSP programme aims to provide a comprehensive training solution that addresses the unique cybersecurity challenges faced by this critical sector.

2.3 Training material and Video Teasers for CSP Training Modules for Maritime

As mentioned, this deliverable contains the unique codes for each of the CSP training modules along with the details associated with each of the modules. In addition, the syllabus for each module is listed and finalised in this deliverable. But what is very important and should be noted is that the training material along with the video teaser for each module is located on the **Digital Content Management** (DCM) server, which is a platform where the user will login and find the material for all the presented modules. The details concerning this platform are presented on the deliverable D3.1.

3 CyberSecPro Customised Modules Syllabus for Maritime

3.1 Module 1 - Cybersecurity Essentials and Management for Maritime

3.1.1 CSP001_C_M: Cybersecurity Essentials and Management for Maritime

3.1.1.1 Description of Training Module

The module provides a comprehensive overview of cybersecurity's essential concepts and principles for managers and maritime cybersecurity aspiring professionals. ***This training module is specifically designed for individuals involved in the maritime sector, including seafarers, ship owners, port authorities, and maritime organisations, who seek to enhance their understanding of cybersecurity essentials and management principles***

It provides foundational skills and knowledge, including cybersecurity body-of-knowledge and management aspects. It equips participants with the knowledge and skills necessary to create a strategy to protect critical systems and data. The module covers a wide range of topics, including topics from the famous cybersecurity body of knowledge, the different types of cybersecurity threats and vulnerabilities, the principles of cybersecurity risk management, ethical and professional practices, soft skills needed to work in teams and the basic cybersecurity controls.

Table 1: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_C_M**
Module Title *The title of the training module*	**Cybersecurity Essentials and Management for Maritime**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	Cybersecurity Essentials for Maritime Cybersecurity Management Cybersecurity for the Modern Workplace- Cybersecurity Essentials and Principles A Comprehensive Overview of Cybersecurity Core Concepts for Maritime From Essentials to Management: Cybersecurity for Managers and Leaders Essential Cybersecurity Skills for Managers and Leaders Introduction to Information and Cyber Security for Maritime Management of Information Security

Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	C
Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This training module provides a foundational understanding of cybersecurity essentials and management principles, equipping participants with the knowledge and skills to manage information and cybersecurity in the maritime sector.
Module description *Indicates the main purpose and description of the module.*	This training module Cybersecurity Essentials and Management for the Maritime Sector provides a comprehensive introduction to cybersecurity for the maritime sector, equipping participants with the knowledge and skills to protect their organisations from cyber threats. Through a combination of interactive presentations, case studies, and practical exercises, participants will gain a deep understanding of cybersecurity fundamentals, human factor considerations, secure network architecture, security controls, incident response, compliance, and case studies.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge:** Define cybersecurity and its significance in the maritime sector. Identify and assess maritime cybersecurity threats. Understand the principles of cybersecurity risk management. Understand the principles of network segmentation, firewall configuration, and access control. Understand the importance of password security, multi-factor authentication (MFA), data encryption, and patch management. Understand the importance of incident response planning and procedures.

	Understand maritime cybersecurity regulations and guidelines. Analyse real-world maritime cybersecurity cases. **Skill and Competence:** Develop and execute cybersecurity risk management plans. Design and implement secure network architectures. Deploy and manage security controls for maritime systems. Develop and execute incident response plans. Comply with maritime cybersecurity regulations and guidelines. Apply cybersecurity concepts and techniques through practical exercises. Communicate cybersecurity risks, policies, and procedures effectively. Develop and maintain cybersecurity documentation. Demonstrate a willingness to stay up-to-date with the latest cybersecurity threats and trends.
Main topics and content list *A list of main topics and key content*	Understand the importance of ethical conduct and professionalism in maritime cybersecurity. Foundational Knowledge and Taxonomy of Maritime Cybersecurity Maritime Threats and Vulnerabilities Maritime Cybersecurity Risk Management Human Factor Considerations in Maritime Cybersecurity Secure Architecture Design and Implementation for Maritime Systems Security Controls Selection and Implementation for Maritime Environments Data Security and Privacy by Design for Maritime Operations Cybersecurity Governance for Maritime Organizations Maritime Cybersecurity Compliance and Regulations Case Studies and Practical Exercises

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Formative assessment*: Ongoing process of evaluating participants' learning during a training programme including pre-assessment, during and post-assessment in each training topic. It provides valuable feedback to instructors and participants, helping to ensure that learning goals are being met and that participants are making progress. *Summative assessment*: Learner needs to produce a targeted outcomes and deliverables at the end of the training by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to tackle the threats based on a real-world scenario.
Training Provider *Name(s) of training providers.*	LAU and UPRC
Contact *Name(s) of the main contact person and their email address.*	Prof. Nineta Polemi polemid@unipi.gr Paresh Rathod paresh.rathod@laurea.fi
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	12 weeks
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	**Mainly KA1** Minor content matches with other including KA2, KA3, KA4, KA5, KA6, KA10
Pre-requisites	Basic IT and Security Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	ECSF Profile 1: Chief Information Security Officer (CISO)
Tools to be used *A list of tools that will be used for the operation of this training module.*	Nmap, Nessus and Wireshark
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	Recommended equivalent to 5 ECTS

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *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.*	Refer and check online CyberSecPro DCM System for current information.

3.1.1.2 Adapted Syllabus

Table 2: Adapted Syllabus

Main topics	Suggested Content
Topic-1: Understanding the Importance of Ethical Conduct and Professionalism in Maritime Cybersecurity	Recognise the ethical principles that underpin cybersecurity practices. Understand the importance of responsible professional disclosure and ethical practices. Implement appropriate ethical guidelines and policies for maritime cybersecurity.
Topic-2: Foundational Knowledge and Taxonomy of Maritime Cybersecurity	Define maritime cybersecurity and its significance in the maritime domain. Understand the various components of a maritime cybersecurity ecosystem. Classify cybersecurity threats and vulnerabilities specific to maritime systems.

Topic-3: Maritime Threats and Vulnerabilities	Identify and categorise common maritime cybersecurity threats, such as malware, ransomware, phishing, and social engineering. Recognise the specific vulnerabilities that maritime systems face, including outdated software, weak passwords, and unpatched vulnerabilities. Understand the role of human error and insider threats in maritime cybersecurity incidents.
Topic-4: Maritime Cybersecurity Risk Management	Conceptualise maritime cybersecurity risk management and its importance. Identify and assess cybersecurity risks associated with maritime operations. Implement appropriate risk mitigation strategies to protect maritime systems and data. Continuously monitor and update cybersecurity risk management plans.
Topic-5: Human Factor Considerations in Maritime Cybersecurity	Recognise the role of human error as a significant contributor to cybersecurity incidents. Understand the psychology of cybersecurity threats and how they exploit human behaviour. Implement effective cybersecurity awareness training and education programs. Encourage a culture of cybersecurity vigilance and responsibility among maritime personnel.
Topic-6: Secure Architecture Design and Implementation for Maritime Systems	Design and implement secure network architectures for maritime systems. Utilise network segmentation to isolate critical systems and reduce the impact of cyberattacks. Configure firewalls and access control systems to protect maritime networks and restrict unauthorised access. Employ VPNs for secure remote access to maritime systems and sensitive data.
Topic-7: Security Controls Selection and Implementation for Maritime Environments	Select and implement appropriate security controls based on the specific needs of maritime systems. Implement strong password policies and multi-factor authentication (MFA) to protect user accounts. Encrypt sensitive data at rest and in transit to prevent unauthorised access and data breaches. Regularly apply security updates and patches to software systems to address vulnerabilities.

Topic-8: Data Security and Privacy by Design for Maritime Operations	Implement data security measures to protect sensitive maritime data, including personal information and operational data. Employ privacy by design principles to integrate data protection into the development and operation of maritime systems. Comply with relevant data privacy regulations and maritime cybersecurity guidelines.
Topic-9: Cybersecurity Governance for Maritime Organizations	Establish a comprehensive cybersecurity governance framework for maritime organisations. Designate a cybersecurity champion or team to oversee and manage cybersecurity initiatives. Develop and implement cybersecurity policies and procedures that align with organisational goals. Conduct regular cybersecurity risk assessments and audits to maintain an effective cybersecurity posture.
Topic-10: Maritime Cybersecurity Compliance and Regulations	Understand and comply with relevant maritime cybersecurity regulations, including IMO guidelines and BIMCO guidelines. Implement a process for monitoring and staying up-to-date with evolving cybersecurity regulations. Conduct periodic cybersecurity compliance audits to ensure adherence to regulatory requirements.
Topic-11: Case Studies and Practical Exercises	Analyse real-world maritime cybersecurity cases to gain insights into incident response strategies and mitigation techniques. Engage in hands-on cybersecurity exercises to reinforce knowledge and skills, such as vulnerability scans, penetration tests, and incident response simulations. Develop a practical cybersecurity awareness program for maritime personnel.

3.1.1.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.1.1.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.1.2 CSP001_S_M: Maritime Cybersecurity Certification Seminar

3.1.2.1 Description of Training Module

Table 3: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_S_ M**
Module Title *The title of the training module*	**Maritime Cybersecurity Certification Seminar**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Cybersecurity Essentials for Maritime Cybersecurity Management Cybersecurity for the Modern Workplace - Cybersecurity Essentials and Principles A Comprehensive Overview of Cybersecurity Core Concepts for Maritime From Essentials to Management: Cybersecurity for Managers and Leaders Essential Cybersecurity Skills for Managers and Leaders Introduction to Information and Cyber Security for Maritime Management of Information Security
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S)
Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This training module provides a foundational understanding of maritime cybersecurity essentials and management principles, equipping participants with the knowledge and skills to

	manage information and cybersecurity in the maritime sector.
Module description *Indicates the main purpose and description of the module.*	This training module Cybersecurity Essentials and Management for the Maritime Sector provides a comprehensive introduction to cybersecurity for the maritime sector, equipping participants with the knowledge and skills to protect their organisations from cyber threats. Through a combination of interactive presentations, case studies, and practical exercises, participants will gain a deep understanding of cybersecurity fundamentals, human factor considerations, secure network architecture, security controls, incident response, compliance, and case studies.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** Understanding of cybersecurity threats specific to the maritime sector. Familiarity with relevant cybersecurity frameworks, regulations, and standards governing maritime cybersecurity. Knowledge of cyber risks prevalent in maritime operations. Awareness of case studies and real-world examples of cybersecurity incidents in the maritime industry. Understanding of risk assessment methodologies and tools tailored to the maritime sector. Understanding of information security and maritime concepts. Understanding of best practices for securing maritime IT and OT systems. Knowledge of cybersecurity certification standards and schemes specific to the maritime industry. Familiarity with core concepts related to cybersecurity certification. Understanding of best practices for achieving and maintaining maritime cybersecurity certification.

	Skills & Competencies: Ability to identify and assess cybersecurity threats in maritime operations. Capacity in applying risk assessment methodologies and tools specific to the maritime sector. Competence in applying cybersecurity standards and best practices to safeguard maritime systems and infrastructure. Skill in interpreting and adhering to relevant cybersecurity standards and regulations in a maritime context. Ability to analyze case studies and real-world examples of cybersecurity incidents in the maritime industry. Competence in navigating and understanding cybersecurity certification standards and schemes applicable to the maritime sector. Capacity in utilizing cybersecurity certification methodologies to achieve compliance and certification in maritime cybersecurity. Competence in contributing to the overall cybersecurity posture and resilience of maritime organizations.
Main topics and content list *A list of main topics and key content*	Maritime, information security, and certification core concepts Cybersecurity threats in the maritime sector Cybersecurity frameworks, regulations, standards, and certification schemes applicable to the maritime industry Maritime cyber risks identification Maritime cybersecurity incidents case studies and real-world examples Risk assessment VS risk management Best practices for securing maritime IT and OT systems Best practices for maritime cybersecurity certification

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery by the instructor.
Training Provider *Name(s) of training providers.*	TUC, UPRC
Contact *Name(s) of the main contact person and their email address.*	Pinelopi Kyranoudi pkyranoudi@tuc.gr, Prof. Nineta Polemi dpolemi@gmail.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted in DCM
Duration *Duration of the training.*	To be posted in DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*KA1 – Cybersecurity Management* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance*
Pre-requisites	Basic IT knowledge

Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	CHIEF INFORMATION SECURITY OFFICER (CISO) CYBER LEGAL, POLICY & COMPLIANCE OFFICER CYBER THREAT INTELLIGENCE SPECIALIST CYBERSECURITY AUDITOR CYBERSECURITY IMPLEMENTER CYBERSECURITY RISK MANAGER
Tools to be used *A list of tools that will be used for the operation of this training module.*	Information and maritime security standards, guidelines and certification schemes (e.g., ISO 27001, Common Criteria, IMO, NIST, ENISA, EUCC) CYSMET Risk Management Methodology CYRENE Risk and Conformity Assessment Methodology
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	N/A
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	To be posted in DCM
Other important dates *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.*	To be posted in DCM

3.1.2.2 Adapted Syllabus

Table 4: Adapted Syllabus

Main topics	Suggested Content
1. Introduction to Maritime Cybersecurity	Overview of cybersecurity threats in the maritime sector Importance of maritime cybersecurity Introduction to relevant cybersecurity frameworks and regulations (e.g., IMO Guidelines on Cyber Risk Management)
2. Understanding Maritime Cyber Risks	Identification of cyber risks in maritime operations Case studies and real-world examples of cybersecurity incidents in the maritime industry Risk assessment VS risk management
3. Cybersecurity Standards and Best Practices	Overview of cybersecurity standards applicable to the maritime industry (e.g., ISO 27001, NIST Cybersecurity Framework) Overview of information security and maritime core concepts Best practices for securing maritime IT and OT systems (e.g., ENISA Guidelines - Cyber Risk Management for Ports, CYSMET Risk Management Methodology)
4. Maritime Cybersecurity Certification	Cybersecurity certification standards and schemes applicable to the maritime industry (e.g., Common Criteria, EUCC) Overview of cybersecurity certification core concepts Best practices for maritime cybersecurity certification (e.g., CYRENE Risk & Conformity Assessment Methodology)

3.1.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.1.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.1.3 CSP001_CS-E_M: RxB - Cyber security management game

3.1.3.1 Description of Training Module

RxB is an asymmetrical strategy game about cyber-attacks and defence. You play as the blue team trying to protect your system against various attacks from the red team. Your goal is to find vulnerability in your system and learn how to respond to threats. The module introduces the well-known red vs. blue approach to understanding cybersecurity through gamification. The game covers essential concepts and management strategies in the context of cybersecurity within the maritime sector. The learning material is targeted toward beginners/intermediates in the cybersecurity field, and therefore requires the user to have a basic knowledge of cybersecurity frameworks and terms. It may appeal to security managers or IT-support employees working in the maritime sector, who want to expand their knowledge. Additionally, it may also appeal to university students who study IT and cybersecurity on a basic level. The RxB game aims to equip users with knowledge of different cyber security protocols as well as a variety of cyberattacks that occur in the maritime industry on a regular basis.

Table 5: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_CS-E_H**
Module Title *The title of the training module*	**RxB - Cyber security management game**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	"Cyber security management game" "RxB - cyber security game" "Educational game for teaching cyber security management"
Training offering type *Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O).*	CS-E
Level *Training level: B (Basic), A (Advanced)*	B (Basic)

Module overview *High-level module overview*	The training module will consist of a playthrough of the "RxB - Cyber security management" game. The users will play through a maritime specific training scenario, where they will play as a cyber security manager.
Module description *Indicates the main purpose and description of the module.*	The player's goal is to identify vulnerabilities in their network, detect threats and protect your assets, so their company avoids any major damage from outside cyber attacks. In the game the players will have to assign their team members (non-playable characters), to various tasks and improve their skill sets as the game progresses. Throughout the game, the Red team (hackers) will continuously try and breach your security and exploit various vulnerabilities. The maritime section of the game will feature a number of different events and assets that are specific to the given sector. No practical technical skill is required to play. However, it helps to know about cybersecurity terminology and concepts - if not, the user will learn by failing.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner should have gained an understanding of various concepts in the following areas: **Knowledge:** Cybersecurity Essentials and Management **Skill and Competence:** Risk assessment, prioritisation and resource management Recognize different types of vulnerabilities Learn about various attack vectors and strategies Learn about various defensive mitigations and strategies Learn about protocols from the NIST framework
Main topics and content list *A list of main topics and key content*	RxB aims to deliver more awareness within the following topics: Cyber security defences require regular adjustment Promote situation awareness by navigating through an active attack Familiarisation with hacker and cyber defence terminology How and when specific protocols are used in the NIST framework

Training Provider *Name(s) of training providers.*	Serious Games Interactive Louise Præstin Martin Bärmann
Contact *Name(s) of the main contact person and their email address.*	lp@seriousgames.dk mba@seriousgames.net
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	45 minutes exercise
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	**Mainly KA1** Secondary areas would include: KA2 and KA3
Pre-requisites	Basic IT and Security Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF.*	ECSF Profile 1: Chief Information Security Officer (CISO)

Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	Not applicable.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	NA
Other important dates	NA

3.1.3.2 Adapted Syllabus

Table 6: Adapted Syllabus

Main topics	Suggested Content
Threats and Vulnerabilities for maritime Sector	Signs of threats or cyber security breaches Introduction to network assets and asset specific vulnerabilities. Introduction to the NIST protocols.
Introduction to Human Aspects of maritime Cybersecurity	Examples based on case studies from real-world maritime incidents. Consequences of neglecting the human factor in the maritime sector.

3.1.3.3 Planning for Preparedness

The training can be carried out both virtually or physically. When carried out virtually, the game would either be sent out as a link, or hosted on an online platform that distributes learning materials. The game will primarily work as a self-facilitated exercise, and it is therefore not a requirement that facilitators are present during the exercise. The exercise can be carried out at any physical location, as long as the user has a computer and internet connection.

3.1.3.4 Materials and Exercises

The cybersecurity exercise only requires the user to have a computer, internet connection and a method of distribution for the game. Examples of distribution channels could be the form of email, online platforms, QR codes or similar methods.

3.2 Module 2 - Human Factors and Cybersecurity for Maritime

3.2.1 CSP002_S_M: Human Factors and Cybersecurity

3.2.1.1 Description of Training Module

This module is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing.

Table 7: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	CSP002_S_M: Human Factors and Cybersecurity
Module Title *The title of the training module*	**Human Aspects of Maritime Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	The Human Dimension in Maritime Cybersecurity Navigating Maritime Cyber Threats: The Human Element Elements of Cyberpsychology in Maritime” Humans in Maritime Cybersecurity Human centric cyber defence in maritime domains
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S

Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	The module aims to provide maritime stakeholders with the knowledge necessary about human aspects of cybersecurity pertinent for the maritime domain, both at the individual and organisational levels, as well as at the strategic, operational, and tactical levels
Module description *Indicates the main purpose and description of the module.*	This course navigates through the human aspects of maritime cybersecurity, examining the psychological, social, and organizational influences on security practices and decisions in a maritime context. Attendees will uncover insights into human vulnerabilities that cyber attackers target in maritime operations and acquire methods to cultivate a cybersecurity-aware culture within maritime organizations. It further highlights the vital importance of communication and collaboration at strategic, operational, and tactical levels specific to the maritime sector. Participants will investigate how proficient communication between maritime domains and effective decision-making can strengthen cybersecurity measures in maritime operations.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge:** · Gain an understanding of the psychological, social, and organizational elements that shape cybersecurity actions within the maritime domain. · Understand the critical role of communication and teamwork in bolstering maritime cybersecurity across different sectors. · How decision-making frameworks are used at strategic, operational, and tactical levels within maritime cybersecurity. · Recognize the profiles and strategies of adversaries targeting maritime operations. · Evaluate human-related threats and vulnerabilities in maritime contexts. **Competencies:** · Understand the discussions pertinent to maritime cybersecurity at various levels of decision-making. · Cultivate an environment of transparent communication and teamwork focused on maritime cybersecurity.

	· Reflect on cybersecurity decision-making with the understanding of how human factors are related in the maritime arena. · Identify human-centric threats and vulnerabilities in maritime operations.
Main topics and content list *A list of main topics and key content*	Ethical and professional practices Introduction to Human Aspects of Maritime Cybersecurity Psychological and Social Factors in Maritime Cybersecurity Human Vulnerabilities in Maritime Cybersecurity Organisational Culture, Communication, and Cybersecurity Communication and Collaboration Across Domains Decision Making at Strategic, Operational, and Tactical Levels Training, Awareness, and Communication Programs for Maritime personell Future Trends, Challenges, and the Role of Communication
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Formative assessment*: Learner needs to answer short questions to show an understanding of different human aspects *Summative assessment*: Learner needs to produce a 1500-word report based on a maritime cybersecurity case study that reflects over different human aspects of a maritime cybersecurity breach
Training Provider *Name(s) of training providers.*	TalTech, Trustilio
Contact *Name(s) of the main contact person and their email address.*	Ricardo Lugo Ricardo.Lugo@taltech.ee Kitty Kioskli kitty.kioskli@trustilio.com Paresh Rathod Paresh.Rathod@laurea.fi

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	6 hours
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*(2)Human Aspects of Cybersecurity* *(7) Cybersecurity Threat Management*
Pre-requisites	None

Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Cybersecurity Educator Chief Information Security Officer Cybersecurity Researcher Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this training module.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	3 Summer school
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.2.1.2 Adapted Syllabus

Table 8: Adapted Syllabus

Main topics	Suggested Content
Introduction to Human Aspects of Maritime Cybersecurity	Maritime Cybersecurity landscape Cost of neglecting the human element Examining real-world maritime incidents
Psychological and Social Factors in Maritime Cybersecurity	Understanding cognitive biases Social engineering techniques Group dynamics
Human Vulnerabilities in Maritime Cybersecurity	Insider threats Impact of stress and fatigue Case studies Mitigation strategies
Organisational Culture, Communication, and Maritime Cybersecurity	Organisational values Leadership's role Proactive security culture for maritime
Communication and Collaboration Across Domains	Effective communication Role of mediators
Decision Making at Strategic, Operational, and Tactical Levels	Layers of decision-making Role of data-driven decision-making.
Training, Awareness, and Communication Programs	Designing Impactful training Role of Continuous education Leveraging technology to enhance training
Future Trends, Challenges, and the Role of Communication	Anticipating threats Role of Emerging technologies in maritime. AI and automation

3.2.1.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.2.1.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.2.2 CSP002_SS_M: Human Factors and Cybersecurity

3.2.2.1 Description of Training Module

This module is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing.

Table 9: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	CSP002_SS_M: Human Factors and Cybersecurity
Module Title *The title of the training module*	**Human Aspects of Maritime Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	The Human Dimension in Maritime Cybersecurity Navigating Maritime Cyber Threats: The Human Element Elements of Cyberpsychology in Maritime” Humans in Maritime Cybersecurity Human centric cyber defence in maritime domains
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	SS
Level *Training level: B (Basic), A (Advanced)*	A (Advanced)

Module overview *High-level module overview*	The module aims to provide maritime stakeholders with the knowledge necessary about human aspects of cybersecurity pertinent for the maritime domain, both at the individual and organisational levels, as well as at the strategic, operational, and tactical levels
Module description *Indicates the main purpose and description of the module.*	This course navigates through the human aspects of maritime cybersecurity, examining the psychological, social, and organizational influences on security practices and decisions in a maritime context. Attendees will uncover insights into human vulnerabilities that cyber attackers target in maritime operations and acquire methods to cultivate a cybersecurity-aware culture within maritime organizations. It further highlights the vital importance of communication and collaboration at strategic, operational, and tactical levels specific to the maritime sector. Participants will investigate how proficient communication between maritime domains and effective decision-making can strengthen cybersecurity measures in maritime operations.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge:** Gain an understanding of the psychological, social, and organizational elements that shape cybersecurity actions within the maritime domain. Understand the critical role of communication and teamwork in bolstering maritime cybersecurity across different sectors. How decision-making frameworks are used at strategic, operational, and tactical levels within maritime cybersecurity. Recognize the profiles and strategies of adversaries targeting maritime operations. Evaluate human-related threats and vulnerabilities in maritime contexts. How to implement cybersecurity trainings in maritime operations **Skills:** Use effective communication plans tailored to maritime cybersecurity needs. Detect and counteract human-centric threats and vulnerabilities in maritime operations. Engage with interdisciplinary teams to tackle the human dimensions of cybersecurity in maritime settings. Examine real-world maritime cybersecurity breaches to pinpoint human errors and lapses in communication.

	Classify adversaries targeting maritime interests and scrutinize their tactics. Design and evaluate cybersecurity trainings tailored for maritime domains. **Competencies:** Lead the discussions pertinent to maritime cybersecurity at various levels of decision-making. Cultivate an environment of transparent communication and teamwork focused on maritime cybersecurity. Understand the needs of training within cybersecurity
Main topics and content list *A list of main topics and key content*	Ethical and professional practices Introduction to Human Aspects of Maritime Cybersecurity Psychological and Social Factors in Maritime Cybersecurity Human Vulnerabilities in Maritime Cybersecurity Organisational Culture, Communication, and Cybersecurity Communication and Collaboration Across Domains Decision Making at Strategic, Operational, and Tactical Levels Training, Awareness, and Communication Programs for Maritime personell Future Trends, Challenges, and the Role of Communication
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Formative assessment*: Learner needs to answer short questions to show an understanding of different human aspects *Summative assessment*: Learner needs to produce a 3000-word report based on a maritime cybersecurity case study that reflects over different human aspects of a maritime cybersecurity breach and possible mitigation strategies at the individual and organisational level, develop a training plan for promoting cybersecurity behaviours in maritime personell.
Training Provider *Name(s) of training providers.*	TalTech, Trustilio

Contact *Name(s) of the main contact person and their email address.*	Ricardo Lugo Ricardo.Lugo@taltech.ee Kitty Kioskli kitty.kioskli@trustilio.com Paresh Rathod Paresh.Rathod@laurea.fi
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	1 week
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies*	*(2)Human Aspects of Cybersecurity* *(7) Cybersecurity Threat Management*

KA9 – Penetration Testing *KA10 – Cyber Incident Response*	
Pre-requisites	None
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Cybersecurity Educator Chief Information Security Officer Cybersecurity Researcher Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this training module.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	3 Summer school
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.2.2.2 Adapted Syllabus

Table 10: Adapted Syllabus

Main topics	**Suggested Content**
Introduction to Human Aspects of Maritime Cybersecurity	Maritime Cybersecurity landscape Cost of neglecting the human element Examining real-world maritime incidents
Psychological and Social Factors in Maritime Cybersecurity	Understanding cognitive biases Social engineering techniques Group dynamics
Human Vulnerabilities in Maritime Cybersecurity	Insider threats Impact of stress and fatigue Case studies Mitigation strategies
Organisational Culture, Communication, and Maritime Cybersecurity	Organisational values Leadership's role Proactive security culture for maritime
Communication and Collaboration Across Domains	Effective communication Role of mediators
Decision Making at Strategic, Operational, and Tactical Levels	Layers of decision-making Role of data-driven decision-making.
Training, Awareness, and Communication Programs	Designing Impactful training Role of Continuous education Leveraging technology to enhance training
Future Trends, Challenges, and the Role of Communication	Anticipating threats Role of Emerging technologies in maritime. AI and automation

3.2.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.2.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.3 Module 3 - Cybersecurity Risk Management and Governance for Maritime

3.3.1 CSP003_S_M: Cybersecurity Risk Management and Governance for Maritime

3.3.1.1 Description of Training Module

Table 11: Description of Training Module

Code *Code format: CSP003_x where x is the training of offering type (see below)*	**CSP003_ S_M**
Module Title *The title of the training module*	**Maritime Cybersecurity Risk Management and Governance**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Information Security Risk Management Security Management Trust Management Risk Assessment and Management Enterprise Risk Management Risk Assessment and Mitigation Risk Control and Governance Risk Minimization Strategies Risk Analysis and Remediation Risk Mitigation and Compliance Strategic Risk Planning Risk Avoidance and Management Threat Management and Mitigation Risk Intelligence and Decision-Making

Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S)
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	This module focuses on acquainting maritime stakeholders with the principles and requirements in relation to security and privacy of Information Systems (IS). The technical, legal and policy aspects of risk analysis and management will be addressed.
Module description *Indicates the main purpose and description of the module.*	This module aims to to provide the basic principles, phases and methodologies for risk assessment of maritime systems and their supply chains.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** Basic definitions related to Information Security Management Systems and Information Security Governance Basic phases and principles for an effective risk management methodology for port facilities and ships. Standards and Methodologies of Risk Management of maritime assets. Legal and Policies related to Risk Management published by IMO, ENISA, BIMCO Measurements, Scales and Metrics of Risks Technical and non Technical Mitigation Actions appropriate for the security of port and ships operations.

	Skills: (applying) a suitable methodology for Information Security Risk Management and Risk Assessment applicable to maritime ecosystems;. (analysing) Information Security Risk utilising different methodologies; (creating) policies, procedures Select and implement appropriate mitigation actions and controls based on IMO guidelines (ISPS, ISM Code); Develop Security Policy and Procedures Develop BCS, DRP; Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards; Analyse and consolidate organisation's quality and risk management practices **Competencies:** Lead and participate in strategic, operational, and tactical maritime cybersecurity discussions. Lead the design, development, operation and improvement of an Port/vessel Information Security Management System. Support ports in enhancing their cybersecurity; Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories Knowledge of cybersecurity-related technologies and controls Knowledge of monitoring, implementing,
Main topics and content list *A list of main topics and key content*	Maritime threat landscape Risk management related standards The scope and purpose of an Information Security Management System Information Security Risk Management definitions and principles Maritime cyber-Threats and vulnerabilities Measurements and Metrics Risk assessment and management processes and methodologies Security Reports

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery orally by the instructor.
Training Provider *Name(s) of training providers.*	UPRC, SLC, APIRO, AIT
Contact *Name(s) of the main contact person and their email address.*	polemi@gmail.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	5-7/2/2024: Duala, Cameroon To be posted in DCM
Duration *Duration of the training.*	To be posted in DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual and Physical
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*(1)Cybersecurity Management* *(3)Cybersecurity Risk Management* *(4)Cybersecurity Policy, Process, and Compliance*

Pre-requisites	Basic IT training
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	CHIEF INFORMATION SECURITY OFFICER (CISO) CYBER LEGAL, POLICY & COMPLIANCE OFFICER CYBERSECURITY AUDITOR CYBERSECURITY RISK MANAGER
Tools to be used *A list of tools that will be used for the operation of this training module.*	Mitigate, Risk calculators
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek, Portuguese
ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	To be posted in DCM
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	To be posted in DCM
Other important dates *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.*	To be posted in DCM

3.3.1.2 Adapted Syllabus

Table 12: Adapted Syllabus

Main topics	Suggested Content
Introduction to Information Security	Threat and attack landscape in the maritime sector
Maritime cybersecurity standards and best practices	ISO, IMO, BIMCO relative standards, ENISA guidelines, IMO MSC-FAL 1/Circ 3 guidelines
The scope and purpose of an ISMS	Within this topic, information is provided on what is an ISMS and which are the benefits and objectives of its implementation in the ports and vessels.
Information Security Risk Management definitions and principles Threats and vulnerabilities ISO 27005 and ISO 31000 basic structure, IMO/BIMCO guidelines	The phases of a risk management process are explained and an exercise is performed to cover the following phases: Context - Risk identification - Risk Analysis - Risk Evaluation - Risk Treatment of the maritime systems and their supply chains
Threat Models and Technical Vulnerabilities and Measurements	Technical and non technical threats and vulnerabilities will be analysed. The various metrics systems (e.g. CVE, CVSS4, CWE) will be presented and illustrated with various examples.
Other Risk Assessment methodologies and tools	This topic introduces a list of risk assessment methodologies and tools appropriate for the maritime sector (e.g ENISA 2019) .
Security Policies and Procedures	The development of security policy, BCP, DRP and procedures based on standards will be covered in this section.

3.3.1.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.3.1.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.3.2 CSP003_S_M: Cybersecurity Risk Management and Governance for Maritime

3.3.2.1 Description of Training Module

Table 13: Description of Training Module

Code	**CSP003_S_ M**
Module Title	Cybersecurity Risk Management and Governance for Maritime Sector
Alternative Title(s)	Management of Risk and Goverance in Maritime
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S)
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	The course imparts an understanding of the underlying principles associated with the cybersecurity risk management for the maritime sector.
Module description *Indicates the main purpose and description of the module.*	The aim of the module is to provide the learner with the ability to assess and manage cybersecurity risk and critically evaluate the protection mechanisms used to ensure security and governance of the maritime sector. It provides an understanding of current security threats and vulnerabilities trends within the maritime sector and gain knowledge to ensure governance for the maritime sector.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge and understanding:** Demonstrate an in-depth understanding of cyber security risk management and governance in maritime sector. Identify and critically analyse the assets and their dependencies. Recognise the significant of governance structures and processes in maritime sector

	Skill and Competence: Critically evaluate information assets and assess their vulnerabilities and threats for the systems within the maritime supply chain. Demonstrate an in-depth understanding of an effective security governance and document accordingly in a professional manner.
Main topics and content list *A list of main topics and key content*	An overview of cyber security, threats and vulnerabilities in maritime sector Maritime assets and their dependencies Risk Management framework, qualitative and quantitative risk assessment Governance processes Security controls and industry specific standards related to security management and governance
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Summative assessment: This assessment component assess the learners' knowledge based on the topics covered by the module through presentation and viva.
Training Provider *Name(s) of training providers.*	SLC
Contact *Name(s) of the main contact person and their email address.*	Prof. Shareeful Islam, Shareeful@gmail,com Athina Labropoulou , athina.labropoulou@securitylabs.ie
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted in DCM
Duration *Duration of the training.*	To be posted in DCM

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual and Physical
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*KA1 – Cybersecurity Management* *– Cybersecurity Risk Management*
Pre-requisites	Basic IT and security Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Chief Information Security Officer (CISO) Cyber Legal, Policy & Compliance Officer Cybersecurity Auditor Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this training module.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	N/A

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.3.2.2 Adapted Syllabus

Table 14: Adapted Syllabus

Main topics	Suggested Content
Topic 1: Cyber security in maritime sector	An overview of cyber security, threats and vulnerabilities in maritime sector Maritime assets and their dependencies
Topic 2: Risk Management framework	Risk management Basics Principles of risk management and process Threats and vulnerability management for maritime sector
Topic 3: Governance processes and control	Introduction to security governance process Introduction to ISO/IEC 27001 and controls (Clauses 1-4 and Annex A). ISO 27001:2022 / ISO/IEC 27002:2022 control themes Terms and definitions of ISO 27000 adapted to the energy utility domain Guidance on the controls of ISO/IEC 27002:2022 adapted to the energy utility domain. Ships and marine technology security control

3.3.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.3.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.4 Module 4 - Network Security for Maritime

3.4.1 CSP004_C_M: Network Security for Maritime

3.4.1.1 Description of Training Module

Table 15: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP004_S_M**
Module Title *The title of the training module*	**Security Aspects for Maritime Networks**
Alternative Title(s) *Used alternative titles for the same module by many instututes and raining providers*	Network Security Management in the Maritime Domain Security Strategies for Maritime Networks Secure Network Architectures for the Maritime Domain Protecting Network Infrastructure in the Maritime Domain System and Network Security for Maritime Systems
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S (Seminar)
Level *Training level: B (Basic), A (Advanced)*	A (Advanced)

Module overview *High-level module overview*	This seminar will provide participants with the necessary knowledge to identify and address potential security problems and threats associated with the emergence of various types of communication networks within port infrastructures and the maritime domain in general. Participants will learn about most common vulnerabilities and threats for specific network systems. This seminar will also focus on concepts, techniques and tools to protect the networks within maritime infrastructures and describe the important concepts of networks security.
Module description *Indicates the main purpose and description of the module.*	In the beginning, the participants will get a general overview on communication networks and how they are used in the maritime domain. This will be accompanied by a selection of recent or most prominent attacks that happened in the maritime domain, i.e., on port infrastructures or vessels, together with a description of the attack vector and the consequences in the maritime sector. Then, the seminar will cover design principles and architecture examples for building secure networks for the maritime domain, including topics such as network segmentation and isolation, security zones and conduits. In that context, the importance of security devices for network infrastructures in the maritime domain will be discussed. The seminar will also look at the basic cryptographic principles required for securing data transmissions and where the are applied in the maritime domain. Finally, a list of security mechanisms will be discussed that can be applied along the OSI reference model to achieve the security objectives. Moreover, the participants will learn how these mechanisms can protect against or counter the different types of attacks that are commonly seen in maritime network infrastructures.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	A comprehensive understanding of the challenges, strategies, and best practices involved in securing maritime networks against multiple threats from various threat actors, the ability to design and build secure network infrastructures as well as the understanding of attack strategies and respective security mechanisms to prevent or counter them.
Main topics and content list *A list of main topics and key content*	• Introduction to communication networks • Recent Attacks and their Effects in the Maritime Sector • Secure Network Architecture and Design • Overview on Cryptographic Techniques • Security Mechanisms, Services and Attacks

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery orally by the instructor.
Training Provider *Name(s) of training providers.*	AIT
Contact *Name(s) of the main contact person and their email address.*	Stefan Schauer (stefan.schauer@ait.ac.at) Abdelkader Shabaan (abdelkader.shabaan@ait.ac.at)
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	TBA
Duration *Duration of the training.*	4 hours
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual or Hybrid
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance*	*(5) Network and Communications Security*

KA5 – Network and Communication Security *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	
Pre-requisites	Basic IT training + suggested minimum know-how in above section
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Chief Information Security Officer (CISO), Chief Security Officer (CSO) Network Security Architect Network Security Specialist
Tools to be used *A list of tools that will be used for the operation of this training module.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, German
ECTS *If applicable, the number of ECTS.*	N/A
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	TBD

Other important dates *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.*	TBD

3.4.1.2 Adapted Syllabus

Table 16: Adapted Syllabus

Main topics	Suggested Content
Secure Network Architecture and Design	This topic will discuss building a cyber security resilience system for the maritime sector. It will include a risk management approach, including types of cyber threats, security vulnerabilities, and the countermeasures that should be considered for mitigating cyber risks. Additionally, it will explore the multiple categories of security requirements based on ISA/IEC 62443 security standard, which describes different categories of system components and multiple levels of protection to ensure improved security. Furthermore, it will address how segmentation and isolation are applied to create security zones and conduits to meet specific security requirements for securing maritime assets.
Cryptographic Techniques for Ensuring Secure Data Transmission	This topic will cover the basic concepts of cryptography, including encryption and decryption, and will present the differences between symmetric and asymmetric encryption approaches, including some examples of each mechanism. Additionally, it will provide an overview of digital signatures and explain their importance in ensuring the authentication of digital data transmission among computer networks.
Security mechanisms, services, and attacks in OSI reference model	This part will introduce the X.800 security architecture for OSI and provide details about the OSI security architecture. It will focus on various types of security attacks, services, and mechanisms. Additionally, it will discuss the placement of security services and mechanisms within the OSI framework. Moreover, it will describe the different types of security attacks that could pose threats to computer network security.

3.4.1.3 Planning for Preparedness

The course can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable presenters, location (in case it is a physical seminar) or tools (in

case it is delivered online). Students should have a laptop or desktop and a good internet connection for physical and/or online lessons.

3.4.1.4 Materials and Exercises

The training seminar is supported by the following material:

Presentation material that will be used during the course and be provided digitally to the trainees.

3.4.2 CSP004_S_M: Network Security for Maritime

3.4.2.1 Description of Training Module

Table 17: Description of Training Module

Code *Code format: CSP003_x where x is the training of offering type (see below)*	**CSP004_S_ M**
Module Title *The title of the training module*	**Network Security for Maritime**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Computer Networks and Security Network Security Introduction to Network Security Network Security: Attacks and Defences
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S)
Level *Training level: B (Basic), A (Advanced)*	B

Module overview *High-level module overview*	This module focuses on introducing the basic security threats and defences in networked systems with emphasis on maritime.
Module description *Indicates the main purpose and description of the module.*	Maritime systems are often interconnected and exchange information using the network; the module introduces the basic principles for guarding a networked communication from external threats.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, participants will have gained the following: **Knowledge:** Understand network threats and threat models affecting different OSI layers Understand the role of cryptography in network security Understand how TLS can safeguard the network for Man-in-the-Middle attackers **Skills:** Apply the right defences for relevant threats in the network Configuration and handling of TLS and certificates **Competencies:** Knowledge of how cryptographic principles protect network communications Support ports in enhancing their cybersecurity Knowledge of cyber threats, threats taxonomies Knowledge of cybersecurity-related technologies and controls

Main topics and content list *A list of main topics and key content*	Introduction to OSI layers with a focus on security Attacks and defences for networked systesm TLS
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery orally by the instructor.
Training Provider *Name(s) of training providers.*	UCY
Contact *Name(s) of the main contact person and their email address.*	Elias Athanasopoulos, athanasopoulos.elias@ucy.ac.cy
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted in DCM
Duration *Duration of the training.*	To be posted in DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual and Physical

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*Network and Communication Security*
Pre-requisites	Basic IT training
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	CHIEF INFORMATION SECURITY OFFICER (CISO)
Tools to be used *A list of tools that will be used for the operation of this training module.*	-
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek

ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	To be posted in DCM
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	To be posted in DCM
Other important dates *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.*	To be posted in DCM

3.4.2.2 Adapted Syllabus

Table 18: Adapted Syllabus

Main topics	Suggested Content
Introduction to Network Security	Introduction to the main security issues arising when systems are networked
Network Attacks	Overview of basic threat models, such as Man-in-the-Middle
TLS	Leverage cryptography for protecting communications from specific attacks

3.4.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.4.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.5 Module 5 - Data Protection and Privacy Technologies for Maritime

3.5.1 CSP005_SA_M: Data Protection and Privacy Technologies for Maritime

3.5.1.1 Description of Training Module

Data protection and privacy technologies for maritime environments are crucial due to the increasing digitization of maritime operations and the sensitivity of data involved. The implementation of a comprehensive approach that combines related technologies and practices may significantly enhance data protection and privacy in maritime environments, safeguarding sensitive information against cyber threats and ensuring compliance with relevant regulations.

Shipping companies maintain access to personal data of various sources, including personnel, agents, customers, etc. They store and process large amounts of data, and even transfer data across borders and legislations. Market reports indicate that maritime companies experience an increased number of cyber-attacks, that may even become fatal in some cases, especially if they orient vulnerable onboard systems. In any case, they have to be compliant with the GDPR.

Table 19: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP005_SA_M**
Module Title *The title of the training module*	**Data Protection and Privacy Technologies for Maritime**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	-
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S
Level *Training level: B (Basic), A (Advanced)*	B (Basic)

Module overview *High-level module overview*	This training seminar provides an introduction to the data protection and privacy technologies for the maritime industry. This includes (a) Data protection, (b) Privacy and online rights, (c) Application on the maritime industry.
Module description *Indicates the main purpose and description of the module.*	This training seminar provides an introduction to the data protection and privacy technologies for the maritime industry. This includes (a) Data protection, like subject matters and regulatory focus, international data transfer, personal data breach, GDPR, etc. (b) Privacy and online rights, including privacy and control, privacy and transparency, etc. (c) Application on the maritime industry, including the application of GDPR in maritime, privacy be design and privacy by default, risk assessment in the maritime industry, cybersecurity maritime, etc.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon completion of this module the trainee will be able to: **Knowledge:** Understand the key terms used in data protection law. Understand data subject rights, including access rights and the right to be forgotten. Recognise the responsibilities of data controllers, data processors and data protection officers. Define what privacy is Explain what a privacy breach is and list the three most common types of privacy breaches that occur Define and distinguish privacy and confidentiality Implement the GDPR in maritime Recognize privacy be design and privacy by default Implement risk assessment frameworks Implement cybersecurity principles in maritime **Skill and Competence:** Implement data protection plans in the maritime industry Allocate work to data controllers, data processors and data protection officers Design and implement data breach protection plans Implement GDPR in the maritime industry Implement cybersecurity principles in maritime Develop and execute risk assessment plans

Main topics and content list *A list of main topics and key content*	Data protection, Subject matter and regulatory focus Core regulatory principles Investigation and prevention of crime and similar activities Security measures Assessment and design of processing systems International data transfer Personal data breach Enforcement and penalties Privacy technologies Privacy and online rights Privacy as confidentiality Privacy and control Privacy as transparency Privacy technologies and democratic values Privacy engineering Applications in maritime GDPR in maritime Privacy by design and privacy by default Risk assessment in the maritime industry Cybersecurity in maritime
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Summative assessment multiple choice questions will be used to assess the completion of learning learning outcomes. There will be at least one assessment question per learning outcome.
Training Provider *Name(s) of training providers.*	MAG and SLC
Contact *Name(s) of the main contact person and their email address.*	Spiros Borotis, George Kliafas spiros.borotis@maggioli.gr , george.kliafas@maggioli.gr

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM and the CSP website
Duration *Duration of the training.*	12 hours seminar (learning equivalent)
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual (link to the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	**Mainly KA6** Content matches KA2, KA3, KA4, KA6
Pre-requisites	Basic IT Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Cyber Legal, policy & compliance officer Cybersecurity auditor

Tools to be used *A list of tools that will be used for the operation of this training module.*	-
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	-
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *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.*	Refer and check online CyberSecPro DCM System for current information.

3.5.1.2 Adapted Syllabus

Table 20: Adapted Syllabus

Main topics	Suggested content
Data protection	Subject matter and regulatory focus Core regulatory principles Investigation and prevention of crime and similar activities Security measures Assessment and design of processing systems International data transfer Personal data breach

	Enforcement and penalties
Privacy technologies	Privacy and online rights Privacy as confidentiality Privacy and control Privacy as transparency Privacy technologies and democratic values Privacy engineering
Applications in maritime	GDPR in maritime Privacy by design and privacy by default Risk assessment in the maritime industry Cybersecurity in maritime

3.5.1.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.5.1.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.6 Module 6 - Cyber Threat Intelligence for Maritime

3.6.1 CSP006_SA_M: Cyber Threat Intelligence for Maritime

3.6.1.1 Description of Training Module

Table 21: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP006_S_M**
Module Title *The title of the training module*	**Cyber Threat Intelligence and sharing in the SeaPort**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	Cybersecurity Intelligence Collaboration Threat Intelligence Exchange Security Threat Information Sharing Cyber Threat Analysis and Collaboration Intelligence-driven Cyber Defense Threat Information Collaboration Cybersecurity Intelligence Fusion Collaborative Threat Mitigation Intelligence-led Cybersecurity Threat Sharing and Analysis
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S
Level *Training level: B (Basic), A (Advanced)*	A (Advance)
Module overview *High-level module overview*	The module aims to provide maritime stakeholders with an overview of threat intelligence. It allows the learners to analyse the known and unknown threats and determine the actions to tackle them.

Module description *Indicates the main purpose and description of the module.*	The module provides an understanding of the underlying properties and principles associated with cyber threats within a maritime organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence. Upon completion of the module, the learners can adopt the knowledge and skill to analyse the threats in their organisational context.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge:** Demonstrate knowledge and understanding of threats Attacks and Attack actors Critically evaluate the cyber threats of an organisation by following threat intelligence properties. **Skill and Competence:** Analyse the results of a threat assessment and provide recommendations. Ability to perform vulnerability assessment and measure how it contributes to threat mitigation. Critically evaluate the necessity of threat hunting techniques and threat intelligence as protection mechanisms.
Main topics and content list *A list of main topics and key content*	Cyber threats taxonomy and threat intelligence Vulnerabilities assessment techniques Threat modelling Threat hunting concept and standard Threat intelligence information sharing standard, reporting, and feed Security controls and standards
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Summative assessment*: Learner needs to produce a 2000-word report at the end of the module by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to part of port facility or vessel.

Training Provider *Name(s) of training providers.*	UPRC, AIT
Contact *Name(s) of the main contact person and their email address.*	Prof. Nineta Polemi polemid@unipi.gr
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	6 hours
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*(1)Cybersecurity Management* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology*

Pre-requisites	Basic IT and security Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Cyber Threat Intelligence Specialist Cybersecurity Implementer
Tools to be used *A list of tools that will be used for the operation of this training module.*	CVSS v4.0 calculator
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.6.1.2 Adapted Syllabus

Table 22: Adapted Syllabus

Main topics	Suggested Content
Cyber threats taxonomy and threat intelligence for port authorities and ships	Cyber threats and types of threats Attacks and Mitigations Attack actors Advanced persistent threat
Legal Instruments and Standards	Relevant EU cybersecurity legislation EU cybersecurity standards, IMO/BIMCO guidelines
Threats and Attacks in the Port facilities and vessels.	Threat modelling MITRE ATT&CK /ENISA/IMO Framework
Security controls in Port Community Systems and Ships systems.	Goals of security control, security control types, security control functions, Access control properties, patch management, CIS Critical Security Controls

3.6.1.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.6.1.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.6.2 CSP007_S_M: AI and Cybersecurity Research in Maritime

3.6.2.1 Description of Training Module

Table 23: Description of Training Module

Code	**CSP006_S_ M**
Module Title	Cyber Threat Intelligence for Maritime
Alternative Title(s)	Cyber Threat intelligence Information Sharing in Maritime
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Seminar (S)
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	The modules aims to provide learners with an overview of the threat intelligence and sharing in maritime sector
Module description *Indicates the main purpose and description of the module.*	The aim of the module is to provide the learner with the ability to understand cyber threat intelligence properties and sharing common knowledge among entities in maritime sector.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: **Knowledge and understanding:** Demonstrate an in-depth understanding of cyber threat intelligence and adoption in maritime sector. Identify and critically analyse the threat in maritime sector **Skill and Competence:** Critically evaluate vulnerabilities and threats for the systems within the maritime supply chain. Demonstrate an in-depth understanding of threat intelligence information sharing standards

Main topics and content list *A list of main topics and key content*	
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Summative assessment: This assessment component assess the learners' knowledge based on the topics covered by the module through presentation and viva.
Training Provider *Name(s) of training providers.*	SLC
Contact *Name(s) of the main contact person and their email address.*	Prof. Shareeful Islam, Shareeful@gmail,com Athina Labropoulou , athina.labropoulou@securitylabs.ie
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted in DCM
Duration *Duration of the training.*	To be posted in DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Virtual and Physical

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies*
Pre-requisites	Basic IT and security Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Chief Information Security Officer (CISO) Cyber Legal, Policy & Compliance Officer Cybersecurity Auditor Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this training module.*	Virustotal Phishtank Threatminer Mozilla observatory Threatfeeds Malware bazaar CVSS v4.0 calculator
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English

ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.6.2.2 Adapted Syllabus

Table 24: Adapted Syllabus

Main topics	Suggested Content
Topic 1: Cyber threat and threat intelligence	An overview of threat and threat intelligence in maritime sector Threat taxonomy and threat intelligence properties
Topic 2: Threat and Vulnerability assessment	Vulnerabilities assessment using CVSS4.0 Threat modelling and management
Topic 3: Threat intelligence information sharing	Threat feed Threat intelligence information sharing standard, TAXII,MISP and STIX Threat intelligence information sharing guideline- NIST SP 800-150

3.6.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.6.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.7 Module 7 - Cybersecurity in Emerging Technologies for Maritime

3.7.1 CSP007_S_M: AI and Cybersecurity Research in Maritime

3.7.1.1 Description of Training Module

The main objective of this training module is to understand the role and significance of AI in cybersecurity. The dimensions that will be addressed include the following three:

AI to support cybersecurity: This category focuses on the use of AI as a means to create advanced cybersecurity by developing more effective security controls. Examples may include the application of AI-driven approaches to enhance network security, endpoint security, and overall cybersecurity posture. It aims to provide insights into how AI technologies can be integrated with cybersecurity frameworks, such as intrusion detection systems (IDS), user and entity behavior analytics (UEBA), and threat intelligence.

Malicious use of AI: This category focuses on the adversarial or malicious use of AI to create more sophisticated types of attacks, as well as attacks against AI systems. It aims to provide a comprehensive understanding of how AI technologies can expand the existing cyber threat landscape.

Cybersecurity for AI: This category focuses on the use of cybersecurity to protect AI systems from attacks. The goal is on securing AI, ensuring the security and trustworthiness of AI technologies and preventing their malicious use. Examples may include understanding ethical considerations and ensuring responsible development and deployment of AI in cybersecurity operations. Additionally, it involves exploring examples of protection mechanisms to safeguard AI-driven systems from adversarial threats.

The module will focus within the maritime sector, emphasizing the importance of robust AI specific to maritime cybersecurity. Participants will explore various topics related to AI technologies in cybersecurity defense, including intrusion detection systems (IDS), user and entity behavior analytics (UEBA), threat intelligence, network security, and endpoint security, tailored to maritime operations. Through practical examples and case studies, participants will learn how AI can be leveraged in adversary emulation with focus on maritime environments to enhance the resilience of cybersecurity defenses. Additionally, the module will address the integration of AI-driven approaches into existing cybersecurity frameworks, ensuring participants gain practical insights into implementing AI technologies effectively to safeguard maritime systems and the relevant assets.

Table 25: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP007_S_M**
Module Title *The title of the training module*	AI and Cybersecurity Research in Maritime
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Maritime Cyber Defense: Leveraging AI for Threat Mitigation Maritime Cybersecurity: Advanced AI Applications AI and Maritime Cybersecurity
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	Looking at both sides of the use of AI in the context of cybersecurity, this module aims to provide a comprehensive understanding of how AI technologies can be integrated into cybersecurity frameworks to strengthen threat detection, prevention, and response. Through exploration of various AI-driven approaches such as intrusion detection systems (IDS), user and entity behavior analytics (UEBA), threat intelligence, and endpoint security, participants will gain practical insights into enhancing cybersecurity defenses. Additionally, the module will cover topics related to how AI technologies can expand the cyber threat landscape, equipping participants with strategies to safeguard against adversarial threats and ensure the trustworthiness of AI models within broader systems.

Module description *Indicates the main purpose and description of the module.*	Equip with the knowledge and skills necessary to leverage AI technologies effectively in cybersecurity defense, including the understanding and mitigation of adversarial AI threats. Explore various AI-driven approaches, such as intrusion detection systems (IDS), user and entity behavior analytics (UEBA), threat intelligence, and endpoint security, with a focus on enhancing threat detection, prevention, and response capabilities. Participants will gain practical insights into the integration of AI with existing cybersecurity frameworks and learn how to implement adversary emulation techniques to test and improve the resilience of cybersecurity defenses.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Knowledge: Understand the potential of cybersecurity related to AI in maritime. Apply AI and machine learning techniques to enhance maritime cybersecurity practices, focusing on threat detection and analysis. Understand research methodologies and conduct research, innovation, and development work in maritime-related cybersecurity topics. Generate and manifest research and innovation ideas specific to maritime cybersecurity. Advance the current state-of-the-art in maritime-related cybersecurity topics through knowledge acquisition and critical analysis. Identify and assist in the development of innovative cybersecurity-related solutions in relation to the maritime. Skills: Conduct experiments for cybersecurity solutions applicable to maritime. Select and apply frameworks, methods, standards, or tools to support cybersecurity projects in the maritime. Contribute to the creation of cutting-edge cybersecurity ideas and solutions specifically designed for maritime organisations. Assist in cybersecurity-related capacity building within maritime settings, including security awareness, theoretical and practical training, and knowledge sharing. Identify cross-sectoral cybersecurity achievements and apply them to the maritime sector, or propose innovative approaches and solutions adapted to maritime.

Main topics and content list *A list of main topics and key content*	Introduction to AI and Cybersecurity with Applications to Maritime AI-driven Cybersecurity Approaches in Maritime Cyber Defense Malicious Use of AI and Securing AI Maritime Datasets for AI-driven Cybersecurity: Analysis and Applications Data Extraction Techniques in Maritime Systems
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Projects and/or hands-on exercises
Training Provider *Name(s) of training providers.*	SINTEF, PDMFC, UNSPMF
Contact *Name(s) of the main contact person and their email address.*	Prof. Danijela Boberic Krsticev: dboberic@uns.ac.rs Dr. Nektaria Kaloudi: nektaria.kaloudi@sintef.no Dr. Stylianos Karagiannis: stylianos.karagiannis@pdmfc.com
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	To be posted on the DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* KA1 – Cybersecurity Management KA2 – Human Aspects of Cybersecurity KA3 – Cybersecurity Risk Management KA4 – Cybersecurity Policy, Process, and Compliance KA5 – Network and Communication Security KA6 – Privacy and Data Protection KA7 – Cybersecurity Threat Management KA8 – Cybersecurity Tools and Technologies KA9 – Penetration Testing KA10 – Cyber Incident Response	**Mainly KA8** Minor content matches with others including KA3, KA5, KA7, KA10
Pre-requisites	Good programming skills, particularly in languages commonly used in machine learning, such as Python.
Relevance to European Cybersecurity Skills Framework (ECSF) An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.	ECSF Profile 9: Cybersecurity Researcher
Tools to be used *A list of tools that will be used for the operation of this training module.*	Metadon, Notebook Jupyter (or Google Colab), Wireshark, scikit-learn, pyOD
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	English, Portuguese, Serbian

ECTS If applicable, the number of ECTS.	To be posted on the DCM (Recommended equivalent to 5 ECTS)
Certificate of Attendance (CoA) Indicates Yes or No (even in case of partial attendance)	To be posted on the DCM
Module enrolment dates Indicates the enrolment dates for the operation of this training module.	Refer and check online CyberSecPro DCM System for current information.
Other important dates 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.	Refer and check online CyberSecPro DCM System for current information.

3.7.1.2 Adapted Syllabus

Table 26: Adapted Syllabus

Main topics	Suggested Content
Topic-1: Introduction to AI and Cybersecurity with Applications to Maritime	The role and significance of AI in cybersecurity for strengthening threat detection, prevention, and response in maritime cybersecurity, as well as the introduction to malicious use of AI and their implications for maritime cybersecurity Overview of cybersecurity threats specific to the maritime
Topic-2: AI-driven Cybersecurity Approaches for Maritime Cyber Defense	Integrating AI-driven approaches into existing cybersecurity frameworks Strategies for implementing AI technologies effectively to safeguard maritime systems and assets Practical insights and hands-on simulations to apply AI algorithms for advanced threat detection, prevention and response in maritime settings

	Application of AI technologies such as IDS, UEBA, threat intelligence, and endpoint security in maritime cybersecurity
Topic-3: Malicious use of AI and Securing AI	Definition and characteristics of adversarial AI and AI-powered cyberattacks Understanding the motives, goals, and techniques behind adversarial AI and AI-powered cyberattacks Analyzing real-world examples to illustrate the differences between the two concepts Importance of understanding adversarial AI models for enhancing cybersecurity defenses in maritime operations Strategies for detecting, mitigating, and defending against adversarial AI and AI-powered cyberattacks in maritime cybersecurity.
Topic-4: Maritime Datasets for AI-driven Cybersecurity: Analysis and Applications	Overview of datasets relevant to maritime cybersecurity and AI applications types of data sources commonly used in maritime cybersecurity, such as AIS (Automatic Identification System) data, radar data, satellite imagery, and maritime communication data Understanding the challenges and considerations in collecting, processing, and utilizing maritime datasets for AI-driven cybersecurity applications Practical applications of maritime datasets in enhancing threat detection, prevention, and response using AI technologies Case studies and examples demonstrating the use of maritime datasets for training AI models and improving cybersecurity defenses in maritime environments.
Topic-5: Data Extraction Techniques in Maritime Systems	Overview of data extraction techniques used in maritime systems Types of data sources commonly utilized in maritime systems, such as AIS (Automatic Identification System), radar data, satellite imagery, and maritime communication data techniques for extracting and processing data from various sources in maritime environments Challenges and considerations in data extraction from maritime systems, including data quality, reliability, and compatibility Practical applications of data extraction techniques in maritime cybersecurity and AI-driven approaches

	Case studies and examples demonstrating the use of data extraction techniques to enhance threat detection, prevention, and response in maritime cybersecurity.

3.7.1.3 Planning for Preparedness

The "AI and Cybersecurity Research in Maritime" training module incorporates a diverse range of materials and exercises to provide participants with a comprehensive learning experience.

Presentation material that will be used during the session and relevant research findings will be utilized to convey theoretical concepts.

Practical and hands-on exercises include the identification and analysis of AI cybersecurity challenges and solutions faced by the maritime domain.

3.7.1.4 Materials and Exercises

At the conclusion of the training module, participants will be encouraged to complete an evaluation form assessing the topics covered and the knowledge gained. This feedback will be considered to improve future sessions and better meet the participants' needs.

3.8 Module 8 - Critical Infrastructure Security for Maritime

3.8.1 CSP008_C_M: Critical Infrastructure Security for Maritime

3.8.1.1 Description of Training Module

The training module dedicated to the Critical infrastructure security for Maritime focuses on the digital risks and ad-hoc protection measures for entities recognized as Maritime Critical Infrastructure (e.g. harbors, offshore oil & gas / energy activities and underwater networks).

The module describes the risks and stakes under the perspective of legal, technical, economic aspects in order to present the concerned entities and link them to the existing legal frameworks as critical infrastructure, but also as potential OES with regards to the NIS directive.

3.8.1.2 Adapted Syllabus

Table 27: Adapted Syllabus

Main topics	Suggested Content
Introduction to Maritime Cybersecurity	Description of maritime systems (ships and harbours) Focus on Port community systems and Cargo Community Systems Overview of maritime critical infrastructure and Operators of essential services Cybersecurity risks and mitigations
Threats and Vulnerabilities in Maritime Operations	Analysis of recent cyber incidents in maritime sectors Vulnerability assessment of systems and networks operated by harbours
Risk Management and Cybersecurity Frameworks	NIST directive Risk Management methodology (EBIOS RM) Cybersecurity framework implementation (NIST, ISO/IEC 27001)
Maritime Regulations and Compliance	International Maritime Organization (IMO) guidelines and recommendations BIMCO guides and studies Quotation agencies developments (BV, DNVGL) International regulatory frameworks
Maritime Studies	EU cybersecurity study for Harbours (2019) Analysis of MAERSK cybersecurity Attack 2017

3.8.1.3 Planning for Preparedness

The module encompasses several training material as presentations on several thematics, such as Portuary systems (Port community systems, Cargo community Systems), maritime systems (IoT networks and dependencies), submarine technologies cables.

Presentation material that will be used during the module are prepared and adapted to the audience by the different trainers in the month before the delivery of the different modules

3.8.1.4 Materials and Exercises

PowerPoint presentations and text documents.

3.8.2 CSP008_S_M: Critical Infrastructure Security in Maritime

3.8.2.1 Description of Training Module

This module is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing.

Table 28: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP008_S_M**
Module Title *The title of the training module*	Critical Infrastructure Security for Maritime
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	C
Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This module focuses on Critical Infrastructure Security within the Maritime Cybersecurity domain The primary aim is to equip participants with the knowledge and skills necessary to understand, evaluate, and enhance cybersecurity measures in maritime environments, where critical infrastructure such as ports, shipping operations, and associated logistics play a pivotal role in global trade and security. The workshop is structured to address the unique challenges and threats faced by maritime sectors, emphasizing practical solutions and strategic approaches to safeguarding these vital assets against cyber threats.

Module description *Indicates the main purpose and description of the module.*	The maritime industry, integral to global commerce and communication, faces increasing cyber threats that could compromise critical infrastructure, leading to significant economic and security repercussions. This module delves into the intricacies of maritime cybersecurity, covering the technological, regulatory, and operational aspects essential for protecting infrastructure. Through a blend of theoretical knowledge and practical exercises, participants will gain a thorough understanding of cybersecurity principles, the nature of cyber threats specific to the maritime sector, and the latest strategies for risk management and incident response. The workshop encourages active engagement through case studies, group discussions, and hands-on activities, aiming to foster a proactive cybersecurity culture among maritime professionals.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	· Understand the Cybersecurity Landscape: Grasp the scope of cybersecurity within the maritime sector, including key concepts, terminology, and the significance of protecting maritime critical infrastructure. · Identify Maritime Cyber Threats and Vulnerabilities: Recognize the specific cyber threats and vulnerabilities facing maritime operations, including the risks to shipping companies, ports, and supply chains. · Implement Risk Management Strategies: Apply effective risk management strategies tailored to maritime operations, incorporating cybersecurity best practices, policies, and procedures. · Develop Incident Response Plans: Formulate and execute incident response plans for maritime cybersecurity incidents, ensuring rapid recovery and minimal operational disruption. · Comply with Regulations and Standards: Navigate the complex landscape of international and national regulations, standards, and guidelines related to maritime cybersecurity. · Foster a Culture of Cybersecurity Awareness: Promote cybersecurity awareness within maritime organizations, emphasizing the importance of individual and collective actions in maintaining security.

Main topics and content list *A list of main topics and key content*	· Introduction to Maritime Cybersecurity · Threats and Vulnerabilities in Maritime Operations · Risk Management and Cybersecurity Frameworks · Maritime Cybersecurity Regulations and Compliance · Incident Response and Recovery in Maritime Environments · Business continuity and disaster recovery strategies
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Formative assessment*: Case Study Analysis: Participants will analyse a real-world maritime cyber incident, identifying the causes, impacts, and the effectiveness of the response. This exercise will assess their ability to apply theoretical knowledge to practical scenarios. *Summative assessment*: an integrated assessment combining an Incident Response Simulation with a Written Examination, enabling participants to apply practical skills in a simulated cyber incident before demonstrating their theoretical knowledge. This approach ensures a comprehensive evaluation of participants' abilities to manage real-world cybersecurity challenges and their understanding of underlying principles and regulations in the maritime sector.
Training Provider *Name(s) of training providers.*	TalTech
Contact *Name(s) of the main contact person and their email address.*	Ricardo Lugo Ricardo.Lugo@taltech.ee
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	6 hours

Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	KA1 – Cybersecurity Management KA2 – Human Aspects of Cybersecurity KA3 – Cybersecurity Risk Management KA4 – Cybersecurity Policy, Process, and Compliance KA7 – Cybersecurity Threat Management KA10 – Cyber Incident Response
Pre-requisites	Foundational Knowledge in Cybersecurity IT and Network Systems Familiarity Understanding of Maritime Operations Basic technical skills, including familiarity with operating systems (such as Windows, Linux, etc.), command-line interfaces, and the use of cybersecurity tools. Participants without these prerequisites might find it challenging to fully grasp the advanced concepts discussed in the course.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	Cyber Incident Responder, Cybersecurity Risk Manager Cyber Legal, Policy & Compliance Officer

Tools to be used *A list of tools that will be used for the operation of this training module.*	nMap,OpenVAS
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	3
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM
Other important dates *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.*	See DCM

3.8.2.2 Adapted Syllabus

Table 29: Adapted Syllabus

Main topics	Suggested Content
Introduction to Maritime Cybersecurity	Overview of maritime critical infrastructure Cybersecurity fundamentals in the maritime context

Threats and Vulnerabilities in Maritime Operations	Analysis of recent cyber incidents in maritime sectors Vulnerability assessment of maritime systems and networks
Risk Management and Cybersecurity Frameworks	Risk assessment methodologies Implementation of cybersecurity frameworks (e.g., NIST, ISO/IEC 27001)
Maritime Cybersecurity Regulations and Compliance	International Maritime Organization (IMO) guidelines National and international regulatory frameworks
Incident Response and Recovery in Maritime Environments	Designing and testing incident response plans
Business continuity and disaster recovery strategies	Building a Cyber-Resilient Maritime Culture Cybersecurity training and awareness programs Best practices for cybersecurity hygiene in maritime operations

3.8.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.8.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.9 Module 9 - Software Security for Maritime

3.9.1 CSP009_W_M: Software Security for Maritime

3.9.1.1 Description of Training Module

Table 30: Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP009_W_M**
Module Title *The title of the training module*	Securing Maritime Web Applications
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Maritime Web Application Software Security – OWASP Top 10
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	W/S
Level Training level: B (Basic), A (Advanced)	B
Module overview High-level module overview	Throughout this workshop, students are introduced to the architecture of web applications, as well as to their common bugs. After a short presentation in theory students, each presented bug category is illustrated through a practical example, students are also provided the required resources to execute the same in their own laptop. These examples apply directly to websites used by maritime companies to track shipments, routes and other logistic information.

Module description Indicates the main purpose and description of the module.	The purpose of this workshop is to provide an interactive, safe environment where the students can view different implementations of code with different levels of security and actively try known attacks against them to undertake an attacker's perspective. Then they can examine the code within their maritime web applications and mitigate such issues.
Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Understanding Web Application Vulnerabilities Taking advantage of web application vulnerabilities Securing web applications against known attacks.
Main topics and content list A list of main topics and key content	Topics Covered within this workshop include: · Injection · Broken Authentication, authorization and session management · Cross-Site Scripting · Insecure Direct Object Reference · Security Misconfiguration · Sensitive Data Exposure · Missing Function-Level Access Controls · Cross-Site Request Forgery · Using Components with Known Vulnerabilities · Unvalidated Redirects and forwards.
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	The virtual machine (VM) designed for this workshop is intentionally embedded with various bugs across multiple categories to simulate real-world scenarios. At the culmination of the workshop, students are divided into teams. Each team is tasked with selecting and resolving one bug from each category. This hands-on approach not only tests their technical skills but also encourages collaboration and problem-solving strategies. Following the bug-fixing exercise, teams are required to present their solutions in a concise format.
Training Provider *Name(s) of training providers.*	Focal Point

Contact *Name(s) of the main contact person and their email address.*	Christos Grigoriadis cgrigor@focalpoint-sprl.be
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	Upon Request from organization
Duration *Duration of the training.*	1 full day
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	*Both, Physical upon request and coordination and Virtual either through Microsoft Teams or Discord.*
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* KA1 – Cybersecurity Management KA2 – Human Aspects of Cybersecurity KA3 – Cybersecurity Risk Management KA4 – Cybersecurity Policy, Process, and Compliance KA5 – Network and Communication Security KA6 – Privacy and Data Protection KA7 – Cybersecurity Threat Management KA8 – Cybersecurity Tools and Technologies KA9 – Penetration Testing KA10 – Cyber Incident Response	*KA1 – Cybersecurity Management* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing*
Pre-requisites	Basic PHP knowledge Basin Knowledge on Kali Linux Toolkit

Relevance to European Cybersecurity Skills Framework (ECSF) An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.	Cybersecurity Researcher Security Software Developer
Tools to be used *A list of tools that will be used for the operation of this training module.*	Tools used within this workshop include: Burp Suite · DirBuster · Nikto · sqlmap · w3af · WebSploit · ZAP
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	English
ECTS If applicable, the number of ECTS.	No
Certificate of Attendance (CoA) Indicates Yes or No (even in case of partial attendance)	No
Module enrolment dates Indicates the enrolment dates for the operation of this training module.	-
Other important dates 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.	-

3.9.1.2 Adapted Syllabus

Table 31: Adapted Syllabus

Main topics	Suggested Content
Injection:	Delving into various forms of injection attacks, emphasizing their impact on web applications and demonstrating prevention techniques.
Broken Authentication:	Exploring the mechanisms by which authentication and session management can be compromised, leading to unauthorized access.
Sensitive Data Exposure:	Understanding the ways sensitive data can be inadequately protected, leading to breaches of confidentiality and integrity.
XML External Entities (XXE):	Investigating how outdated or poorly configured XML processors can be exploited to carry out attacks against web applications.
Broken Access Control:	Examining the failures in access control mechanisms that allow attackers to bypass authorization and access sensitive data or functionality.
Security Misconfigurations:	Identifying common security misconfigurations and strategies for securing web applications effectively.
Cross-Site Scripting (XSS):	Learning about XSS vulnerabilities that allow attackers to execute scripts in the browsers of unsuspecting users.
Insecure Deserialization:	Exploring the risks associated with deserializing data from untrusted sources and the potential for remote code execution.
Using Components with Known Vulnerabilities:	Discussing the dangers of using third-party components with known vulnerabilities and methods for managing such risks.
Insufficient Logging & Monitoring:	Highlighting the importance of logging and monitoring to detect and respond to security incidents promptly.

3.9.1.3 Planning for Preparedness

For optimal preparedness, participants are required to have foundational knowledge in HTML, Bash scripting, and basic PHP programming. Familiarity with the Kali Linux toolkit, including tools like DirBuster, Nikto, sqlmap, w3af, WebSploit, and ZAP, is essential. Participants must install their own Kali Linux VM and another VM shared in advance of the course. This setup ensures that all students come equipped with the necessary skills and tools to fully engage with the workshop's practical components.

3.9.1.4 Materials and Exercises

The workshop will provide a comprehensive set of materials and exercises to facilitate learning. Slides with embedded code snippets illustrating various vulnerabilities will be shared, alongside links to the required VMs. This approach allows for a hands-on learning experience, where participants can apply what they've learned in real-time. Shared materials through chat and slides ensure that participants have access to all necessary resources for a deep understanding of web application security.

3.9.2 CSP009_SA_M: Software Security for Maritime

3.9.2.1 Description of Training Module

Table 32: Description of Training Module

Code *Code format: CSP009_x where x is the training of offering type (see below)*	**CSP009_SA_M**
Module Title *The title of the training module*	**Maritime Software Security Seminar**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	-
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S

Level *Training level: B (Basic), A (Advanced)*	A (Advanced)
Module overview *High-level module overview*	This CSP module delves into the intricacies of software security in the maritime sector, building upon foundational cybersecurity knowledge. It provides students with specialized skills and strategies for securing software built for the maritime industry throughout its entire lifecycle, from design and development to deployment and maintenance.
Module description *Indicates the main purpose and description of the module.*	This CSP training module dives deep into the essential principles and practices of maritime software security. Participants will gain hands-on experience identifying, understanding, and mitigating software vulnerabilities of the maritime applications throughout the development lifecycle. The participants will gain in-depth knowledge of secure coding, secure software development methodologies, threat modelling, risk assessment, and security architecture, equipping them to build and maintain secure software throughout its lifecycle. Through rich materials, and exercises, the module equips individuals with the necessary skills to build secure and resilient software applications.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	This seminar syllabus aims to provide participants with a comprehensive understanding of software security principles, practices, and methodologies tailored specifically for the maritime industry. By the end of the seminar, participants will possess the the following knowledge, skills, and competencies: Knowledge: Understanding of software security concepts and their relevance to the maritime industry. Familiarity with common software vulnerabilities and threats specific to maritime systems. Knowledge of secure software development frameworks, standards, and guidelines applicable to maritime software development. Understanding of threat modelling techniques and their application in identifying and mitigating software security risks in maritime environments. Awareness of software security testing methodologies, including static and dynamic analysis, and their application to maritime software systems. Overview of emerging technologies such as IoT, AI, and blockchain and their impact on maritime software security. Skills and competences:

	Ability to analyze and assess software security risks in maritime systems and applications. Capacity in implementing secure coding practices, including input validation and error handling. Competence in conducting threat modelling exercises to identify potential security vulnerabilities. Skill in performing software security testing using various methodologies to ensure the integrity of maritime software. Capability to participate in group discussions and collaborative problem-solving to address software security challenges in maritime scenarios. Proficiency in communicating software security concepts and solutions effectively to stakeholders in the maritime industry. Competence in identifying opportunities for continuous improvement in software security practices within maritime organizations.
Main topics and content list *A list of main topics and key content*	Overview of software security concepts and their importance in the maritime sector. Ensuring the safety and integrity of maritime operations - real-world scenarios and incidents. Secure software development frameworks, standards, guidelines, and practices relevant to maritime software development. SDLC models, challenges and best practices. Threat modelling for identifying and mitigating maritime software security risks. Secure Deployment and Configuration Management Software security testing and applications to maritime software systems. Hands-on exercises and simulations to reinforce software security concepts and techniques. Exploration of future trends and emerging technologies shaping the future of software security in the maritime sector.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessments:** These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered during the seminar delivery by the instructor.

Training Provider *Name(s) of training providers.*	TUC, MAG
Contact *Name(s) of the main contact person and their email address.*	Pinelopi Kyranoudi pkyranoudi@tuc.gr Spiros Borotis spiros.borotis@maggioli.gr
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	To be posted on the DCM
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Diverse topics from many KAs, especially: KA1 – Cybersecurity Management KA8 – Cybersecurity Tools and Technologies KA9 – Penetration Testing
Pre-requisites	Basic IT training, programming, software development, cybersecurity basics
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	CYBERSECURITY AUDITOR CYBERSECURITY RESEARCHER PENETRATION TESTER
Tools to be used *A list of tools that will be used for the operation of this training module.*	
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek

ECTS *If applicable, the number of ECTS.*	N/A
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	To be posted in DCM
Other important dates *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.*	To be posted in DCM

3.9.2.2 Adapted Syllabus

Table 33: Adapted Syllabus

Main topics	Suggested Content
1. Introduction to Software Security in the Maritime Industry	Overview of software security concepts and their importance in the maritime sector. Introduction to common software vulnerabilities and threats specific to maritime systems and applications. Understanding the role of software security in ensuring the safety and integrity of maritime operations - real-world scenarios and incidents.
2. Principles of secure software development lifecycle (SDLC) tailored for the maritime industry.	Introduction to secure software development frameworks, standards, guidelines, and practices relevant to maritime software development. SDLC models, challenges and best practices.

	Best practices for secure coding, including input validation, secure authentication, and error handling.
3. Understanding the process of threat modelling for identifying and mitigating maritime software security risks.	Application of threat modelling techniques to maritime software systems and applications. Case studies and examples of threat modelling in the maritime sector. Secure Deployment and Configuration Management.
4. Overview of software security testing methodologies, including static and dynamic analysis.	Types of tests (e.g., penetration testing, DAST, MAST) Application of security testing techniques to maritime software systems. Hands-on exercises and simulations to reinforce software security concepts and techniques.
5. Exploration of future trends and emerging technologies shaping the future of software security in the maritime sector.	Group discussions to explore software security challenges and solutions in maritime scenarios. Discussion on the impact of IoT, AI, and blockchain on maritime software security. Consideration of future challenges and opportunities for enhancing software security in maritime operations.

3.9.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.9.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.10 Module 10 - Penetration Testing for Maritime

3.10.1 CSP0010_W_M: Penetration Testing for Maritime

3.10.1.1 Description of Training Module

Table 34: Description of Training Module

Code	**CSP010_W_M**
Module Title *The title of the training module*	Penetration Testing for Maritime IT Infrastructures
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Penetration Testing for Maritime IT Infrastructure - Active Directory Attacks
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Workshop
Level Training level: B (Basic), A (Advanced)	A
Module overview High-level module overview	This module 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 against background maritime IT infrastructure used for operations, such as an active directory environment.

Module description Indicates the main purpose and description of the module.	Under the guidance of instructors, students learn the intricacies of red teaming, starting with the fundamentals and gradually progressing to more advanced techniques. The curriculum covers a wide range of offensive security topics, including reconnaissance, network exploitation, privilege escalation, and lateral movement. All these stages are highly applicable to background Maritime IT infrastructure used for operations.
Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Learning Outcomes Include: Understanding Active Directory Vulnerabilities Understanding Weak points of a Network Understanding and implementing Red Teaming Methodologies
Main topics and content list A list of main topics and key content	Topics Covered within this workshop include: · Password reuse between computers (PTH) · Spray User = Password · Password in description · SMB share anonymous · SMB not signed · Responder · Zerologon · ASREPRoast · Kerberoasting
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	-
Training Provider *Name(s) of training providers.*	Focal Point

Contact *Name(s) of the main contact person and their email address.*	Christos Lazaridis-Christos Grigoriadis clazar@focalpoint-sprl.be cgrigor@focalpoint-sprl.be
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	Upon Request from organization
Duration *Duration of the training.*	2 full days
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	*Both, Physical upon request and coordination and Virtual either through Microsoft Teams or Discord.*
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* KA1 – Cybersecurity Management KA2 – Human Aspects of Cybersecurity KA3 – Cybersecurity Risk Management KA4 – Cybersecurity Policy, Process, and Compliance KA5 – Network and Communication Security KA6 – Privacy and Data Protection KA7 – Cybersecurity Threat Management KA8 – Cybersecurity Tools and Technologies KA9 – Penetration Testing KA10 – Cyber Incident Response	*KA1 – Cybersecurity Management* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing*

Pre-requisites	Understanding of Active Directory Initial Understanding of Active Directory Attacks Networking Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.	Penetration Tester
Tools to be used *A list of tools that will be used for the operation of this training module.*	Tools used within this workshop include: · Nmap · Powershell · Exploits · Mimikatz · Hashcat
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	English
ECTS If applicable, the number of ECTS.	No
Certificate of Attendance (CoA) Indicates Yes or No (even in case of partial attendance)	No
Module enrolment dates Indicates the enrolment dates for the operation of this training module.	-

Other important dates 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.	-

3.10.1.2 Adapted Syllabus

Table 35: Adapted Syllabus

Main topics	Suggested Content
Password Reuse Between Computers (Pass-the-Hash/PtH):	Examination of how attackers exploit password reuse across different systems to gain unauthorized access without needing the plaintext password.
Spray User = Password:	Discussion on the technique of password spraying, specifically targeting user accounts where the username and password are the same, a common weak security practice.
Password in Description:	Identifying and exploiting instances where passwords are insecurely stored in user or computer account descriptions within AD.
SMB Share Anonymous:	Exploring the vulnerabilities associated with anonymously accessible SMB shares and how they can be exploited to access sensitive information.
SMB Not Signed:	Understanding the risks and exploitation techniques for SMB sessions that are not signed, allowing for potential man-in-the-middle attacks.
Responder:	Utilizing the Responder tool to perform LLMNR, NBT-NS, and MDNS poisoning, capturing hashes and credentials on a network.
Kerberoasting:	Techniques for extracting service account credentials from AD by requesting TGS tickets and cracking them offline to reveal plaintext passwords.

Zerologon:	Detailed analysis of the Zerologon vulnerability (CVE-2020-1472), demonstrating how an attacker can exploit the Netlogon protocol to compromise an AD domain controller.
ASREPRoast:	Discussing attack scenarios where attackers can request AS-REP tickets for users without pre-authentication, leading to offline cracking of user passwords.

3.10.1.3 Planning for Preparedness

To ensure that participants can fully engage with the workshop material and exercises, they are expected to have:

· A foundational understanding of Active Directory and its common attack vectors.

· Initial knowledge of Active Directory attacks to grasp the advanced concepts more effectively.

· A solid grounding in networking principles to understand how AD attacks can be propagated across networked environments.

Participants will be provided with remote connections to lab environments, eliminating the need for local installations. This setup allows for a hands-on learning experience in a controlled and realistic setting.

3.10.1.4 Materials and Exercises

The workshop will employ a variety of materials to facilitate learning:

· Slides: Comprehensive slides will be shared, covering theoretical concepts, attack methodologies, and case studies to illustrate real-world applications of the techniques discussed.

· Remote Labs: Participants will have access to remote lab environments that simulate real-world AD infrastructures, allowing for practical application of penetration testing techniques in a safe and controlled manner.

3.10.2 CSP0010_S_M: Penetration Testing for Maritime

3.10.2.1 Description of Training Module

The Penetration Testing for Maritime aims at providing training on AIS transponders. During the activity a group of trainees will have the opportunity to practise simulated attacks.

Most often observed attacks of AIS (including attacks via GNSS) are detailed and presented during the course and a specific analysis is conducted on events such as the attack of the Italian Coast Guards and the most recents spoofing of vessels in the Russo-Ukrainian war.

3.10.2.2 Adapted Syllabus

Table 36: Adapted Syllabus

Main topics	Suggested Content
Introduction to Maritime Cybersecurity	Description of AIS as a target System for jamming or spoofing Cybersecurity risks and mitigations for systems relying on GNSS
Threats and Vulnerabilities in Maritime Operations	Analysis of recent cyber incidents in maritime sectors Vulnerability assessment of AIS and GNSS Identification of threats, vulnerability and risks associated with applications and services relying on AIS Common attack tactics, techniques used when hacking web servers, applications and wireless networks Security controls for information systems against common threats Theoretical hacking exercises in a realistic training environment.
Risk Management and Cybersecurity Frameworks	IMO AIS regulation ITU radio communications regulation
Studies	Studies on AIS spoofing and jamming Analogy with other PNT systems ADSB system in Air transport

3.10.2.3 Planning for Preparedness

The planning of a training needs the deployment of a simulating environment as well as the connection to an AIS transponder and/or a connected system.

3.10.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.11 Module 11 - Cyber Ranges and Operations for Maritime

3.11.1 CSP0011_W_M: Cyber Ranges and Operations for Maritime

3.11.1.1 Description of Training Module

Code	**CSP011_W_M**
Module Title *The title of the training module*	Detection Engineering on a Cyber Range of a Maritime IT infrastructure-Active Directory
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Blue Teaming Detection Engineering MITRE ATT&CK Chains MITRE ATT&CK Mitigations & Detections
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Workshop
Level Training level: B (Basic), A (Advanced)	A
Module overview High-level module overview	This module offers a comprehensive course focused on blue teaming, where students are not only taught but also actively engage in performing a variety of detection engineering methodologies. The purpose of this course is to provide hands-on experience and in-depth knowledge of blue teaming methodologies and techniques, empowering students to detect real-world cyber-attacks against background maritime infrastructures used for operations, such as an active directory environment.

Module description Indicates the main purpose and description of the module.	Under the guidance of instructors, students learn the intricacies of blue teaming, starting with the fundamentals and gradually progressing to more advanced techniques. The curriculum covers a wide range of defensive security topics, including detections for reconnaissance, network exploitation, privilege escalation, and lateral movement techniques.
Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Learning Outcomes Include: Understanding Active Directory Vulnerabilities Understanding Weak points of a Network Understanding and implementing Red Teaming Methodologies Understanding of Detection Engineering Techniques
Main topics and content list A list of main topics and key content	Topics Covered within this workshop include: • Detections of Spray User = Password • Detection of SMB share anonymous • Detection of SMB not signed • Responder • Detection on Zerologon • Detection ofASREPRoast • Detection of Kerberoasting
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	Participants are split into teams at the end of the event, they are given a specific timeframe to investigate through sentinel, then verbally discuss their solutions.
Training Provider *Name(s) of training providers.*	Focal Point
Contact *Name(s) of the main contact person and their email address.*	Christos Lazaridis-Christos Grigoriadis clazar@focalpoint-sprl.be cgrigor@focalpoint-sprl.be

Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	Upon Request from organization
Duration *Duration of the training.*	2 full days
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	*Both, Physical upon request and coordination and Virtual either through Microsoft Teams or Discord.*
Pre-requisites	Understanding of Active Directory Initial Understanding of Active Directory Attacks Networking Knowledge
Relevance to European Cybersecurity Skills Framework (ECSF) An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.	Cyber Security Engineer
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* KA1 – Cybersecurity Management KA2 – Human Aspects of Cybersecurity KA3 – Cybersecurity Risk Management KA4 – Cybersecurity Policy, Process, and Compliance KA5 – Network and Communication Security KA6 – Privacy and Data Protection	*KA1 – Cybersecurity Management* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing*

KA7 – Cybersecurity Threat Management KA8 – Cybersecurity Tools and Technologies KA9 – Penetration Testing KA10 – Cyber Incident Response	
Tools to be used *A list of tools that will be used for the operation of this training module.*	Tools used within this workshop include: • Bloodhound • Sentinel • Wazuh
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	English
ECTS If applicable, the number of ECTS.	No
Certificate of Attendance (CoA) Indicates Yes or No (even in case of partial attendance)	No
Module enrolment dates Indicates the enrolment dates for the operation of this training module.	-
Other important dates 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.	-

3.11.1.2 Adapted Syllabus

Main topics	Suggested Content
Detection of Spray User = Password:	Techniques and strategies for identifying and alerting on password spraying attempts, utilizing behavior analysis and anomaly detection.
Detection of SMB Share Anonymous:	Configuring detection rules to identify unauthorized anonymous access to SMB shares, highlighting potential misuse or exploitation.
Detection of SMB Not Signed:	Methods for detecting SMB sessions that are not signed, potentially indicating man-in-the-middle (MitM) attacks or other malicious activities.
Responder Detection:	Implementing network monitoring and anomaly detection strategies to identify the use of tools like Responder for LLMNR, NBT-NS, and MDNS poisoning attacks.
Detection of Zerologon (CVE-2020-1472):	Setting up specific detection mechanisms to alert on exploitation attempts of the Zerologon vulnerability, using traffic patterns and anomaly detection.
Detection of ASREPRoast:	Techniques for identifying AS-REP roasting attacks through abnormal AS-REP ticket requests without pre-authentication, indicating potential credential theft.
Detection of Kerberoasting:	Configuring alerts for unusual TGS ticket requests that could signify kerberoasting attempts, focusing on abnormal service ticket activity.

3.11.1.3 Planning for Preparedness

Participants are expected to have:

- An understanding of cyber range operations and the foundational principles of detection engineering.
- Knowledge of Sentinel and Wazuh, or a willingness to learn about these tools during the workshop.
- Basic familiarity with the attacks discussed in the penetration testing lab, as this workshop will focus on detecting rather than executing these attacks.
- Participants will be given remote access to lab environments. This approach allows for hands-on practice with detection tools and techniques in a realistic setting, without the need for local installations.

3.11.1.4 Materials and Exercises

Materials and exercises include:

Slides: Comprehensive slides will be shared, detailing detection methodologies, configuration guides for Sentinel and Wazuh, and case studies demonstrating successful detection of the specified attacks.

Remote Labs: Participants will have access to remote lab environments equipped with Sentinel and Wazuh, enabling them to configure and test detection rules against simulated attack scenarios.

3.11.2 CSP0011_S_M: Cyber Ranges and Operations for Maritime

3.11.2.1 Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP011_S_M**
Module Title *The title of the training module*	**Cybersecurity in Ports**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	*Cybersecurity in Maritime*
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S
Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This Seminar is a specialized and intensive program focused on enhancing cyber security in port environments. This seminar is dedicated to imparting vital knowledge and hands-on skills necessary for protecting port systems and infrastructure from cyber threats. Trainees will immerse themselves in the complex world of port cyber security, examining the myriad of threats and attacks that could jeopardize the security and efficiency of port operations..

Module description *Indicates the main purpose and description of the module.*	The CyberPort training program is designed to specifically address the unique cyber security challenges in port environments. It brings together world-renowned experts to enhance technical skills in key areas of cyber security, with a special focus on ports. The program covers ethical hacking, risk management, incident handling, and practical cybersecurity issues specific to maritime ports.
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Understanding of Port-Specific Cyber Threats: Participants will gain a comprehensive understanding of the unique cyber threats faced by maritime ports, including asset vulnerabilities and potential attack vectors. Proficiency in Binary Exploitation Techniques: Trainees will develop skills in binary exploitation, learning how to identify and exploit vulnerabilities in software used in port systems. Effective Cyber Attack Response: Participants will be trained in hands-on cyber attack response techniques, enabling them to effectively manage and mitigate incidents in real-time. Risk Assessment and Management Skills: The ability to conduct thorough risk assessments, identify critical assets, and implement robust risk management strategies specific to port environments. Practical Experience with Cybersecurity Tools: Hands-on experience with popular cybersecurity tools and platforms, including penetration testing and red-teaming tools.

Main topics and content list *A list of main topics and key content*	Introduction to Maritime Port Cybersecurity Overview of cyber threats specific to maritime ports The importance of protecting critical port assets Binary Exploitation and Vulnerability Assessment Fundamentals of binary exploitation Tools and techniques for vulnerability assessment in port systems Risk Assessment in Port Environments Methodologies for conducting risk assessments Identifying and prioritizing critical assets in ports Cyber Attack Response and Incident Handling Strategies for effective cyber attack response Hands-on incident handling exercises Compliance and Regulatory Frameworks Understanding legal and regulatory requirements in maritime cyber security
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	*Practical Exercises and Labs: Assessment of skills through hands-on exercises evaluating participants' abilities in binary exploitation, risk assessment, and cyber attack response.* *Written Examination: A comprehensive written test to assess understanding of theoretical concepts, including maritime port cybersecurity threats, risk management, and compliance frameworks.* *Incident Response Simulation: A simulated cyber attack scenario to evaluate participants' practical skills in real-time incident handling and response.* *Participation and Engagement: Continuous assessment of participant engagement and contribution during seminar discussions and group activities.*
Training Provider *Name(s) of training providers.*	UPRC

Contact *Name(s) of the main contact person and their email address.*	Prof. Nineta Polemi polemid@unipi.gr
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	5th to 9th February 2024
Duration *Duration of the training.*	5d
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*(4) Cybersecurity Policy, Process, and Compliance* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *(9)Penetration Testing*

Pre-requisites	Kali Linux -> Nmap, GDB compiler
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	-
Tools to be used *A list of tools that will be used for the operation of this training module.*	Custom VMs
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	TBA
Other important dates *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.*	-

3.11.2.2 Adapted Syllabus

Main topics	Suggested Content
Day 1: Introduction to Maritime Port Cybersecurity	Introduction to the seminar The effect of digitalization of maritime operations on efficiency Practical aspects of the seminar
Day 2: Maritime security environment: the state of play	Security Fundamentals in the port environment Fundamental cybersecurity concepts Maritime threats landscape Real life security incidents in the ports Recognizing vulnerabilities and attacks
Day 3 :Practical Security Management	Stages of Risk Management Efficient cybersecurity governance model (ISMS) based on ISO 27001 Estimating risk levels and mitigation measures based on ISO 27005 ISPS security management The interplay of physical and cybersecurity risk management Incident handling processes
Day4: Security Procedures and Policies	Mitigation Plan Security Policy Business Continuity and Disaster Recovery Plan Supply chain services Supply Chain Threats Identification and response on cyber attacks
Day5: Future Challenges and Directions	How to recover from cyber attacks Emerging threats in the maritime sector in the years to come Practical skills and defensive competencies needed

3.11.2.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.11.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.11.3 CSP0011_SA_M: Cyber Ranges and Operations for Maritime

3.11.3.1 Description of Training Module

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP011_SA_M**
Module Title *The title of the training module*	**Maritime Cyber Security Summer School - CyberHot**
Alternative Title(s) *Used alternative titles for the same module by many instututes and trainning providers*	*Cyber Ranges and Operations for Maritime*
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	S
Level *Training level: B (Basic), A (Advanced)*	A (Advance)
Module overview *High-level 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 *Indicates the main purpose and description of the module.*	The CyberHOT training program brings worldwide experts to raise the technical capabilities in various areas of Cyber Security including ethical hacking, risk management, incident handling and sector specific cybersecurity practical issues in the areas of maritime, maritime and energy. It will enable the participants to implement various red-teaming methodologies and tools. Utilizing dedicated labs (e.g. by HacktheBox), a wide range of penetration testing scenarios will be showcased. The aim is to raise the skills of the workforce to meet current and future cyber incidents and challenges. Each training module will include introductory lectures on basic concepts and challenges to enhance the Cyber Threat Intelligence; will cover popular risk assessment/red-teaming/penetration testing tools, along with basic steps followed in risk management penetration testing methodologies. The trainees will be introduced to the Dedicated labs of the Hack the Box platform where each participant will boot their own instances of attacker and target machines and pawn them along with the lecturers.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Upon successful completion of this module the learner will be expected to be able to: Develop advanced technical skills in various aspects of Cyber Security. Gain expertise in ethical hacking and penetration testing. Acquire knowledge and capabilities in risk management and incident handling. Understand sector-specific cybersecurity challenges in maritime, maritime, and energy industries. Implement red-teaming methodologies and tools effectively. Enhance skills in Cyber Threat Intelligence. Perform enumeration on web services. Research vulnerabilities in known components. Exploit existing vulnerabilities using tools like Metasploit and public exploits. Implement privilege elevation on compromised targets.
Main topics and content list *A list of main topics and key content*	Introduction to Cyber Security and Ethical Hacking. Risk Management and Incident Handling in Cyber Security. Sector-specific Cybersecurity Challenges (Maritime, Maritime, Energy). Red-Teaming Methodologies and Tools. Penetration Testing Concepts and Tools. Cyber Threat Intelligence Basics. Enumeration Techniques for Web Services. Researching Vulnerabilities in Known Components. Exploiting Vulnerabilities with Metasploit and Public Exploits. Implementing Privilege Elevation on Compromised Targets.
Evaluation and verification of learning outcomes	*Assessment will include hands-on practical exercises and labs.*

Assessment elements and high-level process to determine participants have achieved the learning outcomes	*Participants will engage in penetration testing scenarios using dedicated labs.* *Completion of CTF (Capture The Flag) challenges on the Hack the Box platform.* *Evaluation of the participants' ability to implement enumeration, research vulnerabilities, and exploit them.* *Assessment of privilege elevation skills on compromised targets.* *Theoretical knowledge will be tested through quizzes and exams.* *Continuous evaluation of participants' progress during the training modules.* *Certificates of completion may be awarded to participants who meet predefined performance criteria.*
Training Provider *Name(s) of training providers.*	UPRC, FP, TUC, trustilio
Contact *Name(s) of the main contact person and their email address.*	Prof. Nineta Polemi polemid@unipi.gr info@cyberhot.eu
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	To be posted on the DCM
Duration *Duration of the training.*	1d
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, Virtual, or Both (please check the DCM)

Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	*(4) Cybersecurity Policy, Process, and Compliance* *(7)Cybersecurity Threat Management* *(8)Cybersecurity Tools and Technology* *(9)Penetration Testing*
Pre-requisites	Kali Linux -> Nmap, Sqlmap, Hydra, BurpSuite, Owasp-zap, Metasploit
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	-
Tools to be used *A list of tools that will be used for the operation of this training module.*	HtB platform
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
ECTS *If applicable, the number of ECTS.*	NA
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	CoA
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	See DCM

Other important dates *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.*	See DCM

3.11.3.2 Adapted Syllabus

Main topics	Suggested Content
Introduction to HtB (Hack the Box) platform - Penetration Testing Walkthroughs 1	Basic Windows knowledge Port and Service Enumeration Exploit Modification Metasploit
Penetration Testing Walkthroughs 2	Linux Port Scanning and Enumeration Web Fuzzing Locating Recently Modified Files
Capture the Flag, Penetration Testing Exercise	Challenge 5 Highlights: § Python § Linux § XXE Injection § Source Code Review Challenge 6 Highlights: § Enumeration § Exploit Development § ROP § Cracking keepass databases Challenge 7 Highlights: § Enumeration § SQL Injection § Java Classes § Debugging with JDWP

	§ Speech to Text

3.11.3.3 Planning for Preparedness

Refer and check online CyberSecPro DCM System for current information.

3.11.3.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.12 Module 12 - Digital Forensics for Maritime

3.12.1 CSP0012_S_M: Digital Forensics for Maritime

3.12.1.1 Description of Training Module

Systems as AIS and GNSS are often targeted by third parties to hamper maritime operations. After an attack by spoofing mainly the research for proofs and elements confirming the attack are needed, They serve as forensic evidence during investigations and enable maritime law enforcement forces or security agencies to maintain robust cybersecurity and privacy practices while effectively managing and securing their assets.

3.12.1.2 Adapted Syllabus

Main topics	Suggested Content
Cybersecurity Forensics in Maritime system	Identification of attacks on dedicated maritime systems AIS as an example of attacks satellite based GNSS systems Evidence of attacks findings
Identification of evidence after Maritime systems	Example of recent cyber incidents in maritime sectors The AIS messages - formats and standards Ways to jam and spoof maritime AIS Jamming of AIS and GNSS Spoofing of AIS and GNSS Common attack tactics, techniques used when hacking AIS systems Security controls for information systems against common threats.
GNSS / AIS legal Frameworks	IMO AIS regulation ITU radio communications regulation GNSS legal aspects
Legal analysis / use cases	AIS spoofing and jamming examples The specific threats on Satellite ADSB system in Air transport

3.12.1.3 Planning for Preparedness

The planning of this module needs the deployment of a simulating environment as well as the connection to an AIS transponder and/or a connected system or a simulated environment.

The presence of an expert from law enforcement agencies (coastguards or maritime police) could be added if available.

3.12.1.4 Materials and Exercises

On hands training and additional exercice with law enforcement agencies (to be confirmed for each session). Powerpoint support slides will be utilised.

4 Conclusions

This manuscript delineates the detailed syllabi for each of the 12 CyberSecPro (CSP) Maritime Modules, meticulously crafted to meet the cybersecurity requirements specific to the maritime sector. These modules have been developed with the aim of arming maritime professionals with indispensable skills and knowledge to safeguard critical maritime information and infrastructure against cyber threats. Each module's syllabus is meticulously formulated, drawing upon the templates outlined in D3.1 and the Cybok framework, thus ensuring its relevance and practical applicability to the unique challenges encountered within the maritime domain.

The overall operational plan for the CSP Maritime Modules takes into account the inherent challenges associated with integrating new courses into established Higher Education Institution (HEI) programs. To circumvent these obstacles, CSP partners have introduced seminars, workshops, and exercises that can be seamlessly incorporated as supplementary topics into existing curricula. This adaptable approach facilitates the inclusion of cutting-edge cybersecurity subjects in maritime professional training, circumventing the need for extensive curriculum revisions. Moreover, these modules can be seamlessly integrated into summer schools and conferences, providing additional avenues for maritime professionals to augment their cybersecurity knowledge and skills.

By adopting this strategy, the CSP Maritime Modules aim not only to uphold academic rigor but also to foster practical relevance, equipping maritime professionals with the necessary resources to effectively combat the evolving cybersecurity threats prevalent within the maritime sector.