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

CyberSecPro

D3.3
CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Health.

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

Related WP	WP3	Dissemination Level	PU - Public
Lead Participant	UPRC	Lead Author	Dimitris Koutras (UPRC)
Contributing Participants	TUBS, LAU, CNR, SINTEF, UNI, IMT, trustilio, FP, IMTL, PDMFC, SGI, SLC, ZEL, FCT	Related Deliverables	D4.1, D3.1

Abstract: The CyberSecPro (CSP) portfolio of cybersecurity curricula and detailed syllabi targeted the critical sector of healthcare. The report is a collection of CSP training courses designed to enhance the skills of healthcare professionals in the realm of cybersecurity. The content of the syllabi combines CSP generic and sector specific aspects to provide holistic CSP module training for the critical health sector. The deliverable reflects the outcomes of Task 3.4.

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 of cybersecurity curricula targeted to the healthcare industry and professionals. The report is a collection of CSP training courses designed to enhance the skills of healthcare professionals in the realm of cybersecurity. The curriculum focuses on the critical areas and topics identified during the study of CSP development work from the market analysis meeting the supply of training from the CSP partners. This is a comprehensive collection of CSP modules and its syllabi for the healthcare specific critical sector. It covers the wide range of CSP module syllabi including (and not limited to) human-factors of cybersecurity, data security and privacy, network and communication security. The content of the syllabi combines CSP generic and sector specific aspects to provide holistic CSP module training for the critical health sector. The goal is to empower healthcare providers with the necessary tools and expertise to protect sensitive patient data and ensure the integrity of their healthcare systems. With a strong focus on hands-on training and practical learning, the CSP curriculum provides healthcare professionals with the opportunity to apply their skills in working-life. CSP portfolio empowers healthcare providers to make informed decisions and take proactive measures to protect their healthcare organisations against cyber threats.

Document information

Contributors

Name	Beneficiary
Dimitris Koutras, Professor Panos Kotzanikolaou, Dimitris Kalergis	UPRC
Paresh Rathod, Paulinus Ofem, Jyri Rajamäki	LAU

Reviewers

Name	Beneficiary
Pinelopi Kyranoudi	TUC
Cristina Alcaraz	UMA
Theodoros Karvounidis	UPRC
Nineta Polemi	UPRC
Jeldo Arno Meppen	ACEEU

History

Version	Date	Contributor(s)	Comment(s)
0.1	2023-09-01	Dimitris Koutras	1st Draft of ToC
0.2	2024-01-30	Paresh Rathod	Draft of the Abstract and Executive Summary
0.3	2024-02-01	Paresh Rathod	Section 3.1.1: Module-1 Syllabus Updated
0.4	2024-02-08	Dimitris Koutras	modules contribution
0.5	2024-02-10	Dimitris Koutras	overall update
0.6	2024-02-14	Dimitris Koutras	overall update-modules addition-template modification
0.7	2024-02-14	Dimitris Koutras	modules addition
0.8	2024-02-29	Dimitris Koutras – Cristina Alcaraz	Information update- revision of the external reviewers proofreading.
0.81	2024-03-18	Dimitris Koutras - Pinelopi Kyranoudi	Information update- revision no 2 of the external reviewers proofreading.
0.9	2024-03-25	Nineta Polemi – Theodoros Karvounidis	review
0.91	2024-04-30	Jeldo Arno Meppen	review
0.92	2024-05-07	Nineta Polemi – Theodoros Karvounidis – Dimitris Koutras	Final reviewed version upload to svn
0.93	2024-05-23	Dimitris Koutras	Send for review before the final upload
0.94	2024-05-30 – 2024-06-03	Ahad Niknia – Dimitris Koutras	Review and improve the layout
1.00	2024-06-06	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Tables

List of Acronyms

2	**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 LAN
	VPN	Virtual Network Private
	VR	Virtual Reality
W	**WAN**	Wide Area Network
	WLAN	Wireless LAN
	WMAN	Wireless MAN
	WP	Work Package
	WPA	Wi-Fi Protected Access
	WPA2	Wi-Fi Protected Access 2
X	**XSS**	Cross Site Scripting

Glossary of Terms

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 health, 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).

1 Introduction

The increasing complexity and volume of cyber threats pose a significant risk to the health sector, necessitating robust cybersecurity training and awareness. The CyberSecPro (CSP) project, through its comprehensive research and analysis, has identified a gap in the current cybersecurity training offerings for healthcare professionals. This gap underscores the need for a specialized education and training programme that addresses the unique challenges and vulnerabilities inherent to the health sector. Recognizing this, the CSP project has developed a series of deliverables, with a particular emphasis on deliverables D2.1, D2.2, and D2.3 from Work Package two. These foundational deliverables have laid the groundwork for a targeted approach to cybersecurity training within the health sector, culminating in the creation of 12 core training modules. These modules are specifically designed to equip healthcare professionals with the skills and knowledge required to navigate and mitigate the cybersecurity threats they face daily. This deliverable aims to outline the structure, requirements, and specifications of these training modules, providing a comprehensive framework for the CyberSecPro education and training programme tailored to the health sector.

1.1 Background

The necessity for specialized training in the health 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, CSP, in 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 skills of professionals in the health sector.

1.2 Purpose and Scope

This section elaborates on the objectives and the breadth of the CyberSecPro training programme, emphasizing its design to fill the cybersecurity skills gap within the health sector. It explains the rationale behind the programme and its expected impact on healthcare professionals' ability to safeguard sensitive information and infrastructures.

1.3 Relation to Other Work Packages and Deliverables

This document will detail the integration and relationships between these deliverable and other components of the CyberSecPro project. It will highlight how these deliverable complements and extends the work done in other packages, illustrating the cohesive effort to bolster cybersecurity in the health sector.

1.4 Structure of the Deliverable

Utilizing the templates from D3.1, this section provides a roadmap for the deliverable, detailing its composition and guiding readers through the sections and subsections. It outlines how the deliverable is organized to offer a thorough understanding of the CyberSecPro programme, specifically tailored to the cybersecurity needs of the health sector.

2 Mapping from Generic to Specific Training Modules

2.1 Value Proposition for Health

The health 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 health sector cannot be overstated, given the potential risks and real-world consequences of cyber incidents. The justification for this targeted focus on health cybersecurity arises from several key considerations:

- **Real Cyberattacks and Vulnerabilities:** The health sector has witnessed numerous cyber incidents, ranging from ransomware attacks that cripple hospital systems to data breaches that expose patient information. Such events not only disrupt healthcare services but also erode patient trust and can lead to direct harm. Analysing these incidents reveals patterns and common vulnerabilities that training can address, making cybersecurity not just an IT concern but a patient safety issue.
- **Needs from D2.1:** The findings from deliverable D2.1 highlight specific cybersecurity knowledge gaps and training needs within the health 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 healthcare 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 healthcare professionals. By focusing on actual incidents and the specific needs identified in D2.1, the CSP Health Modules aim to equip healthcare professionals with the knowledge and skills necessary to safeguard their digital and physical environments against cyber threats, ensuring the continuity and integrity of healthcare services

2.2 Development Methodology for CSP Health Modules

The development of the CSP Health Modules follows a structured methodology designed to ensure that each training module is relevant, comprehensive, and directly applicable to the health 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 healthcare.
   b. **Parametrization and Adaptation to the Application Context:** The syllabus for each module is then tailored to the specific application context of the health 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 healthcare professionals. The adaptation process involves customizing examples, case studies, and exercises to reflect real-world healthcare scenarios, enhancing the applicability and effectiveness of the training.

The methodology behind the development of CSP Health Modules is iterative and collaborative, involving feedback from cybersecurity experts, healthcare 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 healthcare sector. By leveraging the foundational templates and adapting

them to the specific context of health, 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 aspects, ECTS and Video Teasers for CSP Training Modules for Health

As mentioned above, 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. A platform where the user will enter and find all the material for all the modules presented. The details concerning this platform are described in the deliverable D 3.1

Regarding the training material and the aspects discussed in the following chapter, an explanation is provided detailing how these elements of the module are structured and described. For each training module, detailed information is provided in this chapter regarding the following aspects: duration, type, training method, training provider, tools, learning material, means of verifying learning outcomes, certificates awarded, and evaluation processes. All these elements are meticulously documented and presented on a per-module basis to ensure clarity and accessibility of information.

As for the scheduling of training sessions, specific dates are not included in this chapter, as they are subject to change based on the dynamic nature of the training framework. Exceptions may apply in certain cases, where fixed schedules are predefined. For all other instances, trainees are advised to contact the designated training provider or platform for up-to-date scheduling information and any further clarification required.

Regarding the ECTS element, the work package WP3 proposed and built new cybersecurity training modules focusing on the sectors of maritime, health, and energy. In detail, a set of 72 training modules (generic and sector-specific) has been designed. The employed training model is focused to the needs of adult learners, it is aligned with the objectives of training providers to provide courses equipped with micro-credentials addressing market real needs by bridging the gap between education / training and work. This employed training model is based on the principle of learning outcomes so as to exploit effectively and efficiently related EU tools (e.g. ECTS, ECVET, EQF, Europass, etc.). Regarding the ECTS adoption, an in-depth study has been included in the task T3.3 (deliverable D3.2; Section 3.3) which sheds light on the credits in training programs' issue. According to the latest of the EU documents[1,2], and especially the QUATRA - TPG A Working Group on Micro-credentials (Q4 of 2023) guidelines and recommendations[3], the micro-credentials adoption and their ECTS mapping are still missing from the agendas of the EU National Education Authorities, the Higher Education Institutes, and the Quality Assurance Agencies. Nevertheless, the CSP project has proposed a novel and formulated path to calculate the micro-credentials' volume on each CSP module and on any professional training module outside the scope of this project. It must be noted that the micro-credentials volume has been announced on the DCM platform regarding each training module which has been designed during the tasks T3.4, T3.5, and T3.6.

[1] https://www.etf.europa.eu/sites/default/files/2023-05/Micro-Credential%20Guidelines%20Final%20Delivery.pdf
[2] https://education.ec.europa.eu/education-levels/higher-education/micro-credentials
[3] https://ehea.info/Immagini/QUATRA_-_TPG_A_recommendations_on_micro-credentials_09.11_.2023_.pdf

Mapping from Generic to Specific Training Modules

3 CyberSecPro Customised Modules Syllabus for Health

3.1 Module 1 - Cybersecurity Essentials and Management for Health Sector

3.1.1 CSP001_W_H: Cybersecurity Essentials and Management for Health Sector

3.1.1.1 Description of Training Module and Needs

The module provides a comprehensive overview of cybersecurity's essential concepts and management. *This training module dives into the critical world of cybersecurity in the healthcare sector, specifically designed for professionals working in hospitals, clinics, medical devices, and related organisations. Whether you're a healthcare manager, IT professional, or simply someone who handles sensitive patient data, this module equips you with the knowledge and skills to protect vital information and systems.*

Table 1: Module 1.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP001_W_H**
Module Title *The title of the training module*	**Cybersecurity Essentials and Management for Health Sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Healthcare Cybersecurity Foundations 2. Essential Cybersecurity for Healthcare Professionals 3. Healthcare Cybersecurity Fundamentals: Threats, Controls, and Best Practices 4. Managing Cybersecurity Risks in Healthcare: A Practical Training 5. Building a Culture of Security: Essential Practices for Healthcare Organisations
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

Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This comprehensive training module dives deep into the essential concepts and principles of cybersecurity in the healthcare sector. Designed specifically for healthcare professionals, this CSP training module equips you with the knowledge and skills to protect critical patient data and systems from cyber threats.
Module description *Indicates the main purpose and description of the module.*	In the current digital healthcare landscape, safeguarding patient data and critical infrastructure is paramount. The risk of cyberattacks and threads is growing as patient data becomes increasingly digitised and medical devices connect to networks. This training module equips you, the frontline defender, with the knowledge and skills to protect these vital systems and safeguard sensitive patient information. Designed for healthcare professionals at all levels, from managers and administrators to IT specialists and clinical staff, this module offers training on Foundational Cybersecurity Principles, Patient Data Protection, Managing Cybersecurity Risks, Ethical and Professional Practices, Building a Secure Culture, Essential Cybersecurity Controls, Cybersecurity governance and many other topics.

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 (Understanding and Awareness of following)** Key cybersecurity concepts and principles as they apply to the healthcare sector. Common cyber threats and vulnerabilities specific to healthcare IT systems and devices. Patient data privacy regulations and compliance requirements. Risk management frameworks for healthcare cybersecurity. Essential cybersecurity controls and their implementation in healthcare settings. The importance of building a culture of cybersecurity within an organisation. Ethical considerations and professional responsibilities in healthcare cybersecurity. **Skill and Competence (applications and practice):** ● Apply best practices for protecting patient data and privacy in healthcare settings. ● Conduct basic risk assessments for healthcare IT systems and devices. ● Implement and maintain essential cybersecurity controls (e.g., access control, encryption). ● Identify and report suspicious activity or potential security incidents. ● Communicate effectively about cybersecurity risks and best practices to colleagues. ● Analyse real-world healthcare cybersecurity scenarios and propose solutions. ● Evaluate the effectiveness of different cybersecurity controls for specific situations. ● Identify potential ethical challenges in healthcare cybersecurity situations. ● Work effectively with colleagues from different disciplines to address cybersecurity challenges. ● Contribute to building a more secure and aware cybersecurity culture within the organisation. ● 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*	• Introduction to Healthcare Cybersecurity Essentials • Common cybersecurity threats and vulnerabilities in healthcare. • Best practices for protecting patient data and privacy. • Healthcare cybersecurity risks through effective assessment and mitigation strategies. • Essential cybersecurity controls for healthcare IT systems and devices. • Building a secure culture within your organisation. • Ethical and professional challenges in healthcare cybersecurity. • Cybersecurity Governance for Healthcare Organisations • Cybersecurity Compliance and Regulations for Health sector • 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 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).*	Refer and check online CyberSecPro DCM System for current information

Duration *Duration of the training.*	3 h
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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.
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.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3. Recommended equivalent to 5 ECTS
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.*	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: Module 1.1 Syllabus

Main topics	Suggested Content
Topic-1: Introduction to Healthcare Cybersecurity Essentials	• The changing healthcare landscape and growth of digital health technologies and connected medical devices. • Increased reliance on electronic patient records (EHRs) and data analytics. • Cybersecurity threats and impact on healthcare including Data breaches, ransomware attacks, and malware infections. • Financial losses, operational disruptions, and reputational damage. • Patient safety and privacy risks. • Regulatory landscape and compliance requirements including EU health data, HIPAA, HITRUST, and other relevant regulations. • Importance of data privacy and security standards.
Topic-2: Common Cybersecurity Threats and Vulnerabilities in Healthcare	• Malware: Viruses, ransomware, spyware, and other malicious software. • Phishing and social engineering: Techniques to trick users into revealing sensitive information. • Insider threats: Malicious or negligent actions by authorised users. • Unsecured medical devices: Vulnerabilities in medical equipment and connected devices. • Weak password management: Lack of strong passwords and multi-factor authentication. • Unpatched software: Failure to update software with security patches.
Topic-3: Best Practices for Protecting Patient Data and Privacy	• Data classification and encryption: Identifying and protecting sensitive data types. • Access control and user authentication: Limiting access to authorised users. • Data backup and recovery: Ensuring data availability in case of incidents. • Physical security: Protecting IT infrastructure and devices. • Security awareness training: Educating employees about cybersecurity best practices.

Topic-4: Managing Cybersecurity Risks Through Effective Assessment and Mitigation Strategies	• Risk assessment methodologies: Identifying and evaluating potential threats and vulnerabilities. • Risk mitigation strategies: Implementing controls to reduce identified risks. • Incident response planning and procedures: Preparing for and responding to security incidents. • Business continuity and disaster recovery: Ensuring operational continuity after an incident.
Topic-5: Essential Cybersecurity Controls for Healthcare IT Systems and Devices	• Network security: Firewalls, intrusion detection/prevention systems (IDS/IPS). • Endpoint security: Antivirus, application whitelisting, endpoint detection and response (EDR). • Identity and access management (IAM): Strong passwords, multi-factor authentication, role-based access control (RBAC). • Data security: Encryption, data loss prevention (DLP). • Email security: Spam filtering, phishing detection.
Topic-6: Building a Secure Culture within Your Organization	• Human Aspects of Cybersecurity for the Health Sector • Importance of cybersecurity awareness and training: Engaging employees in security practices. • Promoting best practices through communication and collaboration: Sharing responsibility for security. • Reporting suspicious activity and security incidents: Encouraging timely reporting. • Rewarding positive security behaviour: Recognizing employees who contribute to security.
Topic-7: Ethical and Professional Challenges in Healthcare Cybersecurity	• Data privacy and patient confidentiality: Balancing access with security and privacy. • Responsible use of technology and social media: Avoiding misuse of patient data. • Professional codes of conduct and ethical considerations: Acting ethically in cybersecurity situations.
Topic-8: Cybersecurity Governance for Healthcare Organizations	• Roles and responsibilities for cybersecurity: Defining ownership and accountability. • Implementing and maintaining a cybersecurity program: Establishing a structured approach. • Continuous improvement and monitoring efforts: Regularly evaluating and updating security measures.

Topic-9: Cybersecurity Compliance and Regulations for Health Sector	• Overview of the European Regulatory Landscape: General Data Protection Regulation (GDPR), Network and Information Systems (NIS) Directive, eIDAS Regulation and Cybersecurity Act • Specific EU Regulations for Healthcare: EU Directive on cross-border healthcare, Medical Device Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR), EU Clinical Trials Regulation (CTR) • Understanding HIPAA, HITRUST, and other relevant regulations. • Implementing compliance requirements and best practices. • Strategies for ongoing compliance and reporting.
Topic-10: Case Studies and Practical Exercises	• Apply learned concepts to real-world healthcare cybersecurity scenarios. • Conduct mock risk assessments and incident response exercises. • Configure essential security controls in simulated environments. • Develop skills in communication and collaboration for security awareness.

3.1.1.3 Planning for Preparedness

As long as the trainees cover the required knowledge for the level of this seminar, its structure is designed in such a way that no special preparation is required on their part. Everything needed will be provided in advance on the DCM platform and will be covered throughout the seminar. Participants will be encouraged to lead discussions of various subjects.

3.1.1.4 Materials and Exercises

The training material is to be shared on the DCM platform in the form of comprehensive slides. Any exercises and tests related to this will be shared with trainees during the seminar.

3.1.1.5 Verification of Learning Outcomes, and Skills

Successful completion of attendance and at least borderline pass of the mean of the grades of the quizzes done during the seminar.

3.1.2 CSP001_CS-E_H: RxB - Cyber security management game

3.1.2.1 Description of Training Module and Needs

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 healthcare 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 healthcare 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 healthcare industry on a regular basis.

Table 3: Module 1.2 Description

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 institutes and training 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 health specific training scenario, where they will play as a cyber security manager of a hospital.
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 health 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).*	Refer and check online CyberSecPro DCM System for current information
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; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	Refer and check online CyberSecPro DCM System for current information. The dates on which the module is offered are subject to change and considered dynamic.
Other important dates	Refer and check online CyberSecPro DCM System for current information.

3.1.2.2 Adapted Syllabus

Table 4: Module 1.2 Syllabus

Main topics	Suggested Content
Threats and Vulnerabilities for the health 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 Cybersecurity in the health sector	• Examples based on case studies from real-world health incidents. • Consequences of neglecting the human factor in the health sector.

3.1.2.3 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.

3.1.2.4 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.

3.1.2.5 Verification of Learning Outcomes, and Skills

The RxB exercise will primarily be evaluated through **performance based assessment.** This will primarily be through feedback within the game, which gives the user an idea of how their choices impacted the outcome. Furthermore, the user will be given a questionnaire that will have the user reflect upon cybersecurity practices and priorities that were presented in the game, which would fall under **attitudinal assessments**.

3.2 Module 2 - Human Factors and Cybersecurity for Health

3.2.1 CSP002_S_H: Cybersecurity and Health

3.2.1.1 Description of Training Module and Needs

The "Cybersecurity and Health" course is designed to address the intersection of cybersecurity principles and the healthcare sector. This comprehensive training module aims to provide participants with a nuanced understanding of the unique challenges and requirements in securing health-related data and systems. The course will cover key topics such as data protection, regulatory compliance, and risk management specific to the healthcare industry. Through a combination of theoretical insights and practical scenarios, participants will gain the necessary skills to navigate the evolving landscape of cybersecurity within the health domain. This training is tailored to professionals seeking a specialized knowledge base to effectively safeguard sensitive health information and contribute to the overall resilience of healthcare cybersecurity frameworks.

Table 5: Module 2.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP002_S_H**
Module Title *The title of the training module*	**Cybersecurity and Health**

Alternative Title(s) Used alternative titles for the same module by many institutes and training providers	"Securing Healthcare: A Cybersecurity Approach" "Digital Health Protection: Cybersecurity Essentials" "HealthTech Security: Navigating the Cyber Landscape" "Guarding Wellness: Cybersecurity in Healthcare Systems" "E-Security in Health: Safeguarding Patient Data" "Healthcare Cyber Resilience: Strategies for Protection" "Digital Patient Safety: Cybersecurity in Health Technologies" "Cyber Hygiene for Health Professionals" "Secure Health Infrastructures: Cyber Challenges and Solutions"
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	In ”Cybersecurity and Health" seminar where we will delve into the critical intersection of cybersecurity and healthcare. We will cover essential topics such as the evolving threat landscape, vulnerabilities in medical devices, regulatory compliance, practical strategies for healthcare institutions, and the human element in cybersecurity. Through informative sessions, real-world case studies, and expert insights, attendees will gain a comprehensive understanding of the challenges and opportunities in securing health data and infrastructure, ensuring they leave with practical knowledge to enhance cybersecurity in the healthcare sector.
Module description Indicates the main purpose and description of the module.	The "Cybersecurity and Health" seminar offers an immersive exploration of the dynamic intersection between cybersecurity and the healthcare sector. Attendees will gain valuable insights into the evolving threat landscape, vulnerabilities in medical devices, and regulatory compliance specific to healthcare cybersecurity. The module equips participants with practical strategies tailored for healthcare institutions, emphasizing the importance of addressing the human element in cybersecurity. Through informative sessions, real-world case studies, and expert insights, attendees will leave with a comprehensive understanding of the challenges and opportunities in securing health data and infrastructure. The seminar aims to empower participants with actionable knowledge to enhance cybersecurity measures within the healthcare industry. Throughout the module, participants will delve into the complexities of safeguarding sensitive medical information, understanding regulatory frameworks, and implementing effective cybersecurity strategies. The learning methodology incorporates informative sessions led by industry experts, real-world case studies to illustrate practical applications, and insights from cybersecurity professionals. By the conclusion of the seminar, attendees will possess a nuanced understanding of the intricacies involved in healthcare cybersecurity and be well-prepared to contribute actively to the ongoing enhancement of cybersecurity measures within the healthcare sector.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Knowledge: • *Comprehensive Understanding:* Develop a profound understanding of the evolving threat landscape in healthcare cybersecurity, including emerging risks and trends. • *Regulatory Awareness:* Acquire knowledge of regulatory frameworks governing cybersecurity in healthcare, ensuring compliance and adherence to industry standards. • *Medical Device Security:* Gain insights into vulnerabilities inherent in medical devices and technologies, with the ability to implement effective measures for securing critical healthcare components. Skills: *Practical Strategies:* Develop practical strategies for healthcare institutions, encompassing the implementation of robust cybersecurity measures to safeguard patient information and ensure the integrity of healthcare operations. • *Risk Mitigation:* Acquire skills in identifying, assessing, and mitigating cybersecurity risks specific to the healthcare sector, fostering proactive measures to counter potential vulnerabilities. • *Human Element Integration:* Incorporate behavioural insights into cybersecurity practices, implementing training protocols and awareness initiatives to fortify the human element in healthcare cybersecurity. Competences: *Regulatory Compliance Implementation:* Demonstrate the ability to navigate and implement effective strategies to meet regulatory compliance requirements, ensuring the seamless integration of cybersecurity practices within healthcare institutions. • *Critical Analysis:* Apply critical analysis skills to real-world case studies, extracting lessons learned, identifying successful implementations, and understanding challenges in healthcare cybersecurity. • *Collaborative Contribution:* Develop competences to actively contribute to the ongoing enhancement of cybersecurity measures within the healthcare sector, fostering a collaborative and proactive approach to cybersecurity challenges. These learning outcomes and targets aim to equip participants with a well-rounded set of knowledge, skills, and competences necessary for addressing the multifaceted challenges posed by cybersecurity in the healthcare domain.

Main topics and content list A list of main topics and key content	· Introduction to Cybersecurity in Healthcare · Evolving Threat Landscape in Healthcare · Vulnerabilities in Medical Devices and Technologies · Regulatory Compliance in Healthcare Cybersecurity · Practical Strategies for Healthcare Institutions · The Human Element in Healthcare Cybersecurity · Real-World Case Studies in Healthcare Cybersecurity · Expert Insights and Future Trends
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	Summative assessment: Learners are required to generate a comprehensive 2000-word report at the conclusion of the 'Cybersecurity and Healthcare' module. This report should encompass a series of tasks aimed at showcasing the outcomes of a threat and vulnerability assessment within the context of healthcare cybersecurity. Learners must address real-world scenarios, demonstrating their ability to identify and control threats effectively in the healthcare environment.
Training Provider *Name(s) of training providers.*	trustilio, SLC
Contact *Name(s) of the main contact person and their email address.*	Dr Shareeful Islam shareeful@gmail.com (SLC) Dr Kitty Kioskli kitty.kioskli@trustilio.com (trustilio)
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).*	● Date: 19/3/2024 ● Time: 13:00-15:00 UK Time ● Location: ARU Science Building, East Road, CB1 1PT, Cambridge, UK ● Date: 26/3/2024 ● Time: 13:00-15:00 UK Time ● Location: ARU Science Building, East Road, CB1 1PT, Cambridge, UK
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

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* (2) *Human Aspects of Cybersecurity* (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.*	All the tools and the platforms that they will be presented, are online so the trainers will need a Personal computer with world wide web access.
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; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.

3.2.1.2 Adapted Syllabus

Table 6: Module 2.1 Syllabus

Main topics	Suggested Content
Introduction to Cybersecurity in Healthcare	Explore the foundational principles of cybersecurity as they apply to the healthcare sector, delving into the unique challenges and critical importance of safeguarding sensitive patient data and medical infrastructure.
Evolving Threat Landscape in Healthcare	Examine the dynamic nature of cybersecurity threats facing healthcare organizations, from ransomware attacks to targeted breaches, and stay abreast of the latest trends impacting the security landscape in the healthcare industry.
Vulnerabilities in Medical Devices and Technologies	Investigate the potential vulnerabilities inherent in medical devices and technologies, understanding the risks associated with interconnected healthcare systems and implementing measures to secure critical devices against cyber threats.

Regulatory Compliance in Healthcare Cybersecurity	Navigate the complex regulatory landscape governing healthcare data security, ensuring a comprehensive understanding of compliance requirements and best practices to meet and exceed regulatory standards.
Practical Strategies for Healthcare Institutions	Provide actionable insights into developing and implementing effective cybersecurity strategies tailored specifically to healthcare institutions, covering risk management, incident response, and proactive measures for threat prevention.
The Human Element in Healthcare Cybersecurity	Explore the role of human factors in healthcare cybersecurity, emphasizing the importance of training, awareness programs, and creating a security-conscious culture to mitigate the impact of human-related vulnerabilities.
Real-World Case Studies in Healthcare Cybersecurity	Analyse real-world examples of cybersecurity incidents within the healthcare sector, dissecting the challenges faced, the responses employed, and the lessons learned to inform effective cybersecurity practices.
Expert Insights and Future Trends	Gain valuable perspectives from industry experts on emerging trends and advancements in healthcare cybersecurity, preparing learners to anticipate and adapt to evolving threats and technologies in the future.

3.2.1.3 Materials and Exercises

The "Cybersecurity and Health" seminar incorporates a diverse range of materials and exercises to provide participants with a comprehensive learning experience. Engaging presentations, curated case studies, and relevant research findings will be utilized to convey theoretical concepts and real-world applications. Practical exercises will immerse participants in simulated scenarios, allowing them to apply cybersecurity principles specifically tailored to the healthcare domain. Hands-on activities will include risk assessment simulations, incident response drills, and the evaluation of cybersecurity tools relevant to health information protection. Interactive discussions and group exercises will foster collaboration and critical thinking, enabling participants to address the unique challenges of securing sensitive health data. The seminar's well-rounded approach to materials and exercises ensures that participants gain both theoretical knowledge and practical skills essential for effective cybersecurity management in the healthcare sector.

3.2.1.4 Verification of Learning Outcomes, and Skills

At the conclusion of the seminar, participants will be encouraged to complete a brief evaluation assessing the topics covered and the knowledge imparted during the program. This feedback is invaluable in gauging the effectiveness of the seminar and tailoring future sessions to better meet the participants' needs. Furthermore, upon successful completion of the seminar, attendees will have the option to receive a Certificate of Attendance, recognizing their commitment to enhancing their understanding of the subjects discussed. This certificate can serve as a tangible acknowledgment of their participation and dedication to furthering their knowledge in the cybersecurity and health domain.

3.2.2 CSP002_SA_H: Human Aspects of Healthcare Cybersecurity

3.2.2.1 Description of Training Module and Needs

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: Module 2.2 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	CSP002_SA_H: Human Factors and Cybersecurity
Module Title *The title of the training module*	**Human Aspects of Healthcare Cybersecurity**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. The Human Dimension in Healthcare Cybersecurity 2. Navigating Healthcare Cyber Threats: The Human Element 3. Elements of Cyberpsychology in Healthcare" 4. Humans in Healthcare Cybersecurity 5. Human centric cyber defence in healthcare 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 healthcare stakeholders with the knowledge necessary about human aspects of cybersecurity pertinent for the healthcare 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 healthcare cybersecurity, examining the psychological, social, and organizational influences on security practices and decisions in a healthcare context. Attendees will uncover insights into human vulnerabilities that cyber attackers target in healthcare operations and acquire methods to cultivate a cybersecurity-aware culture within healthcare organizations. It further highlights the vital importance of communication and collaboration at strategic, operational, and tactical levels specific to the healthcare sector. Participants will investigate how proficient communication between healthcare domains and effective decision-making can strengthen cybersecurity measures in healthcare 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 healthcare domain. · Understand the critical role of communication and teamwork in bolstering healthcare cybersecurity across different sectors. · How decision-making frameworks are used at strategic, operational, and tactical levels within healthcare cybersecurity. · Recognize the profiles and strategies of adversaries targeting healthcare operations. · Evaluate human-related threats and vulnerabilities in healthcare contexts. **Competencies:** · Understand the discussions pertinent to healthcare cybersecurity at various levels of decision-making. · Cultivate an environment of transparent communication and teamwork focused on healthcare cybersecurity. · Reflect on cybersecurity decision-making with the understanding of how human factors are related in the healthcare arena. · Identify human-centric threats and vulnerabilities in healthcare operations.

Main topics and content list *A list of main topics and key content*	• Ethical and professional practices • Introduction to Human Aspects of Healthcare Cybersecurity • Psychological and Social Factors in Healthcare Cybersecurity • Human Vulnerabilities in Healthcare 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 Healthcare personnel • 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 healthcare cybersecurity case study that reflects over different human aspects of an healthcare cybersecurity breach
Training Provider *Name(s) of training providers.*	TalTech, Trustilio, Laurea
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*	Refer and check online CyberSecPro DCM System for current information

(e.g., even after the end of the CSP programme).	
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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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.*	Personal computer with world wide web access necessary. No special tools need to be installed

Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	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

3.2.2.2 Adapted Syllabus

Table 8: Module 2.2 Syllabus

Main topics	Suggested Content
Introduction to Human Aspects of Healthcare Cybersecurity	Healthcare cybersecurity landscape Cost of neglecting the human element Examining real-world healthcare incidents

Psychological and Social Factors in Healthcare Cybersecurity	Understanding cognitive biases Social engineering techniques Group dynamics
Human Vulnerabilities in Healthcare Cybersecurity	Insider threats Impact of stress and fatigue Case studies Mitigation strategies
Organisational Culture, Communication, and Healthcare Cybersecurity	Organisational values Leadership's role Proactive security culture for healthcare
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 healthcare. AI and automation

3.2.1.3 Planning for Preparedness

The seminar does not rely on specific practical tools, eliminating the need for extensive pre-planning.

3.2.1.4 Materials and Exercises

The "Cybersecurity and Health" seminar incorporates a diverse range of materials and exercises to provide participants with a comprehensive learning experience. Engaging presentations, curated case studies, and relevant research findings will be utilized to convey theoretical concepts and real-world applications.

3.2.1.5 Verification of Learning Outcomes, and Skills

At the conclusion of the seminar, participants will be encouraged to complete a brief evaluation assessing the topics covered and the knowledge imparted during the program.

3.3 Module 3 - Cybersecurity Risk Management and Governance for Health

3.3.1 CSP003_C_H: Cybersecurity Risk Management and Governance in the Healthcare sector

3.3.1.1 Description of Training Module and Needs

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet. The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

The requirements of ISO/IEC 27001 are generically phrased to be able to cover all organisations irrespective of size or industry. Although being able to support any organisation is one of the goals of the standard, adaptations, customizations and translations need to be implemented by organisations belonging to a specific sector. To facilitate this customization but also to further support the critical domain of Healthcare, ISO has created a topic specific standard called ISO 27799:2016, Information security management in health using ISO/IEC 27002. This standard builds upon ISO/IEC 27001 and ISO/IEC 27002 and provides guidance and recommendations for the healthcare domain, and allows learners of the healthcare domain to receive more concrete guidance, adapted to their language and context. This seminar focuses in providing an overview on how ISO 27799:2016 can help cybersecurity professionals in the healthcare domain, details some of the recommendations and guidance and instructs learners on how to read the standard in conjunction with the rest of the standards of the family.

Table 9: Module 3.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP003_SA_H**
Module Title *The title of the training module*	Cybersecurity Risk Management and Governance in the Healthcare sector

Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Cybersecurity Governance in Health 2. Health Cybersecurity Risk Management 3. ISO 27001 controls adapted to the healthcare domain
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 health stakeholders with an overview of cybersecurity risk management and governance. It allows the learners understand the mains concepts and identify the differentiation of the concepts when applied within the Healthcare domain.
Module description *Indicates the main purpose and description of the module.*	The module provides an understanding of the underlying properties and principles associated with cybersecurity risk management. Furthermore, the learners are provided with the opportunity to understand first the generic standards that are applicable and cover the domains of risk management and governance and understand how they are customized to fit the healthcare domain.

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 risk management as a process ● Gain knowledge of the different stages of risk management ● Gain knowledge on the governance structures and processes for cybersecurity ● Understand the various definitions regarding cybersecurity in the health domain. ● Become acquainted of the controls applied and the specific directions provided by standard ISO 27799, Health informatics – Information security management in health using ISO/IEC 27002. **Skill and Competence:** ● Analyse the results of a cybersecurity risk assessment. ● Ability to perform a risk assessment methodology and produce the relevant risk assessment results. ● Select suitable controls (as adapted and customized by ISO 27799) to treat relevant un acceptable risks.
Main topics and content list *A list of main topics and key content*	● Risk Management ● Governance processes ● Role, responsibilities and authorities ● Security controls and standards of the specific domain.
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 develop log book based on the individual exercise covered at the end of each session to demonstrate their understanding of the knowledge covered by the module. ● *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 tackle the threats based on a real-world scenario.

Training Provider *Name(s) of training providers.*	UPRC, APIRO
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).*	Refer and check online CyberSecPro DCM System for current
Duration *Duration of the training.*	8 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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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*
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.*	The tools to be used will be installed before the beginning of the course and will be changed according to the needs of the trainees
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.

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

3.3.1.2 Adapted Syllabus

The training module covers the following topics:

- Introduction to ISO/IEC 27001
- The relationship between clauses, Annex A and ISO/IEC 27002
- Current revision status of all relevant standards
- Terms and definitions of ISO 27000 adapted to the healthcare domain
- Guidance and recommendations on ISO 27002 controls for the healthcare domain.

Table 10: Module 3.1 Syllabus

Main topics	Suggested Content
Security controls and standards of the specific domain.	Introduction to ISO/IEC 27001, status, versions, structure (Clauses 1-4 and Annex A). ISO 27001:2013 control areas and ISO 27001:2022 control themes Terms and definitions of ISO 27000 adapted to the healthcare domain Guidance on existing ISO 27002 controls for the healthcare domain. Specific recommendations of ISO 27799 on cybersecurity in the healthcare domain

3.3.1.3 Planning for Preparedness

The seminar is not supported by any practical tools, so there are no specific needs for planning beforehand. The seminar can be either delivered online or face-to-face and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar) or tools (in case it is delivered online).

3.3.1.4 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 learners
- Standards for view only during the course: ISO/IEC 27001:2013, ISO/IEC 27001:2022, ISO/IEC 27002:2013, ISO/IEC 27002:2022, ISO/IEC 27799:2016.
- Exercises in the identification and mapping of specific controls within the healthcare domain.

The seminar is not supported by any practical tools, but the material and course presentation will be constructed in such a way that will promote interaction and participation of the learners. Activities and questions shall be included and carried out.

3.3.1.5 Verification of Learning Outcomes, and Skills

At the end of the seminar, the learners will be expected to fill in a quick evaluation on the subjects introduced and the knowledge provided.

Upon the completion of the seminar, it is possible to provide a Certificate of Attendance.

3.4 Module 4 - Network Security for Health

3.4.1 CSP004_C_H: Network Security for Health

3.4.1.1 Description of Training Module and Needs

In this training module the students are going to learn several basics on network protocols and how to administer networks in order to keep them secure and without creating any technical conflicts between communicating devices. Also, several principles and policies are presented in order to keep data and networks secure. Software techniques and hardware deployments are explained and also how they work on computer networks. Finally, security vulnerabilities are presented and explained in order to help students to understand how vulnerabilities work and how to prevent unauthorised access.

Table 11: Module 4.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP004_C_H**
Module Title *The title of the training module*	**Network Security for Health**

Alternative Title(s) *Used alternative titles for the same module by many institutes and training linuxproviders*	• Computer Networks: Protocols, Vulnerabilities, Data Protection, Policies and Linux Prerequisites for Efficient Administration and Setup
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, O (Lab)
Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	The module aims to provide health stakeholders with an overview of basic knowledge of network protocols, Linux commands to administer networks, known vulnerabilities and applied policies to secure networks and prevent unauthorised access
Module description *Indicates the main purpose and description of the module.*	The module provides an understanding of what the network protocols are, how they work (according to the RFC standards), known vulnerabilities and policies that should be applied to protect data and networks. Also, there are labs for some hands-on experience in order to display how networks operate in real time scenarios, demonstrate security breaches, prevention methods and live policies that could be applied for prevention and remedy in case of an exploit.

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 networks, security and Linux admin policies ● Gain knowledge of the different policies for authorization ● Gain knowledge about vulnerabilities, applying patches or settings to prevent them ● Usage of industry tools to do all the above. **Skill and Competence:** ● Computer Science focused on network protocols and security. ● Knowledge of Linux OS and use of terminal focusing to administer networks and servers ● Audit networks ● Theoretical knowledge and Reproduction security breaches ● Methods to prevent the above security issues ● Conditional data access and security methods to secure data.
Main topics and content list *A list of main topics and key content*	● Network basics ● Linux OS introduction ● Usage of Linux OS for network administration ● Vulnerabilities ● Security breaches.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	● Lab Exercises

Training Provider *Name(s) of training providers.*	TUBS
Contact *Name(s) of the main contact person and their email address.*	Prof. Vassilios Prevelakis 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).*	Refer and check online CyberSecPro DCM System foe further information concerning the dates when the module is offered.
Duration *Duration of the training.*	12 weeks of 2 academic hour of teaching + 10-15 Labs
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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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*	*(5) Network and Communication Security* *(6) Privacy and Data Protection* *(7) Cybersecurity Threat Management* *(8) Cybersecurity Tools and Technologies* *(9) Penetration Testing* *(10) Cyber Incident Response*
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.*	CYBERSECURITY ARCHITECT CYBERSECURITY AUDITOR CYBER THREAT INTELLIGENCE SPECIALIST PENETRATION TESTER CYBERSECURITY RESEARCHER CYBER INCIDENT RESPONDER
Tools to be used *A list of tools that will be used for the operation of this training module.*	Servers, Presentation files, VPN to access the Lab server and execute the exercises
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; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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. The dates can be changed dynamically.
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.

3.4.1.2 Adapted Syllabus

The training module covers the following topics:

Table 12: Module 4.1 Syllabus

Main topics	Suggested Content
Basic network fundamentals, architectures and protocols in Healthcare	a) Basic Linux Prerequisites, Basic Linux Network commands b) Networking Principles and Basics
Security in advanced network infrastructure in Healthcare	a) Principles For User Authentication b) Linux/Unix Access Control Principles (Bell – LaPadula Model) c) Public Key Encryption, Digital Signatures, PKI technology & interoperability, Cryptography, Ciphers, Perfect Secrecy, IND-CPA security, Hash Functions d) HSM (Hardware Security Modules) e) Integrity Protection Models f) TCSEC and common criteria

	g) Data Privacy
Common weaknesses and attacks in communication networks in Healthcare	a) DNS Security b) Software Vulnerabilities & Secure Software Market Failure

3.4.1.3 Planning for Preparedness

The seminar is supported by practical tools, but the instructions on how to use these tools will be presented also during the course. The course can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, 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 and the labs.

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 learners
- Labs

3.4.1.5 Verification of Learning Outcomes, and Skills

Students should attend all lessons and labs and fulfil the exercise sheets for the labs to get the Certificate of Attendance

3.4.2 CSP004_S_H: Cybersecurity - Endpoint protection in healthcare systems

3.4.2.1 Description of Training Module and Needs

The seminar "Cybersecurity: Endpoint protection in healthcare systems" delves into safeguarding healthcare systems through endpoint protection. It explores the unique cybersecurity challenges in healthcare, emphasising best practices for securing endpoints. Through case studies and collaboration, participants gain insights into defending digital health infrastructure. The seminar equips attendees with strategies to enhance network security, ensuring the integrity and confidentiality of healthcare data amidst evolving cyber threats.

Table 13: Module 4.2 Description

Code **Code format: CSP001_x where x is the training of offering type (see below)**	**CSP004_S_H**
Module Title **The title of the training module**	**Cybersecurity: Endpoint protection in healthcare systems**
Alternative Title(s) Used alternative titles for the same module by many institutes and training providers	“Network Security and Health” "Digital Health Protection: Endpoint protection" "Securing Healthcare Networks: Strategies for Endpoint Protection" "Safeguarding Digital Health: Best Practices for Endpoint Security" "Ensuring Network Security in Healthcare: Focus on Endpoint Protection" "Endpoint Security in Healthcare Networks: Challenges and Solutions" "Defending Digital Health Infrastructure: Endpoint Security Measures" "Network Security Strategies for Health Systems: A Focus on Endpoints" "Protecting Healthcare Data: Endpoint Security Essentials" "Cybersecurity Measures for Health Networks: Endpoint Defence" "Endpoint Security in the Era of Digital Health: Best Practices"

	"Securing Healthcare Information Systems: Endpoint Security Frameworks"
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 seminar delves into safeguarding healthcare systems through endpoint protection. It explores the unique cybersecurity challenges in healthcare, emphasizing best practices for securing endpoints. Through case studies and collaboration, participants gain insights into defending digital health infrastructure. The seminar equips attendees with strategies to enhance network security, ensuring the integrity and confidentiality of healthcare data amidst evolving cyber threats.

Module description Indicates the main purpose and description of the module.	The seminar "Cybersecurity: Endpoint protection in healthcare systems" is a comprehensive exploration of the crucial intersection between cybersecurity and healthcare systems, with a central focus on endpoint protection. Participants will delve into the intricate challenges faced by healthcare organizations in maintaining secure networks and safeguarding sensitive health data. Through in-depth discussions, case studies, and real-world examples, attendees will gain insights into the evolving threat landscape specific to the healthcare sector, including data breaches, and other malicious activities. A key highlight of the seminar is the emphasis on best practices for endpoint security tailored to healthcare environments. Attendees will be informed about industry standards and regulatory requirements, such as HIPAA and HITRUST , governing cybersecurity in healthcare. A unique aspect of the seminar is the demonstration of how Security Infusion agents enable the collection and evaluation of data on edge devices, managed seamlessly through a cloud-based platform. Through collaboration and knowledge-sharing opportunities, participants will leave equipped with practical strategies to enhance network security and protect digital health infrastructure effectively.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Knowledge: · Understanding of the unique cybersecurity challenges faced by healthcare organizations. · Knowledge of industry best practices for securing endpoints in healthcare networks. · Familiarity with the evolving threat landscape specific to healthcare, including common cyber threats and attack vectors. · Basics of regulatory requirements and compliance standards governing cybersecurity in healthcare, such as HIPAA and HITRUST. Skills: · Ability to identify and assess cybersecurity risks within healthcare networks. · Proficiency in implementing endpoint security measures tailored to healthcare environments. · Skills in analyzing and responding to cybersecurity incidents in healthcare settings. · Ability to develop and implement cybersecurity policies and procedures in compliance with regulatory requirements. · Proficiency in leveraging security technologies and tools, especially Security Infusion, to enhance network security in healthcare organizations. Competences: · Competence in evaluating and selecting appropriate cybersecurity solutions for healthcare networks. · Competence in collaborating with stakeholders to develop comprehensive cybersecurity strategies for healthcare organizations. · Competence in communicating effectively with technical and non-technical stakeholders about cybersecurity risks and mitigation strategies.

	· Competence in adapting and responding to evolving cybersecurity threats and challenges in the healthcare sector. · Competence in contributing to a culture of cybersecurity awareness and vigilance within healthcare organizations. Overall, the seminar aims to equip attendees with the knowledge, tools, and strategies necessary to strengthen the security posture of healthcare networks and safeguard digital health information against cyber threats.

Main topics and content list A list of main topics and key content	· Endpoint Protection Fundamentals · Cybersecurity Threat Landscape in Healthcare · Best Practices for Endpoint Security · Regulatory Compliance and Standards · Case Studies and Real-World Examples
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	N/A
Training Provider *Name(s) of training providers.*	itml
Contact *Name(s) of the main contact person and their email address.*	Dimitra Siaili (itml), disiaili@itml.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).*	Refer and check online CyberSecPro DCM System for current information. The dates can be changed dynamically.
Duration *Duration of the training.*	2times x 2hours or 1x 4hours
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 or Virtual. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.

Knowledge area(s) *Mapping 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	KA5 – Network and Communication Security KA8 – Cybersecurity Tools and Technologies KA3 – Cybersecurity Risk Management KA10 – Cyber Incident Response
Pre-requisites	Basic IT and security Knowledge Familiarity with basic hardware and software used in network security.
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 Auditor, Cybersecurity Implementer, Cybersecurity Educator.
Tools to be used *A list of tools that will be used for the operation of this training module.*	Security Infusion
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English/Greek

ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes (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. The dates can be changed dynamically.
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.

3.4.2.2 Adapted Syllabus

Table 14: Module 4.2 Syllabus

Main topics	Suggested Content
Introduction to Network Security in Healthcare	Understanding the unique challenges and vulnerabilities faced by healthcare organizations in maintaining secure networks.
Endpoint Protection Fundamentals	Exploring the concept of endpoints in the context of healthcare networks and the significance of protecting these endpoints from cyber-attacks.
Cybersecurity Threat Landscape in Healthcare	Analysis of the evolving threat landscape specific to healthcare, including ransomware, data breaches, and other malicious activities targeting healthcare systems.
Best Practices for Endpoint Security	Discussion of industry best practices and strategies for implementing robust endpoint security measures tailored to healthcare environments.

Regulatory Compliance and Standards	Overview of regulatory requirements and industry standards governing cybersecurity in healthcare, such as HIPAA (Health Insurance Portability and Accountability Act) and HITRUST (Health Information Trust Alliance).
Case Studies and Real-World Examples	Demonstration on how, via the several Security Infusion agents, data can be collected and evaluated on the endpoint. The evaluation on the edge device will be inducted through a cloud-based manager.
Collaboration and Knowledge Sharing	Opportunities for networking and collaboration among participants to exchange insights, challenges, and best practices in the field of healthcare cybersecurity and endpoint protection.

3.4.2.3 Planning for Preparedness

The seminar is supported by practical tools, but the instructions on how to use these tools will be presented also during the course. The course can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, 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 and the labs.

3.4.2.4 Materials and Exercises

The "Cybersecurity and Health" seminar incorporates a diverse range of materials and exercises to provide participants with a comprehensive learning experience. Engaging presentations, curated case studies, and relevant research findings will be utilized to convey theoretical concepts and real-world applications. Practical exercises will immerse participants in simulated scenarios, allowing them to apply cybersecurity principles specifically tailored to the healthcare domain. Hands-on activities will include risk assessment simulations, incident response drills, and the evaluation of cybersecurity tools relevant to health information protection. Interactive discussions and group exercises will foster collaboration and critical thinking, enabling participants to address the unique challenges of securing sensitive health data. The seminar's well-rounded approach to materials and exercises ensures that participants gain both theoretical knowledge and practical skills essential for effective cybersecurity management in the healthcare sector.

3.4.2.5 Verification of Learning Outcomes, and Skills

Successful completion of attendance and at least borderline pass of the mean of the grades of the quizzes done during the seminar.

3.5 Module 5 - Data Protection and Privacy Technologies for Health

3.5.1 CSP005_S_H: Data Protection and Privacy Technologies for healthcare

3.5.1.1 Description of Training Module and Needs

CSP Module Elements	CSP Module Fields Legend	CSP Module Information
Code	**Code** *Code format: CSP005_x where x is the module offering type (see below) and it(_x) will be included in D4.1 and Sector specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)* *The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.* The Generic Model Syllabi will have simple code, as seen in the next column.	CSP005_S_H
Content	**Module title** *The title of the training module*	Data Protection and Privacy Technologies for healthcare
	Alternative title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Privacy Technologies 2. Privacy by Design 3. Data Security and Protection 4. Data Privacy 5. Privacy and Online Rights

	Module 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
	Level *Training level: B (Basic), A (Advanced)*	B
	Module overview *High-level module overview*	This module will provide a seminar for data protection and privacy for healthcare.
	Module description *Indicates the main purpose and description of the module.*	The module provides techniques for data security policies and tools in healthcare.

	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
	Category(s) of capabilities *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)*	Refer and check D4.1

	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: · Data Protection Best Practices: Gain knowledge of effective data security measures, data retention and deletion practices, and data breach response plans. · Emerging Trends: Recognize the impact of new technologies (e.g., AI, big data) on data privacy and ethical considerations. Skills: · Security Policy and Procedure Development: Define and implement data security policies and procedures, including access control and MFA. · Data Anonymization and Sharing Techniques: Apply PETs to anonymize data and enable secure data sharing. Competencies: · Critical Thinking: Analyse complex data privacy scenarios and recommend appropriate solutions.
	Main topics and content list *A list of main topics and key content*	· Data Protection Lifecycle Management · Privacy-Enhancing Technologies (PETs)

	Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English
Management / Logistics	**Training provider** *Name(s) of training providers.*	CNR - Fabio Martinelli <fabio.martinelli@iit.cnr.it>
	Contact *Name(s) of the main contact person and their email address.*	Fabio Martinelli <fabio.martinelli@iit.cnr.it>
	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).*	Refer and check online CyberSecPro DCM System for current information. The dates can be changed dynamically.
	Duration *Duration of the training.*	3- 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.*	Indicates Physical, Virtual, or Both. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.
	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.*	Cybersecurity Implementer
	Tools to be used *A list of tools that will be used for the operation of this training module.*	Personal computer with world wide web access necessary. There will be online web tools demonstration.
	Recommended ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
	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.*	Refer and check online CyberSecPro DCM System for current information. The dates on which the module is offered are subject to change and considered dynamic
	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.

Outcomes	**Evaluation method(s)** ***Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)***	Indicates physical and/or virtual tests, participation and one final exercise.
	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	A questionnaire examines how well students have comprehended basic ideas regarding the concepts.

3.5.1.2 Adapted Syllabus

Table 15: Module 5.1 Description

Main topics	Suggested Content
Data Protection Lifecycle Management	· Data security and technical safeguards: Encryption, access controls, incident response.
Privacy-Enhancing Technologies (PETs)	· Introduction to PETs and their role in data protection.

3.5.1.3 Planning for Preparedness

We expect the participants to bring their own computer and have basic knowledge of computer science and basic coding. It can be conducted either online or in-person.

3.5.1.4 Materials and Exercises

The "Cyber Threat Intelligence for Healthcare" 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.

3.5.1.5 Verification of Learning Outcomes, and Skills

A questionnaire examines how well students have comprehended basic ideas regarding the concepts.

3.5.2 CSP005_W_H: Data Protection and Privacy Technologies for healthcare

3.5.2.1 Description of Training Module and Needs

Table 16: Module 5.2 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP005_S_H**
Module Title *The title of the training module*	**Data Protection and Privacy Technologies for Healthcare**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	"Healthcare Data Privacy: Technologies and Strategies for Protection" "Protecting Health Information: From Compliance to Advanced Security Technologies" "Navigating Data Privacy in Healthcare" "Health Data Guardianship: Technologies for Ensuring Privacy and Compliance" "Securing Patient Data: Technological Solutions and Frameworks" "Data Protection in Healthcare: A Comprehensive Guide to Technologies and Practices"
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 (W)

Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	The "Data Protection and Privacy Technologies for Healthcare" course is designed to address the concerns of privacy and security risks associated with healthcare information and legal obligations. This course equips participants with essential knowledge and practical skills related to safeguarding health data. It's imperative to acknowledge that Data Privacy and Technology constitute a multifaceted and intricate domain. This course is designed with the intent to equip the attendee with the knowledge necessary to enhance their awareness and expertise as an informed participant in privacy-centric communities, business initiatives, and individual data-sharing protocols.
Module description *Indicates the main purpose and description of the module.*	In an increasingly interconnected healthcare landscape, protecting patient data is paramount. This course equips participants with the knowledge and practical skills needed to navigate the complex intersection of technology, privacy regulations, and healthcare data. Understand the types of healthcare data (e.g., electronic health records, medical images, wearable device data) and delve into the legal and ethical considerations surrounding health data privacy. Discuss the impact of data breaches on patient trust and healthcare organisations. Understanding the types of healthcare data through diving into regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Learn about the responsibilities of covered entities, data controllers, and data processors. Study encryption techniques to safeguard data at rest and in transit. Implement access controls, authentication, and audit trails, while understanding threat detection mechanisms and incident response protocol. Explore anonymization and pseudonymization methods and investigate blockchain applications for secure health data sharing. Discuss the trade-offs between data utility and individual privacy. Analyse the impact of telemedicine, IoT devices, and AI on health data privacy.Debate the ethical use of patient data for research, and marketing.Consider the role of transparency, informed consent, and patient empowerment.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Knowledge: Types of healthcare data. Legal and ethical considerations in health data privacy, including HIPAA and GDPR compliance. The impact of data breaches on patient trust and healthcare organisations. Encryption techniques for safeguarding data at rest and in transit. The role and implications of telemedicine, IoT devices, and AI in health data privacy. Skills: Analytical skills to assess the implications of various data protection regulations and identify compliance requirements. Decision-making skills regarding the ethical use of health data, balancing privacy concerns with the benefits of data analysis and sharing. Evaluative skills to critically assess the impact of emerging technologies on health data privacy and security frameworks. Competences: Ability to analyse the balance between data utility and the privacy rights of individuals. Critical evaluation of ethical considerations in the use of patient data for research and marketing purposes. Understanding the importance of transparency, informed consent, and patient empowerment in the management of health data.

Main topics and content list *A list of main topics and key content*	**1. Introduction to Healthcare Data Privacy** **2. Legal Frameworks and Compliance** **3. Security Measures for Health Data Protection** **4. Privacy-Enhancing Technologies** **5. Emerging Trends and Ethical Dilemmas**
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	Evaluating and verifying learning outcomes in understanding healthcare data and its associated legal and ethical considerations involves a multi-faceted approach. Students should demonstrate comprehensive knowledge of various healthcare data types, including electronic health records, medical images, and wearable device data. They must be able to articulate the legal frameworks such as HIPAA and GDPR, understanding the roles and responsibilities of covered entities, data controllers, and data processors. Practical skills in encryption techniques, access controls, authentication, and audit trails should be assessed through hands-on projects or simulations. Moreover, students should showcase their ability to apply threat detection mechanisms and develop incident response protocols. Evaluations should include critical analyses of anonymization and pseudonymization methods.
Training Provider *Name(s) of training providers.*	ZELUS

Contact *Name(s) of the main contact person and their email address.*	Foteini Petropoulou (f.petropoulou@zelus.gr) Thanos Apostolidis (t.apostolidis@zelus.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).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	3-6 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.*	Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.

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	KA6 – Privacy and Data Protection KA1 – Cybersecurity Management KA4 – Cybersecurity Policy, Process, and Compliance KA7 – Cybersecurity Threat 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.*	Cybersecurity Educator
Tools to be used *A list of tools that will be used for the operation of this training module.*	To effectively engage with the course materials and complete all assignments, students are required to have access to specific tools. A personal computer with reliable access to the World Wide Web is essential. This computer should be capable of handling various

	software applications and accessing online resources without significant delays or interruptions.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	Refer and check online CyberSecPro DCM System for current information. There will be changes to the dates depends on the event that the seminar will take place
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.

3.5.2.2 Adapted Syllabus

Table 17: Module 5.2 Syllabus

Main topics	Suggested Content

1.Introduction to Healthcare Data Privacy	• Understand different types of healthcare data (e.g., electronic health records, medical imaging). • Explore the legal and ethical considerations surrounding health data.
2.Legal Frameworks and Compliance	• Learn about key regulations like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). • Understand how these regulations impact healthcare data handling.
3.Security Measures for Health Data Protection	• Dive into encryption, access controls, and authentication methods. • Explore secure data storage and transmission practices. • Learn about threat detection and incident response strategies.
4.Privacy-Enhancing Technologies	• Discover anonymization and pseudonymization techniques. • Explore the role of blockchain in healthcare data security. • Understand differential privacy for preserving individual privacy.
5.Emerging Trends and Ethical Dilemmas	• Investigate telemedicine and remote patient monitoring. • Learn about AI and machine learning applications in healthcare. • Explore privacy-preserving AI models.

3.6 Module 6 - Cyber Threat Intelligence for Health

3.6.1 CSP006_SA_H: Cyber Threat Intelligence for Healthcare

3.6.1.1 Description of Training Module and Needs

The “Cyber Threat Intelligence for Healthcare” training module aims to provide participants with a deep understanding of how to extract and analyse security data effectively to enhance threat intelligence capabilities. Starting with an introduction to the significance of cyber threat intelligence (CTI) in healthcare, attendees will delve into the practical aspects of data extraction from various sources within healthcare systems, including network logs, system logs, and intrusion detection systems.

Objectives:

- Understand the importance of CTI in healthcare.
- Learn data extraction from healthcare systems.
- Develop skills in advanced data analysis.
- Get familiar with openCTI platform and MISP.
- Explore STIX and TAXII standards.
- Apply CTI techniques to healthcare scenarios.
- Develop actionable insights for threat mitigation.
- Address specific healthcare cybersecurity challenges.
- Enhance ability to safeguard healthcare environments.

Table 18: Module 6.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP006_SA_H**
Module Title *The title of the training module*	**Healthcare and Cyber Threat Intelligence**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Protecting Healthcare: Cyber Threat Intelligence in Action 2. Cyber Defence for Healthcare: The Role of Threat Intelligence 3. Securing Health Systems: Integrating Cyber Threat Intelligence 4. Cyber Intelligence Analysis in Healthcare 5. Cyber Threat Modelling in Healthcare
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/S/W

Level *Training level: B (Basic), A (Advanced)*	B (Basic)
Module overview *High-level module overview*	This comprehensive training module dives deep into the essential concepts and principles of threat intelligence and cybersecurity information in the healthcare sector. The module regards the core principles of CTI and its application in healthcare defence, while focuses on practical techniques for gathering security data from various sources within healthcare systems.
Module description *Indicates the main purpose and description of the module.*	This module regards the essential concepts and principles of threat intelligence and cybersecurity information in the healthcare sector. The core principles of CTI are explained and its application in healthcare defence, while focusing on practical techniques for gathering security data from various sources within healthcare systems. Attendees will gain a deep understanding of how to extract and analyse security data effectively to enhance threat intelligence capabilities, with a particular focus on healthcare scenarios. The module also covers the utilization of platforms such as openCTI and MISP, as well as standards like STIX and TAXII. Participants will develop skills in advanced data analysis and learn to develop actionable insights for threat mitigation, addressing specific healthcare cybersecurity challenges to enhance their ability to safeguard healthcare environments. Designed for: Healthcare IT professionals, Information security analysts, Cybersecurity professionals specializing in healthcare, Network administrators and engineers in healthcare organizations, Incident response teams in healthcare institutions, Healthcare system administrators, Compliance officers in healthcare organizations, Security consultants working with healthcare clients, Government agencies responsible for healthcare cybersecurity, Healthcare technology vendors and service providers.

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 (Understanding and Awareness of following)** ● Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks ● Responsible information disclosure procedures ● Cross-domain and border-domain knowledge related to cybersecurity ● Cyber threats and cyber threat actors ● Cybersecurity attack procedures ● Advanced and persistent cyber threats (APT) ● Threat actors Tactics, Techniques and Procedures (TTPs) ● Importance of Cyber Threat Intelligence (CTI) in healthcare. ● Various sources of security data within healthcare systems, including network logs, system logs, and intrusion detection systems. ● Core principles and concepts of threat intelligence and cybersecurity information in the healthcare sector. ● Utilization of platforms such as openCTI and MISP for threat intelligence management. ● Standards such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) used in CTI. ● Specific healthcare cybersecurity challenges and vulnerabilities. **Skill and Competence (applications and practice):** ● Collaborate with other team members and colleagues ● Collect, analyse and correlate cyber threat information originating from multiple sources ● Identify threat actors TTPs and campaigns ● Automate threat intelligence management procedures ● Conduct technical analysis and reporting ● Identify non-cyber events with implications on cyber-related activities ● Model threats, actors and TTPs ● Communicate, coordinate and cooperate with internal and external stakeholders ● Communicate, present and report to relevant stakeholders ● Use and apply CTI platforms and tools ● Extract security data effectively from various sources within healthcare systems. ● Advanced data analysis techniques relevant to threat intelligence in healthcare. ● Familiarity with using the openCTI platform and MISP for threat intelligence management. ● Application of CTI techniques to healthcare scenarios. ● Develop actionable insights for threat mitigation specific to healthcare environments.

	• Address specific healthcare cybersecurity challenges through practical solutions. • Enhance the ability to safeguard healthcare environments through proactive threat intelligence measures.

Main topics and content list *A list of main topics and key content*	• Introduction to Cyber Threat Intelligence (CTI) in Healthcare • Data Extraction from Healthcare Systems • Core Principles of Threat Intelligence in Healthcare • Practical Techniques for Gathering Security Data • Platforms and Standards for Threat Intelligence Management • Overview of STIX (Structured Threat Information eXpression) standard • Understanding TAXII (Trusted Automated eXchange of Indicator Information) standard • Application of CTI Techniques to Healthcare Scenarios • Proactive measures and strategies for enhancing cybersecurity posture in healthcare organizations • Implementation of effective threat intelligence measures to safeguard healthcare environments
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 the training, 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 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.*	PDMFC and SINTEF
Contact *Name(s) of the main contact person and their email address.*	Dr. Stylianos Karagiannis stylianos.karagiannis@pdmfc.com Dr. Nektaria Kaloudi nektaria.kaloudi@sintef.no

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).*	Refer and check online CyberSecPro DCM System for current information
Duration *Duration of the training.*	Refer and check online CyberSecPro DCM System for current information because the duration can change dynamically. In the most of the cases the duration will be 3 – 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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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 KA7** Minor content matches with others including KA2, KA3, KA5, KA8, 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 4: Cyber Threat Intelligence Specialist
Tools to be used *A list of tools that will be used for the operation of this training module.*	MISP, OpenCTI, Wazuh, Suricata, Digital TORC

Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3. (Recommended equivalent to 5 ECTS)
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.*	Refer and check online CyberSecPro DCM System for current information. The dates will change dynamically.
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.

3.6.1.2 Adapted Syllabus

Table 19: Module 6.1 Syllabus

Main topics	Suggested Content

Topic-1: Introduction to Cyber Threat Intelligence (CTI) in Healthcare	• Understanding the significance of CTI in healthcare security. • Overview of cybersecurity threats specific to the healthcare sector. • Importance of proactive threat intelligence in healthcare defence.
Topic-2: Data Extraction Techniques in Healthcare Systems	• Identifying various sources of security data within healthcare systems. • Techniques for extracting data from network logs, system logs, and intrusion detection systems. • Best practices for effective and efficient data extraction processes.
Topic-3: Core Principles of Threat Intelligence in Healthcare	• Understanding fundamental principles of threat intelligence. • Application of threat intelligence methodologies and frameworks in healthcare defence. • Importance of intelligence-driven security approaches in healthcare settings.
Topic-4: Practical Application of Threat Intelligence Tools	• Hands-on experience with utilizing platforms like openCTI and MISP for threat intelligence management. • Effective utilization of threat intelligence platforms to gather, analyse, and disseminate security data. • Integration of threat intelligence tools into existing healthcare security infrastructure.
Topic-5: Standards and Protocols in Threat Intelligence	• Overview of STIX (Structured Threat Information eXpression) standard and its relevance in healthcare. • Understanding TAXII (Trusted Automated eXchange of Indicator Information) standard and its role in information sharing. • Compliance with industry standards and protocols for effective threat intelligence sharing and collaboration.
Topic-6: Application of CTI Techniques to Healthcare Scenarios	• Real-world case studies illustrating the application of CTI techniques in healthcare environments. • Practical exercises focusing on analysing and mitigating threats specific to healthcare systems. • Customizing CTI approaches to address unique challenges and vulnerabilities in healthcare settings.

Topic-7: Developing Actionable Insights for Threat Mitigation	• Techniques for analysing security data to derive actionable insights. • Strategies for prioritizing and responding to identified threats in healthcare environments. • Integration of threat intelligence insights into incident response and mitigation strategies.
Topic-8: Addressing Specific Healthcare Cybersecurity Challenges	• Identification and analysis of common cybersecurity challenges faced by healthcare organizations. • Tailoring threat intelligence strategies to mitigate specific healthcare-related threats, such as ransomware attacks or data breaches. • Best practices for enhancing overall cybersecurity posture in healthcare environments.
Topic-9: Enhancing Security Posture through Threat Intelligence	• Proactive measures for enhancing cybersecurity posture using threat intelligence. • Implementation of threat intelligence-driven security controls and measures in healthcare organizations. • Leveraging threat intelligence to anticipate and prevent potential security incidents.
Topic-10: Practical Implementation and Integration of Threat Intelligence	• Strategies for effectively implementing threat intelligence initiatives within healthcare organizations. • Integration of threat intelligence into existing security operations and incident response processes. • Continuous improvement and optimization of threat intelligence capabilities to adapt to evolving threats and challenges in healthcare cybersecurity.

3.6.1.3 Planning for Preparedness

We expect the participants to bring their own computer and have basic knowledge of computer science and basic coding. It can be conducted either online or in-person.

3.6.1.4 Materials and Exercises

The “Cyber Threat Intelligence for Healthcare” 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 common cybersecurity challenges faced by the healthcare domain.
- Interactive and group discussions to foster collaboration and critical thinking through the TORC-based training that has a gaming format.

3.6.1.5 Verification of Learning Outcomes, and Skills

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.

3.6.2 CSP006_S_H: Network and IoMT Security

3.6.2.1 Description of Training Module

This training module is designed to equip participants with the knowledge and skills necessary to understand and implement security measures in network systems, with a special focus on the Internet of Medical Things (IoMT). The module emphasizes practical and theoretical aspects of network layer security, IoMT communication protocols, and the formulation of effective network security policies, particularly in healthcare environments.

Objectives:

- To understand the intricacies of network layer security and its importance.
- To gain insights into IoMT communication protocols and their security challenges.
- To learn the principles of designing and implementing robust network security policies.

Table 20: Module 6.2 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP006_S_H**
Module Title *The title of the training module*	**Network and IoMT Security**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Internet Infrastructure and Security 2. Networks and Information Security 3. Network and Applications Security 4. Network Applications

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 module delves into the intricacies of network security at various layers and integrates the emerging field of Internet of Medical Things (IoMT). It is designed to provide comprehensive knowledge on securing data transmission, understanding the potential vulnerabilities in network layers, and implementing robust security policies. Special emphasis is placed on the security of communication protocols within the IoMT framework, coupled with detailed analyses of real-world medical case studies.
Module description *Indicates the main purpose and description of the module.*	In this module, students will explore the critical aspects of network security, from the data-link layer to application-layer firewalls and Intrusion Detection Systems (IDS). Building upon this foundation, the course extends into the specialized domain of IoMT, focusing on the security of communication protocols and the analysis of medical case studies. This module not only imparts theoretical knowledge but also provides practical insights into designing and implementing network security policies effectively in healthcare settings.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Understand Layered Network Security: Gain a deep understanding of security measures at different network layers, including data-link, network, and transport layers. Design Network Security Policies: Develop skills to design and implement comprehensive network security policies. Cross-Layer Security Mechanisms: Learn about the integration and application of cross-layer security mechanisms. IoMT Security Protocols: Acquire knowledge about IoMT-specific communication protocols and their security implications. Medical Case Study Analysis: Analyse real-world medical cases to understand the practical challenges and solutions in IoMT security. Incident Identification and Response: Enhance abilities to identify and respond to network security incidents.
Main topics and content list *A list of main topics and key content*	• Data-Link Layer Security: Understanding MAC, LLC, and encryption techniques. • Network Layer Security: IP security (IPsec), routing security. • Transport Layer Security: SSL/TLS protocols, secure data transmission. • Network Security Policy Design: Frameworks and methodologies. • Cross-Layer Security Mechanisms: Integrated security approaches. • Application-Layer Firewalls and IDS: Implementation and management. • IoMT Security Protocols: Overview and security challenges. • Case Studies in IoMT: In-depth analysis of medical cases with a focus on security of IoMT protocols

Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• ***Assignments:*** *To assess understanding of theoretical concepts.* • ***Case Study Analysis:*** *Students will analyse and present solutions for given medical case studies, focusing on IoMT security aspects.* • ***Practical Project:*** *Designing a network security policy or IoMT security protocol for a hypothetical healthcare organization.* • ***Peer Review and Discussion:*** *Encouraging collaborative learning and critical thinking through peer assessments and group discussions.*
Training Provider *Name(s) of training providers.*	UPRC
Contact *Name(s) of the main contact person and their email address.*	Prof. Panagiotis Kotzanikolaou (pkotzani@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).*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
Duration *Duration of the training.*	3 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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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*	*KA5 - Network and Communication Security* *KA10 – Cyber Incident Response*
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). ECSF Profile 6: Cybersecurity Auditor. ECSF Profile 10: Cybersecurity Risk Manager.
Tools to be used *A list of tools that will be used for the operation of this training module.*	snort
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, Greek

ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically

3.6.2.2 Adapted Syllabus

Table 21: Module 6.2 Syllabus

Main topics	Suggested Content
Network Layer Security	Explores security protocols and mechanisms at the network layer, including IPsec and secure routing practices. Focuses on understanding and mitigating vulnerabilities inherent in network communications.
IoMT Communication Protocols	Introduces the specialized protocols used in the Internet of Medical Things (IoMT), emphasizing their security aspects. Covers the adaptation of these protocols in healthcare environments and their role in patient data protection.
Designing Network Security Policies	Provides an overview of the principles and practices involved in formulating effective network security policies. Includes case studies to illustrate the implementation and challenges in diverse scenarios, particularly in healthcare settings.

3.6.2.3 Planning for Preparedness

Training Duration: The training will be conducted over a period of 5 days, with each day dedicated to different aspects of network and IoMT security.

Target Audience: IT professionals, network administrators, cybersecurity specialists, and healthcare IT staff.

Prerequisites: Basic understanding of networking concepts and cybersecurity fundamentals.

Schedule:

- Introduction to Network Security and IoMT - An Overview
- In-depth Analysis of Network Layer Security
- IoMT Communication Protocols and their Security Aspects
- Practical Applications and Case Study Discussions

3.6.2.4 Materials and Exercises

Materials:

- Comprehensive course notes and reference materials.
- Case studies focusing on real-world security challenges in IoMT.

Exercises:

- Interactive Lectures to introduce and explain core concepts and latest trends.
- Sessions on network security tools and protocols, with a focus on IoMT environments.
- Group Discussions facilitated discussions on case studies and current challenges in the field.
- Assessment Quizzes to evaluate understanding and retention of key concepts.

Final Project: Participants will be required to develop a comprehensive network security policy for a hypothetical healthcare organization, incorporating IoMT security considerations.

3.6.2.5 Verification of Learning Outcomes, and Skills

At the end of the seminar, the learners will be expected to fill in a quick evaluation on the subjects introduced and the knowledge provided.

3.7 Module 7 - Cybersecurity in Emerging Technologies for Health

3.7.1 CSP007_S_H: Practical Insights in Anomaly Detection

3.7.1.1 Description of Training Module

This training module aims to provide a comprehensive understanding of the role of machine learning techniques in identifying and mitigating cybersecurity threats. With the increasing complexity of cyber threats, traditional security measures are often insufficient. Anomaly detection using machine learning offers a proactive approach to cybersecurity, enabling the identification of abnormal patterns and behaviours that may indicate potential security breaches. This training module will explore various machine learning algorithms and methodologies employed in anomaly detection, their applications, challenges, and future prospects in enhancing cybersecurity. This training module will delve into the application of machine learning techniques specifically tailored for the healthcare industry, focusing on the identification and prevention of anomalies that could compromise patient confidentiality, data integrity, and the overall functionality of healthcare systems. This training module will empower healthcare professionals, IT specialists, and cybersecurity experts with the knowledge and tools necessary to protect sensitive healthcare information through the application of machine learning-based anomaly detection techniques.

Table 22: Module 7.1 Description

Code	**CSP007_S_H:**
Module Title *The title of the training module*	**Practical Insights in Anomaly Detection**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Practical Insights in Machine Learning Applications AI Strategies for Effective Anomaly Detection in Practice
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/W
Level Training level: B (Basic), A (Advanced)	B
Module overview High-level module overview	This training module aims to provide a comprehensive understanding of the role of machine learning techniques in identifying cybersecurity threats. This training module will explore various machine learning algorithms and methodologies employed in anomaly detection, their applications, challenges, and future prospects in enhancing cybersecurity.
Module description Indicates the main purpose and description of the module.	This training module will delve into the application of machine learning techniques specifically tailored for the healthcare industry, focusing on the identification and prevention of anomalies that could compromise patient confidentiality, data integrity, and the overall functionality of healthcare systems. This training module will empower healthcare professionals, IT specialists, and cybersecurity experts with the knowledge and tools necessary to protect sensitive healthcare information through the application of machine learning-based anomaly detection techniques.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Knowledge: ● Familiarity with the unique challenges and requirements of cybersecurity in the health sector, including the importance of protecting sensitive patient data. ● In-depth knowledge of various anomaly detection techniques ● Understanding of performance metrics for evaluating anomaly detection models Skills: ● Skills in preprocessing health data, handling missing values, and engineering relevant features for anomaly detection. ● Competence in implementing and utilising anomaly detection algorithms using relevant programming languages (e.g., Python) and tools.
Main topics and content list A list of main topics and key content	● Introduction to anomaly detection in healthcare cybersecurity, ● Machine learning algorithms tailored for healthcare anomaly detection, ● Challenges in healthcare anomaly detection, ● Real-world applications in healthcare.
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	● Projects ● Hands-on exercises
Training Provider *Name(s) of training providers.*	UNSPMF
Contact *Name(s) of the main contact person and their email address.*	Danijela Boberic Krsticev, dboberic@uns.ac.rs
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).*	● May 2024 Refer and check online CyberSecPro DCM System for the new Dates.

Duration *Duration of the training.*	4h
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*, Faculty of Sciences, Novi Sad, Serbia Online
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	KA8 – Cybersecurity Tools and Technologies
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 need this module.	Cyber Threat Intelligence Specialist Cybersecurity Researcher Digital Forensics Investigator

Tools to be used *A list of tools that will be used for the operation of this training module.*	Google Colabs, scikit-learn, pyOD, TensorFlow
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	Serbian, English
ECTS If applicable, the number of ECTS.	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.7.1.2 Adapted Syllabus

Table 23: Module 7.1 Syllabus

Main topics	Suggested Content
Introduction to anomaly detection	• Explain the primary goals of anomaly detection • Define types of anomalies (point anomalies, contextual anomalies, collective anomalies…) • Provide an overview of the various techniques employed in anomaly detection, such as statistical methods, machine learning algorithms, pattern recognition…

Machine learning algorithms tailored for healthcare anomaly detection	• Cover unsupervised anomaly detection techniques (Isolation Forests and One-Class SVM, Clustering-based approaches, autoencoders…) • Cover supervised anomaly detection techniques (SVM, Decision trees, Ensemble approaches…) • Cover time series analysis
Real-world applications in healthcare	• Exploration of AI applications in the health sector • Focus on real-world examples and case studies

3.7.1.3 Planning for Preparedness

This training module can be organised as a two-day seminar. On the first day, we'll dive into the basics of anomaly detection, covering topics like an introduction to the concept, types of anomalies, and the fundamental machine learning algorithms used. On the second day, we will investigate practical applications in real-world scenarios and initiate interactive hands-on exercises, fostering immediate participant engagement.

To attend this training module, it is advisable to possess programming skills, particularly in languages commonly employed in machine learning, such as Python.

3.7.1.4 Materials and Exercises

All materials (including lecture notes and slides, reading references, code examples and assignments) for this training module will be available on the project's DCM.

3.7.1.5 Verification of Learning Outcomes, and Skills

To confirm the knowledge and skills gained in this training module, trainees will undertake practical exercises or projects. They will be working on real-world datasets, using anomaly detection techniques and showing off their practical skills.

3.7.2 CSP007_SA_H: Cybersecurity in Emerging Technologies, in particular explainable AI for healthcare

3.7.2.1 Description of Training Module

Table 24: Module 7.2 Description

CSP Module Elements	CSP Module Fields Legend	CSP Module Information

Code	Code *Code format: CSP007_x where x is the module offering type (see below) and it(_x) will be included in D4.1 and Sector specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)* *The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.* The Generic Model Syllabi will have simple code, as seen in the next column.	CSP007_SA_H
Content	Module title *The title of the training module*	Cybersecurity in Emerging Technologies, in particular explainable AI for healthcare
	Alternative title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Security Challenges in Emerging Technologies
	Module 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.*	Refer and check online CyberSecPro DCM System for current information.
	Level *Training level: B (Basic), A (Advanced)*	B

	Module overview *High-level module overview*	The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating AI in the healthcare sector with particular emphasis on explainable and robust approaches.
	Module description *Indicates the main purpose and description of the module.*	This training module explores the unique cybersecurity challenges and best practices associated with emerging technologies, equipping participants with the knowledge and skills needed to master explainable and robust AI approaches for healthcare.
	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

	Category(s) of capabilities *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)*	Refer and check D4.1
	Learning outcomes and targets *A list of knowledge, skills and competencies achieved by the participants as a result of taking a CSP module*	Upon completing the seminar, the trainees are expected to have knowledge of approaches for explainable and robust AI in healthcare sector including: Knowledge: · Understanding of how to build explainable and robust AI solutions for healthcare · Comprehensive knowledge of specific vulnerabilities in AI. Skills: · Stay informed about new threats and trends, adapting security strategies and practices accordingly. Competences: · Critical thinking and problem-solving in complex emerging technology security scenarios.
	Main topics and content list *A list of main topics and key content*	1. Artificial Intelligence (AI) Security
	Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English

Management / Logistics	Training provider *Name(s) of training providers.*	CNR - Fabio Martinelli <fabio.martinelli@iit.cnr.it>
	Contact *Name(s) of the main contact person and their email address.*	CNR - Fabio Martinelli <fabio.martinelli@iit.cnr.it>
	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).*	Refer and check online CyberSecPro DCM System for current information.The dates can change dynamically.
	Duration *Duration of the training.*	3- 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.*	Indicates Physical, Virtual, or Both. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.
	Pre-requisites	Basic AI 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.*	Cybersecurity Researcher

	Tools to be used *A list of tools that will be used for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
	Recommended ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
	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.
Outcomes	Evaluation method(s) *Method for the evaluation of the learners performance (indicates physical and/or virtual tests, participation, exercises, etc.)*	Indicates physical or virtual tests, participation and live exercises

	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	· A questionnaire examines how well students have comprehended basic ideas regarding the concepts.

3.7.2.2 Adapted Syllabus

Table 25: Module 7.2 Syllabus

Main topics	Suggested Content
Artificial Intelligence (AI) Security	· Security risks associated with AI, including bias and adversarial attacks for healthcare. · Methods for securing AI models and training data.

3.7.2.3 Planning for Preparedness

Preparedness of the course involves trainers to gather the student online or with physical appearance or combination of both for the theoretical part. Theory can be taught using the slides that are uploaded to the DCM platform.

3.7.2.4 Materials and Exercises

The training module is supported by the following material:

- Presentation material that will be used during the course and be provided digitally to the learners.
- Labs.
- This module requires from students to have a laptop, an Internet connection, if possible a fast one with low latency. This way the students will be able to download the material and do the laboratory exercises in case they want to attend remotely.

3.7.2.5 Verification of Learning Outcomes, and Skills

The verification of learning outcomes and skills will be mostly determined during the laboratory exercises. Students will be assessed in terms of their capability to successfully follow the laboratory exercises and if they have attended all theoretical lessons and all lab exercises.

3.8 Module 8 - Critical Infrastructure Security for Health

3.8.1 CSP008_C_H: Advanced Infrastructure Security

3.8.1.1 Description of Training Module and Needs

This comprehensive training module on Critical Infrastructure Security for Health is tailored to equip participants with advanced cybersecurity strategies, ensuring the protection of healthcare systems and patient data. The module covers key topics such as asset identification, network scanning, vulnerability detection, vulnerability mitigation, and patch management to fortify the security posture of healthcare infrastructure.

3.8.1.2 Adapted Syllabus

Table 26: Module 8.1 Description

Code	**CSP008_C_H:**
Module Title *The title of the training module*	**Advanced Infrastructure Security**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Advanced Critical Infrastructure Security for Health
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/W
Level Training level: B (Basic), A (Advanced)	A

Module overview High-level module overview	This training module focuses on securing healthcare networks through a three-tiered approach. Firstly, it covers Foundational Security Measures, including Asset Identification for discovering all devices, Assessment of Security Posture to evaluate the current framework, Implementation of Strong Access Controls for robust authentication, and Segmentation of Devices in the Network to contain potential threats. Secondly, the module delves into Advanced Threat Detection Techniques, involving Network Scanning using advanced methods for comprehensive discovery, Detecting Threats through the utilization of state of the art tools, and the development of Vulnerability and Risk Management Strategies for identifying and managing associated risks. Lastly, the training emphasizes Continuous Optimization of Security Strategy, with a focus on ongoing Vulnerability Detection using tools and methodologies, developing strategies for Vulnerability Mitigation, and establishing effective Patch Management procedures for timely application and system updates. This comprehensive approach aims to empower participants with the knowledge and skills necessary to enhance the security posture of healthcare networks.
Module description Indicates the main purpose and description of the module.	This course is designed to empower healthcare professionals, IT specialists, and cybersecurity experts with advanced knowledge and practical skills in securing critical healthcare infrastructure. By focusing on foundational security measures, advanced threat detection techniques, and continuous optimization strategies, participants will gain the expertise needed to safeguard patient data, ensure data integrity, and fortify the overall resilience of healthcare systems against evolving cyber threats. This course goes beyond basic cybersecurity concepts, providing a deep dive into the intricacies of securing healthcare networks. Participants will explore foundational security measures, including comprehensive asset identification, security posture assessment, strong access controls, and secure network segmentation to contain potential threats. The course then advances into cutting-edge techniques for threat detection, covering network scanning using advanced methodologies and leveraging machine learning algorithms for anomaly detection. Participants will also delve into developing effective strategies for vulnerability and risk management, identifying potential weaknesses and mitigating associated risks to enhance overall security. Continuous optimization of security strategy is a key focus, involving ongoing vulnerability detection through advanced tools

	and methodologies, the development of robust vulnerability mitigation strategies and the establishment of effective patch management procedures for timely updates.
Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Participants in the Advanced Healthcare Cybersecurity course will gain a comprehensive understanding of foundational security measures, including asset identification, security posture assessment, strong access controls, and secure network segmentation. They will develop practical skills in implementing these measures, ensuring robust cybersecurity in healthcare networks. Advanced threat detection techniques, such as employing machine learning algorithms and network scanning, will be mastered to proactively identify anomalies and potential threats. Participants will also acquire skills in developing and implementing effective strategies for vulnerability and risk management, addressing potential weaknesses in healthcare systems. The course will empower participants to continuously optimize security strategies, utilizing advanced tools for ongoing vulnerability detection, and establishing robust procedures for timely patch management and system updates.
Main topics and content list A list of main topics and key content	Foundational Security Measures for Healthcare Networks ● Asset Identification ● Techniques for comprehensive device discovery. ● Security Posture Assessment. ● Evaluation methodologies for existing security frameworks. ● Strong Access Controls Implementation. ● Robust authentication and authorization mechanisms. ● Network Segmentation for Threat Containment. ● Strategies to establish secure network segments. Advanced Threat Detection Techniques for Health Care Networks ● Advanced Network Scanning Methodologies. ● In-depth exploration of advanced scanning techniques. ● Machine Learning for Anomaly Detection. ● Application of machine learning algorithms in healthcare contexts. ● Vulnerability and Risk Management Strategies. ● Effective identification and management of vulnerabilities and associated risks. Continuous Optimization of Security Strategy in Health Care Networks ● Ongoing Vulnerability Detection:

	• Tools and methodologies for continuous monitoring. • Vulnerability Mitigation Strategies: • Formulation and implementation of proactive mitigation plans. • Effective Patch Management and System Updates: • Procedures to ensure timely application and updates for healthcare systems.
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	• Projects • Workshop Hands-on exercises
Training Provider *Name(s) of training providers.*	UNINOVA + PDMFC
Contact *Name(s) of the main contact person and their email address.*	Luis Miguel Campos, Luis Landeiro Ribeiro (luis.ribeiro@pdmfc.com), 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).*	• Second Semester of 2024
Duration *Duration of the training.*	8 - 10 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.*	*Physical - Lisbon / Portugal*

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	KA5 – Network and Communication Security KA7 – Cybersecurity Threat Management KA8 – Cybersecurity Tools and Technologies
Pre-requisites	Basic programming skills. Understanding of basic cybersecurity concepts, including encryption, authentication, and access controls. Proficiency in networking concepts such as IP addressing, routing, and subnetting. Basic IT skills, including familiarity with operating systems, software installation, and troubleshooting.
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 Researcher Digital Forensics Investigator
Tools to be used *A list of tools that will be used for the operation of this training module.*	Online cybersecurity tool. This tool can be a portal to the penetration testing. It will be installed during the seminar

Language Indicates the spoken language and the language for the material and the assessment/evaluation.	Portuguese, English
ECTS If applicable, the number of ECTS.	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.	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.

3.8.1.3 Planning for Preparedness

It's advisable the participants brush up on their network and programming skills.

The course requires a set of exercises that will be hands-on worked by the students. This requires a massive investment of time and effort to conclude beforehand.

It’s advisable for the lecturer to get familiar with the deep subjects that will be presented, this course is not for the faint of heart. The motto will be work hard, or success is dim. Scripts to automate deployment of workshop exercises need to be tested frequently to ensure they work flawlessly and updated to match any dependencies that might have changed since the course was prepared.

Hardware for setting up the environments needs to be tested for scale and ensured to have enough resources for every student to work on at the same time. Considering that if there are n exercises and m students, that they may work at radically different speeds and go through exercises blazing fast, or snaily slow. This means all courses should be available at all times (n x m resources required).

3.8.1.4 Materials and Exercises

Student Hardware:

For the students a fairly recent laptop with wifi and ethernet (recommended) capabilities is a must.

They will need to be able to run the tools locally, as installing the tools and configuring them to perform the required tasks is valuable knowledge in itself. Also a security practitioner is only as good as the tools they can command. We strongly believe that empowering individuals starts with augmenting the environment they have easy access to. This foments practising for fun, which is a key part in having success in this area.

Student Software:

Linux OS is recommended for testing tools, either running on bare metal (recommended) or pass-through on a VM.

Permission rights to install tools on-demand.

Lecturer Hardware:

- For physical locations only:
  - Room with projecting capabilities
- For all:
  - Server with ability to run VMs on demand
  - Laptop or Desktop connected to the internal networks and with internet access

Lecturer Software:

- VM virtualization software, Vmware / KVM / Proxmox or other that you are familiar with.
- Scripts to launch, reset and destroy VMs / course exercises

3.8.1.5 Verification of Learning Outcomes, and Skills

- Participants will acquire a solid understanding of vulnerability management, including identification, detection and mitigation strategy fundamentals.
- Practical skills in applying vulnerability detection techniques to real-world healthcare scenarios will be evaluated in practical workshops.
- Engagement in hands-on exercises will enhance participants' ability to proactively address cybersecurity challenges in healthcare networks.

3.8.2 CSP008_SA_H: Healthcare sector cyber security

3.8.2.1 Description of Training Module and Needs

This module serves as a crucial educational resource designed to address the specific needs of learners within the healthcare sector. Its primary aim is to empower individuals with the knowledge and skills required to comprehensively comprehend and effectively manage vulnerabilities, threats, and risks, all within the context of healthcare systems.

One of the paramount objectives of this module is to instil a systemic approach to risk management, equipping learners with the ability to critically evaluate and appraise the protective mechanisms implemented to bolster the security and resilience of the healthcare sector. By focusing on the unique challenges and intricacies of healthcare, this module caters to the specific demands and requirements of the industry.

Upon successful completion of this module, learners will emerge with a profound capability to identify, assess, and analyse the multitude of threats and risks that may potentially affect the healthcare ecosystem. Furthermore, they will acquire the skills needed to devise and implement effective mitigation

strategies. Beyond this, the module seeks to foster a cybersecurity culture within the broader healthcare landscape, emphasizing the importance of vigilance and proactive measures to safeguard sensitive healthcare data and critical infrastructure.

Table 27: Module 8.2 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP008_SA_H**
Module Title *The title of the training module*	**Healthcare sector cyber security**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Detect vulnerabilities in Healthcare
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/W/S
Level *Training level: B (Basic), A (Advanced)*	B
Module overview *High-level module overview*	The module aims to provide learners with an overview of the cyber security and threats affecting the healthcare sector. It facilitates understanding connected healthcare assets, underlying vulnerabilities, and course of actions for a secure healthcare system.

Module description *Indicates the main purpose and description of the module.*	The module provides the learner with the ability to understand and manage vulnerabilities, threats, and risks with particular focus on healthcare system. It offers systemic risk management practice and supports critically evaluate the protection mechanisms used to enhance the security and resilience of the healthcare sector. Upon completion of the module, the learners will be able to identify and analyse the threats and risks and their mitigation and develop a cybersecurity culture within overall healthcare ecosystem
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 knowledge and understanding of threat and risks in healthcare system. ● Identify and critically analyse the healthcare assets and their dependencies. **Skill and Competence:** ● Critically appraise the cyber security risk and control within overall healthcare ecosystem ● Demonstrate an in-depth understanding of an effective security practice and document accordingly in a professional manner
Main topics and content list *A list of main topics and key content*	● Cyber security in healthcare: concepts, technology, services, challenges ● Vulnerabilities and threats in healthcare ● Cyber-attack path discovery model ● Risk assessment and management in healthcare ● Secure patient data ● Policy and best practice ● Case study in healthcare
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	● *Coursework portfolio (80%) Summative assessment*: Learner needs to produce a 3000-word portfolio at the end of the module by performing a list of tasks to demonstrate the learning outcomes are achieved. ● *Presentation (20%) Summative assessment:* learners need to present the outcomes of the portfolio to demonstrate their understanding.

Training Provider *Name(s) of training providers.*	UPRC, SLC
Contact *Name(s) of the main contact person and their email address.*	Prof. Dr. Shareeful Islam, shareeful@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).*	Refer and check online CyberSecPro DCM System for current. The dates on which the module is offered are subject to change and considered dynamic
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 note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.)

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* *(7) Cybersecurity Threat 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.*	Cybersecurity Implementer
Tools to be used. *A list of tools that will be used for the operation of this training module.*	Open vas and other tools related to vulnerability scanning.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	Spoken: English Material: English Assessment: English

ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	Refer and check online CyberSecPro DCM System for current information. The dates on which the module is offered are subject to change and considered dynamic
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.

3.8.2.2 Adapted Syllabus

Table 28: Module 8.2 Syllabus

Main topics	Suggested Content
Cyber security in healthcare: concepts, technology, services, challenges	Modern healthcare ecosystem and challenges Healthcare information infrastructure and services Connected medical devices and their dependencies
Vulnerabilities and threats in healthcare Cyber-attack path discovery model	Threats and vulnerabilities targeted healthcare sector and medical devices Malware threats and taxonomy, Common Vulnerability Exposure (CVE), CVSS 3.1/CVSS4.0, vulnerability exploitation Cyber-attack path discovery for dependent assets within healthcare information infrastructure
Risk assessment and management in healthcare	Risk assessment and management method and standard (ISO31000) Healthcare system specific risks and mitigation strategy Critical security controls and taxonomy

Secure patient data Policy and best practice	Patient healthcare data types and sensitivity Data security and privacy Policy and best practice guideline for overall security awareness
Case study in healthcare	Relevant case study in healthcare sector

3.8.2.3 Planning for Preparedness

Knowledge and Understanding: Demonstrate knowledge and understanding of threat and risks in the healthcare system.

Skills and Competence: Critically appraise the cybersecurity risk and control within the overall healthcare ecosystem.

3.8.2.4 Materials and Exercises

Knowledge and Understanding: Identify and critically analyse healthcare assets and their dependencies.

Skills and Competence: Demonstrate an in-depth understanding of effective security practices and document them professionally.

3.8.2.5 Verification of Learning Outcomes, and Skills

Knowledge and Understanding:

- Cybersecurity in healthcare: concepts, technology, services, challenges.
- Vulnerabilities and threats in healthcare.
- Cyber-attack path discovery model.
- Risk assessment and management in healthcare.
- Secure patient data.
- Policy and best practices.
- Case study in healthcare.

Skills and Competence:

- Coursework portfolio (80%): Learner needs to produce a 3000-word portfolio at the end of the module by performing a list of tasks to demonstrate the learning outcomes are achieved.
- Presentation (20%): Summative assessment: learners need to present the outcomes of the portfolio to demonstrate their understanding.

3.8.3 CSP008_S_H: Cascading Effects in Complex Health Networks

3.8.3.1 Description of Training Module and Needs

Table 29: Module 8.3 Description

Code	CSP008_S_H

Code format: CSP001_x where x is the training of offering type (see below)	
Module Title *The title of the training module*	**Cascading Effects in Complex Health Networks**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Securing Essential Services and Infrastructure 2. Critical Infrastructure Protection: Security Strategies 3. Infrastructure Resilience and Security 4. Defending Critical Infrastructure from Threats 5. Infrastructure Security and Resilience Measures 6. Ensuring Resilient Critical Infrastructure 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.*	S (Seminar)
Level *Training level: B (Basic), A (Advanced)*	A (Advanced)
Module overview *High-level module overview*	This seminar focuses on providing critical infrastructure operators from the health sector (hospital operators, security officers, medical device managers, etc.) with advanced knowledge on the complex consequences of cyber threats on medical systems. The seminar will cover the identification of interdependencies and the assessment of cascading effects within and among them.
Module description *Indicates the main purpose and description of the module.*	Initially, the importance and characteristics of Critical Infrastructures (CIs) will be discussed, based on the EU's NIS2 and CER directives. Then, it will focus on the different types of dependencies among the ICT and medical devices within a CI from the health sector and among other critical health organisations (pharmaceutical production, medical waste management, sterilisation, etc.). Further, the seminar will elaborate on the definition of cascading effects and their impact with in the (internal) network of medical systems and on other (external) critical health

	infrastructures. Finally, the seminar will describe an approach to model the interdependencies and simulate cascading effects; the participants will use the respective simulation tool to perform analyses on their own.
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 critical medical systems against the impacts of cascading effects and to estimate the impacts of these effects on other medical systems and health infrastructures.
Main topics and content list *A list of main topics and key content*	• Introduction to Critical Infrastructure • Threat Landscape in the Maritime Sector • Critical Infrastructure Interdependence • Cascading Effects and their Impacts • Simulating and Analysing Cascading Effects
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)
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).*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
Duration *Duration of the training.*	2 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 Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.
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 + 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) Medical Technicians / Medical Device Managers

Tools to be used *A list of tools that will be used for the operation of this training module.*	CASSANDRA (Cascading Effects and Risk Assessment Tool)
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, German
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.8.3.2 Adapted Syllabus

Table 30: Module 8.3 Syllabus

Main topics	Suggested Content
Interdependencies among Critical Health Systems Infrastructures	Participants will learn about the strong relation among critical medical systems within health infrastructures and its implications for potential cyber threats. This part will go into detail on the different types of dependencies among critical medical technology systems and also among other critical infrastructures, how these dependencies can be identified and

	characterized. For structural analysis and visualisation, a graph representation (the interdependency graph) will be discussed.
Simulation and Analysis of Cascading Effects	Based on the discussions on interdependencies, this part will cover the implications on threats and their consequences. The concept of cascading effects will be introduced and highlighted by various examples from the literature and from practice. An abstract model for describing the effects of a threat on an individual system with a critical health infrastructure will be presented. Taking the interdependency graph into account, a stochastic model for the simulation of the cascading effects across the internal network of critical medical systems as well as the external network with other medical systems and health infrastructures will be presented and discussed.

3.8.3.3 Planning for Preparedness

Preparedness of the module involves trainers to gather the student online or with physical appearance or combination of both for the theoretical part. Theory can be taught using the slides that are uploaded to the DCM platform.

3.8.3.4 Materials and Exercises

The training module is supported by the following material:

- Presentation material that will be used during the course and be provided digitally to the learners.
- Labs.
- This module requires from students to have a laptop, an Internet connection, if possible, a fast one with low latency. This way the students will be able to download the material and do the laboratory exercises in case they want to attend remotely.

3.8.3.5 Verification of Learning Outcomes, and Skills

Students will be assessed in terms of their capability to successfully follow the exercises and if they have attended all theoretical lessons. During the training, learners will be observed if they can follow the instructions given by the trainers without having difficulty to do so.

3.9 Module 9 - Software Security for Health

3.9.1 CSP009_W_H: Securing Healthcare Web Applications

3.9.1.1 Description of Training Module

This workshop covers a range of known attacks against web applications as selected by OWASP. The trainees are offered a unique perspective by viewing the bugs in the code that cause vulnerabilities and the techniques attackers use to take advantage of them.

Table 31: Module 9.1 Description

Code	**CSP009_W_H:**
Module Title *The title of the training module*	**Securing Healthcare Web Applications**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Healthcare 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 such as doctor-patient portals.

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 healthcare 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.	Available in the DCM
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.9.1.2 Adapted Syllabus

Table 32: Module 9.1 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.

3.10.1.3 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.

3.10.1.4 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.

3.10.1.5 Verification of Learning Outcomes, and Skills

To verify the acquisition of knowledge and skills, the shared vulnerable VM will contain numerous bugs representative of each OWASP Top Ten category. Teams will be tasked with selecting and exploiting a bug from each category, then documenting their process and findings in a short, screenshot-based report at the end of the workshop. This practical exercise not only assesses participants' understanding and ability to apply their knowledge but also encourages teamwork and critical thinking, providing a comprehensive assessment of their learning outcomes.

3.9.2 CSP009_SA_H: Secure Healthcare Software Development

3.9.2.1 Description of Training Module

The "Secure Healthcare Software Development" training module prioritizes privacy and encryption strategies to fortify healthcare applications against evolving cyber threats. With a specific focus on safeguarding patient data, this module equips healthcare professionals, IT specialists, and software developers with advanced knowledge and skills in privacy protection, anonymization techniques, and robust encryption practices for both data at rest and in transit.

3.9.2.2 Adapted Syllabus

Table 33: Module 9.2 Description

Code	**CSP008_SA_H:**
Module Title *The title of the training module*	**Secure Healthcare Software Development**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Secure Healthcare SDLC
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/S
Level Training level: B (Basic), A (Advanced)	A
Module overview High-level module overview	This comprehensive training module on "Secure Healthcare Software Development" emphasizes advanced strategies for safeguarding patient data in healthcare applications. The outline covers the intricate landscape of privacy challenges, regulatory frameworks, and the impact of privacy breaches on patient trust and legal compliance.
Module description Indicates the main purpose and description of the module.	Participants will gain practical insights into anonymization techniques, focusing on effective de-identification strategies while balancing data utility. The module delves into encryption protocols, addressing the secure storage of data at rest, encrypted transmission of data in transit, and comprehensive encryption strategies.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	By integrating privacy considerations into the software development lifecycle, participants will be equipped with the knowledge and skills necessary to contribute to the development of healthcare applications that prioritize patient privacy and comply with stringent data protection regulations.
Main topics and content list A list of main topics and key content	Understanding Privacy Challenges in Healthcare Software ● Overview of privacy concerns in healthcare applications ● Regulatory frameworks and standards for healthcare data privacy ● Impact of privacy breaches on patient trust and legal compliance Anonymization Techniques for Patient Data ● Principles of data anonymization in healthcare ● Implementing effective de-identification strategies ● Balancing data utility with privacy preservation Encryption Protocols for Data at Rest ● Importance of encrypting data stored in healthcare databases ● Secure key management practices ● Implementation of encryption algorithms for data at rest Encryption for Data in Transit ● Securing communication channels within healthcare systems ● TLS/SSL protocols for encrypted data transmission ● Ensuring end-to-end encryption in healthcare applications ● Secure Authentication and Authorization Practices ● Role of authentication in protecting patient privacy ● Authorization controls to restrict access to sensitive healthcare data ● Multi-factor authentication for enhanced security Comprehensive Data Encryption Strategies ● Hybrid encryption models for comprehensive protection ● Secure implementation of cryptographic libraries ● Regular audits and updates to encryption protocols Privacy by Design in Healthcare Software Development

	• Integrating privacy considerations into the software development lifecycle • Conducting privacy impact assessments • Collaborating with stakeholders to ensure privacy-centric design
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	• Projects • Multiple Choice Tests
Training Provider *Name(s) of training providers.*	UNINOVA + PDMFC
Contact *Name(s) of the main contact person and their email address.*	Luis Miguel Campos, Luis Landeiro Ribeiro (luis.ribeiro@pdmfc.com), 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).*	Second Semester of 2024
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 - Lisbon / Portugal*

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	KA4 – Cybersecurity Policy, Process, and Compliance KA6 – Privacy and Data Protection KA8 – Cybersecurity Tools and Technologies
Pre-requisites	Basic understanding of software development processes. Familiarity with healthcare industry operations and data handling.
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.*	Visual Studio Code, Chimera, Golang, Ruby, TOML, OpenSSL
Language Indicates the spoken language and the language for the material and the assessment/evaluation.	Portuguese, English

ECTS If applicable, the number of ECTS.	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

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.

3.9.2.5 Verification of Learning Outcomes, and Skills

Refer and check online CyberSecPro DCM System for current information.

3.10 Module 10 - Penetration Testing for Health

3.10.1 CSP0010_W_H: Penetration Testing for Healthcare IT Infrastructures

3.10.1.1 Description of Training Module and Needs

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 against an active directory environment simulating background healthcare it infrastructure such as workstations and servers.

Table 34: Module 10.2 Description

Code	**CSP010_W_H:**

Module Title *The title of the training module*	**Penetration Testing for Healthcare IT Infrastructures**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	Penetration Testing for Healthcare 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 healthcare infrastructure 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 Healthcare IT infrastructure.
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.	Available in the DCM
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.10.2.2 Adapted Syllabus

Table 35: Module 10.2 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.

3.10.1.5 Verification of Learning Outcomes, and Skills

The effectiveness of the workshop will be assessed through practical exercises within the lab environments. Participants will be tasked with identifying and exploiting vulnerabilities in simulated AD environments, using the techniques discussed. These exercises aim to reinforce learning by applying theory to practice, ensuring that participants gain hands-on experience in penetration testing AD environments.

By the end of the workshop, participants will have a deeper understanding of how to identify, exploit, and mitigate vulnerabilities in Active Directory environments, significantly enhancing their penetration testing skills and cybersecurity expertise.

3.10.2 CSP0010_S_H: Penetration Testing

3.10.2.1 Description of Training Module and Needs

This module is designed for IT professionals, security professionals, and business leaders who need to learn knowledge and skills to perform ethical hacking (exposing organisations' weaknesses), gather intelligence, test and improve security and offer protection against privilege escalation to prevent intrusions. The module aims to provide the trainee with a comprehensive understanding of penetrating testing within the cybersecurity landscape as it affects individuals and public and private organisations.

CSP Module Elements	CSP Module Fields Legend	CSP Module Information
Code	**Code** *Code format: CSP010_x where x is the module offering type (see below) and it(_x) will be included in D4.1 and Sector specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)* *The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.* *The Generic Model Syllabi will have simple code, as seen in the next column.*	**CSP010_S_H**
Content	**Module title** *The title of the training module*	**Penetration Testing**
	Alternative title(s) *Used alternative titles for the same module by many institutes and training providers*	1. Ethical Hacking 2. Security Assessment Testing 3. Vulnerability Testing 4. Red Teaming 5. Security Audit and Testing 6. White-Hat Hacking" 7. Cybersecurity Penetration Testing 8. Network Exploitation Testing 9. Security Validation Testing 10. Attack Simulation and Testing

	Module 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.*	Refer and check online CyberSecPro DCM System for current information.
	Level *Training level: B (Basic), A (Advanced)*	A
	Module overview *High-level module overview*	This advanced course delves deep into the technical and strategic aspects of penetration testing.
	Module description *Indicates the main purpose and description of the module.*	The objective this module is to provide trainees with knowledge and skills for penetration testing to uncover any form of vulnerability ranging from small implementation bugs to major system design flaws resulting from coding errors, system configuration faults, design flaws or other operational deployment weaknesses. This course complements and expands upon foundational cybersecurity knowledge, preparing students for real-world security assessments and ethical hacking scenarios.

	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*	KA9
	Category(s) of capabilities *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)*	Refer and check D4.1

	Learning outcomes and targets *A list of knowledge, skills and competencies achieved by the participants as a result of taking a CSP module*	**Knowledge:** · In-depth understanding of penetration testing methodologies and frameworks. · Comprehensive knowledge of legal and ethical considerations for penetration testing engagements. · Advanced understanding of network protocols, vulnerabilities, and exploitation techniques. · Solid grasp of operating system vulnerabilities, web application security testing methodologies, and mobile application security principles. · Awareness of cloud security concepts and penetration testing techniques. · Knowledge of advanced penetration testing tools and scripting for automation. · Understanding of social engineering techniques and their application in penetration testing. · Knowledge of professional ethics and legal requirements for penetration testers. Skills: · Conduct thorough information gathering and reconnaissance using advanced tools and techniques. · Perform advanced network scanning and vulnerability assessments to identify and exploit vulnerabilities. · Penetrate and exploit operating systems, web applications, and mobile applications using advanced tools and techniques. · Develop and execute post-exploitation strategies for maintaining access and escalating privileges.

		· Write comprehensive and informative penetration testing reports, documenting findings and recommendations. · Effectively communicate test results and vulnerabilities to both technical and non-technical audiences. · Utilize scripting for automation and custom exploit development. · Apply ethical hacking techniques and social engineering in controlled, simulated environments. **Competencies:** · Critical thinking and problem-solving in complex penetration testing scenarios. · Ability to analyse information, identify vulnerabilities, and develop effective exploitation strategies. · Strong analytical and technical skills to utilize advanced penetration testing tools and methodologies. · Effective communication and collaboration skills to work with clients and stakeholders. · Adaptability and continuous learning to stay updated with evolving threats and technologies. · Ability to prioritize risks, make ethical decisions, and act responsibly in penetration testing engagements. · Leadership potential in planning, conducting, and reporting on penetration testing projects.

	Main topics and content list *A list of main topics and key content*	1. Introduction to Penetration Testing 2. Advanced Information Gathering and Reconnaissance 3. Network Penetration Testing 4. System and Application Penetration Testing 5. Essentials of Encryption 6. Advanced Penetration Testing Tools and Techniques 7. Development and Delivery of Reports 8. Ethics and Professionalism in Penetration Testing
	Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English, French, German (2026)
Management / Logistics	**Training provider** *Name(s) of training providers.*	LAU, TalTech, trustilio
	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).*	Refer and check online CyberSecPro DCM System for current information. The dates change dynamically
	Duration *Duration of the training.*	3hours

	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.*	Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.
	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 need this module.*	Penetration Tester (PENT) Vulnerability Assessment and Penetration Testing Specialist (VAPTS) Cybersecurity Incident Responder (CSIR)
	Tools to be used *A list of tools that will be used for the operation of this training module.*	• Kali **Linux**: A specialized operating system for penetration testing and security auditing. • Nmap: A powerful network scanning tool used for network discovery and security auditing. • Wireshark: A network protocol analyzer that captures and interactively analyzes network traffic. • **John the Ripper**: A fast password cracker for testing password strength. • **OWASP ZAP (Zed Attack Proxy)**: A tool for finding vulnerabilities in web applications. •**Nikto**: A web server scanner that performs comprehensive tests against web servers. • **Hydra**: A parallelized login cracker supporting numerous protocols to test password strength.
	Recommended ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3..

	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.*	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.
Outcomes	**Evaluation method(s)** *Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)*	Live exercises and incident demonstrations through Virtual machines.
	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• **Enhanced Technical Skills**: Students will gain advanced proficiency in using a variety of cybersecurity tools and technologies such as Kali Linux, Nmap, Metasploit Framework, Wireshark, Burp Suite, John the Ripper, OWASP ZAP, Nikto, Hydra, and Splunk. • **Comprehensive Understanding of Cyber Threats**: Learners will develop a deep understanding of various cyber threats, including malware, phishing, and network attacks, and learn how to effectively identify and mitigate these risks. • **Practical Penetration Testing Abilities**: Students will acquire hands-on experience in conducting penetration tests, identifying

		vulnerabilities, and exploiting security weaknesses in various systems and applications. • **Vulnerability Assessment Expertise**: Participants will become skilled in performing thorough vulnerability assessments, analyzing system security, and providing detailed reports and recommendations for improvement.

3.10.2.2 Adapted Syllabus

Table 36: Module 10.2 Syllabus

Main topics	Suggested Content
Introduction to Penetration Testing	· Penetration testing concepts, methodologies, and frameworks: Planning and preparation for penetration testing, penetration testing procedures, penetration testing standards, methodologies and frameworks, penetration testing tools. · Legal and ethical considerations for penetration testing engagements. · Planning and scoping penetration testing engagements. · Client communication and documentation best practices.
Advanced Information Gathering and Reconnaissance	· Advanced OSINT techniques (social media, public records, data breaches). · Network reconnaissance and foot printing strategies. · Utilizing advanced information gathering tools (i.e., Maltego, SpiderFoot). · DNS, Web reconnaissance

Network Penetration Testing	· Advanced network scanning and vulnerability assessment methodologies. · Exploiting network vulnerabilities with advanced tools (Metasploit, Nmap NSE scripts). · Wireless network penetration testing (802.11 attacks, wireless intrusion detection/prevention systems). · Post-exploitation techniques for maintaining access and privilege escalation. · TCP, UDP connections, scanning
System and Application Penetration Testing	· Operating system penetration testing (Windows, Linux) with advanced tools (i.e., Mimikatz, PowerSploit). · Web application security testing (OWASP Top 10, SQL injection, XSS, CSRF). · Mobile application security testing (static and dynamic analysis tools). · Cloud security testing concepts and techniques. · Databases, SQL, SQL injection, Web authentication and session management, Browser proxies and non-rendered content, cross-site scripting, HTTP, JavaScript, and command injection
Essentials of Encryption	· Wireless networks and encryption, lock picking, master keys, and oracle hacks, cryptography weaknesses, SSL and TLS encryption
Advanced Penetration Testing Tools and Techniques	· Scripting for automation and custom exploitation. · Social engineering techniques and tools for physical and virtual environments. · Advanced privilege escalation techniques and bypassing security controls. · Cloud penetration testing tools and platforms.
Development of reports	· Vulnerability assessment results report, penetration testing report

Ethics and Professionalism in Penetration Testing	· Conducting penetration testing engagements on simulated real-world scenarios. · Applying learned techniques to exploit vulnerabilities in virtualized environments. · Writing comprehensive penetration testing reports based on lab exercises. · Critically analysing real-world penetration testing case studies.

3.10.2.3 Planning for Preparedness

This module is designed for IT, security professionals, and anyone who needs to understand penetration testing.

Target Audience:

· IT security professionals (security analysts, engineers, auditors).

· Network administrators seeking to bolster security posture.

· Aspiring penetration testers wanting to enter the cybersecurity field.

3.10.2.4 Materials and Exercises

Refer and check online CyberSecPro DCM System for current information.

3.10.2.5 Verification of Learning Outcomes, and Skills

Gain a solid understanding of penetration testing principles and methodologies.

Plan, design, implement and execute penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures within an organisation.

· Develop skills to discover, exploit, and document vulnerabilities in networks, systems, and applications.

· Uncover vulnerabilities that affect the confidentiality, integrity and availability of ICT products.

· Learn to leverage various tools and techniques used by penetration testers (e.g., network scanning, vulnerability scanning, password cracking, social engineering).

· Practice navigating penetration testing frameworks and methodologies.

3.11 Module 11 - Cyber Ranges and Operations for Health

3.11.1 CSP0011_S_H: Cyber Ranges and Operations in healthcare domain

3.11.1.1 Description of Training Module

"Cyber Ranges and Operations in the Health Domain" seminar provides a comprehensive exploration of cybersecurity strategies specifically tailored for the healthcare sector. Attendees will gain practical insights through detailed demonstrations using the Security Infusion tool. The seminar covers topics such as real-time notifications for malicious activities, generating actionable reports on system status, and continuous monitoring of critical infrastructure via a cloud-based security information management system. Participants will leave equipped with the knowledge and skills to fortify cyber defenses and ensure uninterrupted healthcare operations in the face of evolving threats.

Table 37: Module 11.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP011_S_H**
Module Title *The title of the training module*	**Cyber Ranges and Operations in healthcare domain**
Alternative Title(s) **Used alternative titles for the same module by many institutes and training providers**	"HealthCyber: Navigating Cyber Ranges in Healthcare Operations" "Securing Health: Cyber Range Strategies for Healthcare Operations" "HealthGuard: Advancing Cyber Range Operations in Healthcare" "CyberMed: Innovations in Cyber Ranges for Health Operations" "HealthShield: Fortifying Cyber Operations in Healthcare" "CyberCare: Enhancing Healthcare Operations through Cyber Ranges" "HealthNet Defenders: Strategies for Cyber Range Operations in Healthcare" "CyberHealth Ops: Optimizing Cyber Ranges for Healthcare" "Guardians of Health Data: Cyber Range Seminar for Healthcare Operations"

	"SecureCare: Cyber Range Solutions for Health Operations"
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**	"Cyber Ranges and Operations in the Health Domain" seminar provides a comprehensive exploration of cybersecurity strategies specifically tailored for the healthcare sector. Attendees will gain practical insights through detailed demonstrations using the Security Infusion tool. The seminar covers topics such as real-time notifications for malicious activities, generating actionable reports on system status, and continuous monitoring of critical infrastructure via a cloud-based security information management system. Participants will leave equipped with the knowledge and skills to fortify cyber defences and ensure uninterrupted healthcare operations in the face of evolving threats.

Module description **Indicates the main purpose and description of the module.**	"Cyber Ranges and Operations in the Health Domain" seminar offers a comprehensive exploration of cybersecurity strategies tailored specifically for the healthcare sector. Through detailed demonstrations featuring the Security Infusion tool, participants will gain practical insights into fortifying their cyber defences effectively. Attendees will discover how to configure a cloud-based security information management system to receive real-time notifications via email or Slack alerts, empowering IT service providers to swiftly respond to malicious activities. Hands-on exercises will guide participants in configuring notifications for security alerts to ensure rapid threat mitigation. Furthermore, the seminar will delve into generating insightful reports on system status, identifying new vulnerabilities, and providing actionable feedback. Participants will learn to utilize the Security Infusion tool to proactively address security gaps, enhancing the resilience of healthcare operations against cyber threats. In addition, attendees will gain valuable expertise in using a security information management system to continuously monitor a critical infrastructure. They will master the navigation of a centralized dashboard, enabling 24x7 surveillance and analysis of historical events at a granular level. By mastering these techniques, participants can bolster their healthcare organization's cybersecurity posture and ensure uninterrupted operations in today's rapidly evolving threat landscape.

Learning outcomes and targets **A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module**	**Knowledge:** • Understanding of cyber ranges and their application in healthcare operations. • Knowledge of common cyber threats and vulnerabilities specific to the healthcare sector. • Familiarity with real-time threat notification systems and their implementation. • Understanding of vulnerability management principles and practices in healthcare. • Knowledge of cloud-based security management platforms for continuous infrastructure monitoring. **Skills:** • Ability to set up and configure real-time threat notifications via email and Slack alerts. • Proficiency in using the Security Infusion tool for identifying and remediating vulnerabilities. • Skill in generating actionable reports on system status and vulnerabilities for stakeholders. • Competence in setting up and maintaining continuous infrastructure monitoring using cloud-based tools. • Skill in analysing historical events and trends to ensure 24x7 surveillance of critical healthcare systems. **Competences:** • Competence in implementing effective cybersecurity strategies tailored to the healthcare domain. • Ability to respond swiftly and effectively to cybersecurity incidents in healthcare environments. • Competence in proactively identifying and addressing security gaps to enhance healthcare operations resilience. Participants will leave the seminar equipped with the knowledge, skills, and competences necessary to enhance cybersecurity practices and safeguard healthcare operations effectively.

Main topics and content list **A list of main topics and key content**	**·Introduction to Cyber Ranges in Healthcare** **·Real-time Threat Notifications and Response** **·Vulnerability Management and Reporting** **·Continuous Infrastructure Monitoring with Cloud-Based Tools** **·Future Trends and Considerations in Healthcare Cybersecurity**
Evaluation and verification of learning outcomes **Assessment elements and high-level process to determine participants have achieved the learning outcomes**	N/A
Training Provider ***Name(s) of training providers.***	ITML
Contact ***Name(s) of the main contact person and their email address.***	Dimitra Siaili (itml), disiaili@itml.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).***	Dynamically change so you can visit the DCM platform
Duration ***Duration of the training.***	2times x 2hours or 1x 4hours
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 or Virtual. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.

Knowledge area(s) *Mapping 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	KA10 – Cyber Incident Response KA5 – Network and Communication Security 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.	On the next round of contributions
Tools to be used *A list of tools that will be used for the operation of this training module.*	Security Infusion
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English /Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes (CoA)
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically

3.11.1.2 Adapted Syllabus

Table 38: Module 11.1 Syllabus

Main topics	Suggested Content
Introduction to Cyber Ranges in Healthcare	Overview of cyber ranges and their relevance in healthcare operations. Discussion on the unique cybersecurity challenges faced by the healthcare sector. Case studies highlighting the importance of cyber ranges in healthcare incident response.
Real-time Threat Notifications and Response	Demonstration of setting up real-time notifications via email and Slack alerts using a cloud-based manager. Examples of common malicious activities in healthcare IT environments. Best practices for swift and effective response to cybersecurity incidents.
Vulnerability Management and Reporting	Overview of vulnerability management principles in healthcare. Hands-on exercises on using the Security Infusion tool to identify and remediate vulnerabilities. Creating actionable reports on system status and vulnerabilities for stakeholders.

Continuous Infrastructure Monitoring with Cloud-Based Tools	Introduction to cloud-based management platforms for infrastructure monitoring. Live demonstration of setting up continuous monitoring of critical (like healthcare) systems. Demonstration of how to use a centralized dashboard to analyse historical events and ensure 24x7 surveillance and examining any low-level historical event, if needed.
Future Trends and Considerations in Healthcare Cybersecurity	Discussion on the importance of ongoing education and training for cybersecurity professionals in the healthcare domain. Reflection on key takeaways from the seminar and recommendations for continued improvement in healthcare cybersecurity strategies.

3.11.1.3 Planning for Preparedness

Students need to download the corresponding material from the DCM platform, have a laptop and an internet connection to either attend remotely or physically. The seminar can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar). Trainers should just define a time schedule for teaching the course.

3.11.1.4 Materials and Exercises

The training seminar is supported by the following material:

- Presentations that will be used during the course and be provided digitally to the learners from the DCM platform.

3.11.1.5 Verification of Learning Outcomes, and Skills

Multiple assessments will be conducted throughout the course to ensure the full integration of all participants with the course content and to support the overall evaluation of the course.

3.11.2 CSP0011_W_H: Detection Engineering on a Cyber Range of a Healthcare IT infrastructure-Active Directory

3.11.2.1 Description of Training Module

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 to actively secure a cyber range simulating a background healthcare IT infrastructure containing workstations and servers.

Table 39: Module 11.2 Description

Code	**CSP011_W_H:**

Module Title *The title of the training module*	**Detection Engineering on a Cyber Range of a Healthcare 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 MITRE DEF3ND Framework SIEM Tools
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	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 healthcare infrastructure 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.*

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.	Cyber Security Engineer

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.	Available on the DCM
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.11.2.2 Adapted Syllabus

Table 40: Module 11.2 Syllabus

Main topics	Suggested Content
Detection of Spray User = Password:	Techniques and strategies for identifying and alerting on password spraying attempts, utilizing behaviour 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.

3.11.2.3 Planning for Preparedness

For better management and execution of the workshop 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.

3.11.2.4 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.

3.11.2.5 Verification of Learning Outcomes, and Skills

The workshop's effectiveness will be assessed through practical exercises within the lab environments, where participants will configure Sentinel and Wazuh to detect simulated attacks. These exercises aim to reinforce the theoretical knowledge provided in the slides through hands-on application, ensuring participants gain practical experience in detection engineering.

Upon completion, participants will have developed a solid understanding of how to use Sentinel and Wazuh for detecting sophisticated cyber-attacks, enhancing their capabilities in cybersecurity defence and operational security. This workshop will equip them with the necessary skills to improve their organization's security posture by implementing effective detection strategies against common attack vectors

3.11.3 CSP0011_CS-E_H: Simulation of a medical environment

3.11.3.1 Description of Training Module

The objective of the module is to practice penetration testing and defence in hospital environments. The following key points are highlighted for the practice:

- Protection of patient data (electronic health record, prescriptions)
- Protection of mobile and web healthcare applications

Protection of medical devices

3.11.3.2 Adapted Syllabus

Table 41: Module 11.3 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP011-CS-E_H**
Module Title *The title of the training module*	**Cybersecurity attacks and defences in the healthcare sector**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	N/A
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.*	CS-E
Level *Training level: B (Basic), A (Advanced)*	A (Advanced)
Module overview *High-level module overview*	The objective of the module is to practice penetration testing and defence in hospital environments. The following key points are highlighted for the practice: • Protection of patient data (electronic health record, prescriptions) • Protection of mobile and web healthcare applications

	• Protection of medical devices
Module description *Indicates the main purpose and description of the module.*	The module is designed for healthcare IT professional who need to secure healthcare environments, such as hospitals. The module is focusing on hands-on training, requiring students to first develop attack scenarios to compromise the virtual environment of the hospital. In a second step, students are required to go backwards and secure each element that they have been able to compromise.

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	Understanding vulnerabilities in hospital environments, including infrastructure and data issues. Ability to secure such environments.

Main topics and content list *A list of main topics and key content*	• Case Studies and Practical Exercises on a cyber-range hosting the virtual environment.
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	• Capture the flags elements for demonstrating attack successes • Comparison with reference configurations for defenses
Training Provider *Name(s) of training providers.*	IMT
Contact *Name(s) of the main contact person and their email address.*	Prof. Hervé DEBAR
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).*	Fall semester

Duration *Duration of the training.*	1 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.*	Physical only
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*	Includes elements for KA3, KA5, KA6, KA7, KA9
Pre-requisites	Basic IT and Security Knowledge

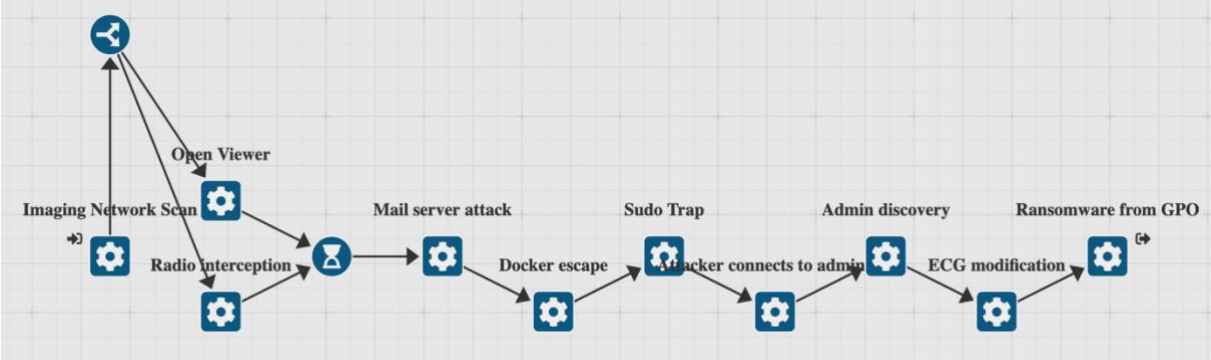
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	ECSF Profile 1: Chief Information Security Officer (CISO)
Tools to be used *A list of tools that will be used for the operation of this training module.*	Nmap, Nessus and Wireshark Specific (generally open source) medical software and emulators.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	French
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.
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.*	September each year
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.*	N/A

3.11.3.3 Planning for Preparedness

Students need to download the corresponding material from the DCM platform, have a laptop and an internet connection to either attend remotely or physically. The seminar can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar). Trainers should just define a time schedule for teaching the course

3.11.3.4 Materials and Exercises

The following figure describes one of the attack paths that will be implemented in the cyber-range.



There are multiple privilege escalation paths, leading to compromise of patient data, alteration of IT services, and data exfiltration. There are several classic IT attacks, but it also includes attack against virtual medical platforms (OpenEMR and OpenELIS in our case), and against specific French mobile applications (iSantéPlus). We also use Bhami as a front end to OpenEMR and OpenELIS, with additional services such as in-patient management, medical image management (PACS), and an Enterprise Resource Planning environment.

To realize the attack path, we deploy multiple versions of each component, including versions with known vulnerabilities (CVEs).

When coming to defenses, students have of course the possibility to use non-vulnerable versions. We also emphasize the use of alternative tools (such as filtering and firewalling, and access control) to ensure that they understand also that they can limit their exposure through proper system and network configuration.

3.11.3.5 Verification of Learning Outcomes, and Skills

Multiple assessments will be conducted throughout the course to ensure the full integration of all participants with the course content and to support the overall evaluation of the module.

3.12 Module 12 - Digital Forensics for Health

3.12.1 CSP0012_SA_H: Digital Forensics for Health Sector

3.12.1.1 Description of Training Module

Table 42: Module 12.1 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP012_SA_H**
Module Title *The title of the training module*	**Digital Forensics for Health Sector**
Alternative Title(s) Used alternative titles for the same module by many institutes and training providers	"Cyber Forensics in health domain" "Security information and event management – Forensics" "Healthcare Cybersecurity Investigations: Unveiling Digital Forensic Techniques" "Securing Health Data: Exploring Cyber Forensics Solutions" "Probing Health Incidents: A Digital Forensics Perspective" "Forensic Analysis in Healthcare: Tracing Digital Trails" "Safeguarding Health Systems: Navigating Cyber Forensic Procedures" "Health Data Breach Investigations: Strategies for Digital Forensics" "Unlocking Health System Vulnerabilities: The Role of Cyber Forensics" "Cybersecurity Resilience in Healthcare: Insights from Digital Forensics" "Investigating Health IT Incidents: A Digital Forensics Approach" "Protecting Patient Privacy: Exploring Cyber Forensics in Healthcare" Security information and event management - Forensics

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 seminar "Digital Forensics for Health" explores the intersection of cybersecurity and healthcare, focusing on investigative techniques to uncover the root causes of security incidents. Participants learn to analyse historical data, reconstruct events, and implement security measures to prevent future breaches, through suitable tools (Security Infusion). Key topics include digital forensic methodologies, incident analysis, restoration strategies, and real-world case studies. By equipping attendees with these skills, the seminar aims to enhance cybersecurity resilience in healthcare, safeguard patient data, and fortify infrastructure against cyber threats.

Module description Indicates the main purpose and description of the module.	The seminar "Digital Forensics for Health" is meticulously designed to offer attendees a comprehensive understanding of the pivotal role played by digital forensics in safeguarding healthcare systems and patient data against cyber threats. Through a meticulously structured program, participants will be guided through a live demonstration utilising the cutting-edge tool, Security Infusion. This demonstration will illustrate the meticulous process of conducting a detailed investigation into historical data, unveiling the precise sequence of events culminating in a security incident within healthcare environments. Moreover, the seminar will provide attendees with a comprehensive framework of guidelines and methodologies essential for executing efficient activities aimed at restoring and fortifying infrastructure against the identified root causes. By dissecting real-world case studies and offering practical insights, participants will gain invaluable expertise in digital forensic methodologies, including evidence collection, analysis, and interpretation. Emphasis will be placed on incident reconstruction techniques, enabling participants to pinpoint and rectify vulnerabilities effectively. Ultimately, the seminar endeavours to equip healthcare professionals with the requisite knowledge and skills to bolster cybersecurity resilience, ensuring the integrity and confidentiality of patient data while fortifying critical systems against cyber threats.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Knowledge: · Understanding of digital forensic methodologies in healthcare settings. · Knowledge of incident analysis and reconstruction techniques. · Familiarity with tools like Security Infusion for digital evidence analysis. · Awareness of regulatory compliance requirements in healthcare cybersecurity. · Understanding of cybersecurity risks and threats specific to healthcare environments. · Knowledge of infrastructure restoration strategies post-security incidents. · Awareness of best practices for securing healthcare systems against cyber threats. · Understanding of patient data protection and confidentiality principles. · Knowledge of industry standards and guidelines for healthcare cybersecurity. · Understanding of emerging trends and advancements in healthcare cybersecurity. Skills: · Ability to collect, analyse, and interpret digital evidence. · Proficiency in using Security Infusion or similar tools for forensic analysis. · Skill in conducting detailed investigations into security incidents. · Critical thinking and problem-solving skills for identifying root causes of incidents. · Communication skills for conveying findings and recommendations effectively. · Technical skills in infrastructure restoration and security implementation. · Risk assessment and management skills in healthcare cybersecurity.

	· Adaptability to evolving cybersecurity threats and technologies. Competences · Competence in applying digital forensic methodologies to healthcare environments. · Competence in incident analysis, reconstruction, and root cause identification. · Competence in using Security Infusion or similar tools for forensic investigations. · Competence in infrastructure restoration post-security incident. · Competence in implementing security measures to safeguard healthcare systems. · Competence in collaborating with stakeholders for effective incident response. · Competence in communicating cybersecurity findings and recommendations. · Competence in adapting to changes and emerging threats in healthcare cybersecurity.

Main topics and content list A list of main topics and key content	1. **Introduction to Digital Forensics in Healthcare** 2. **Investigative Techniques** 3. **Incident Analysis and Reconstruction** 4. **Restoration and Security Measures** 5. **Best Practices and Case Studies**
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	N/A
Training Provider *Name(s) of training providers.*	ITML
Contact *Name(s) of the main contact person and their email address.*	Dimitra Siaili (itml), disiaili@itml.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).*	TBD
Duration *Duration of the training.*	2times x 3hours or 6hours
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 or Virtual. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.

Knowledge area(s) *Mapping 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	KA10 – Cyber Incident Response KA1 – Cybersecurity 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.	Cybersecurity Researcher, Cybersecurity Risk Manager
Tools to be used *A list of tools that will be used for the operation of this training module.*	Security Infusion
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English/Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.

Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	Yes (CoA)
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.
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.*	Please refer to and check the online CyberSecPro DCM System regularly for the most current information. The dates provided will change dynamically.

3.12.1.2 Adapted Syllabus

Table 43: Module 12.1 Syllabus

Main topics	Suggested Content
Introduction to Digital Forensics in Healthcare	Understanding the importance of digital forensics in safeguarding health data and infrastructure.
Investigative Techniques	Learning methodologies and tools used to delve into historical data and reconstruct events leading to security incidents.
Incident Analysis and Reconstruction	Utilising the capabilities of Security Infusion tool, demonstration on how to deliver a detailed investigation into historical data and analyse digital evidence to piece together the sequence of events that caused a security breach or incident in healthcare systems.
Restoration and Security Measures	Providing guidelines for efficiently restoring systems and implementing security measures to prevent future incidents based on the findings of forensic investigations and the identified root cause. Security Infusion tool will be used.

Best Practices and Case Studies	Sharing best practices in healthcare cybersecurity and illustrating key concepts through real-world case studies and examples.

3.11.1.3 Planning for Preparedness

Students need to download the corresponding material from the DCM platform, have a laptop and an internet connection to either attend remotely or physically. The seminar can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar). Trainers should just define a time schedule for teaching the course.

3.11.1.4 Materials and Exercises

The training seminar is supported by the following material:

- Presentations that will be used during the course and be provided digitally to the learners from the DCM platform.

3.11.1.5 Verification of Learning Outcomes, and Skills

Multiple assessments will be conducted throughout the course to ensure the full integration of all participants with the course content and to support the overall evaluation of the course.

3.12.2 CSP012_S_H: Digital Forensics for Health

3.12.2.1 Description of Training Module

Table 44: Module 12.2 Description

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP012_SA_H**
Module Title *The title of the training module*	**Digital Forensics for Health**

Alternative Title(s) Used alternative titles for the same module by many institutes and training providers	"Digital Forensics in the Healthcare Sector" "Forensic Insights into Security Information and Event Management" "Analysing Healthcare Incidents through a Digital Forensic Lens" "Cyber Forensics: The Key to Strengthening Healthcare Systems" "Tactical Approaches to Health Data Breach Investigations" "Exposing Vulnerabilities in Healthcare: A Cyber Forensic Exploration" "Building Cyber Resilience in Healthcare with Forensic Intelligence" "Forensic Examination of Health IT Incidents" "Navigating the Digital Health Landscape: Forensic Principles and Practices"
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 (W)
Level Training level: B (Basic), A (Advanced)	A (Advanced)

Module overview High-level module overview	The workshop titled "Digital Forensics for Health" delves into the critical confluence of digital security and healthcare practices. It emphasises the application of forensic investigation techniques to pinpoint the origins of security breaches. Attendees will gain proficiency in analysing past data, piecing together event timelines, and deploying protective measures to avert future incidents, utilising specialised tools such as SmartViz. The curriculum covers a broad spectrum of subjects, including forensic investigation principles, incident scrutiny, recovery tactics, and insights from actual case studies. This workshop is designed to empower participants with the necessary expertise to boost cybersecurity defences in the healthcare sector, protect sensitive patient information, and strengthen the digital framework against potential cyber-attacks.
Module description Indicates the main purpose and description of the module.	The workshop "Digital Forensics for Health" is intricately designed to provide participants with an in-depth exploration of how digital forensics serves as a cornerstone in protecting healthcare systems and patient information from cyber threats. A hands-on experience will also reveal the step-by-step investigation of historical data, uncovering the exact series of events that lead to a cybersecurity incident within a healthcare setting through gaining insights into privacy considerations and legal ramifications. Delve into real-world scenarios pertaining to breaches of health data security. Furthermore, the workshop will arm participants with a solid set of guidelines and methodologies crucial for carrying out effective measures to rehabilitate and reinforce infrastructure against the root causes of such incidents. Through the examination of case studies, attendees will acquire critical skills in digital forensic techniques, encompassing the gathering, analysis, and interpretation of evidence. Special focus will be given to techniques for reconstructing incidents, allowing attendees to identify and address vulnerabilities with precision. Ultimately, this workshop is tailored to empower the attendees with the essential knowledge and tools to enhance cybersecurity defences, ensuring the protection and privacy of patient information while strengthening critical healthcare infrastructures against cyber threats.

Learning outcomes and targets A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module	Knowledge: ● Understanding of Digital Forensics in Healthcare ● Insights into Cybersecurity Threats and Vulnerabilities ● Familiarity with Forensic Tools and Technologies ● Comprehension of Incident Analysis Skills: Capability to Analyse and Interpret Digital Evidence Incident Reconstruction Implementation of Security Measures Competences: ● Enhanced Cybersecurity Resilience ● Effective Incident Response and Management ● Strategic Problem-Solving ● Data Protection and Compliance

Main topics and content list A list of main topics and key content	• Core Principles of Digital Forensics in Healthcare • Forensic Investigation Methodologies • Strategies for Incident Response and Prevention • Analyse digital evidence using scientifically validated methods • Building Cybersecurity Resilience in Healthcare
Evaluation and verification of learning outcomes Assessment elements and high-level process to determine participants have achieved the learning outcomes	N/A
Training Provider *Name(s) of training providers.*	ZELUS
Contact *Name(s) of the main contact person and their email address.*	Foteini Petropoulou (f.petropoulou@zelus.gr) Thanos Apostolidis (t.apostolidis@zelus.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).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	Refer and check online CyberSecPro DCM System for current information. Approximately 3-6 h
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 or Virtual. Please note that the method used will adapt based on the specific circumstances of each case. Trainees will be notified promptly to ensure they are adequately informed and prepared for any adjustments.

Knowledge area(s) *Mapping 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 KA8 – Cybersecurity Tools and Technologies KA10 – Cyber Incident Response
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.	Digital Forensics Investigator
Tools to be used *A list of tools that will be used for the operation of this training module.*	SmartViz
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	English/Greek
ECTS *If applicable, the number of ECTS.*	Not applicable; Micro-credentials are noted instead. A formula for converting ECTS to micro-credentials will be provided in T5.4-D5.3.

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.*	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.

3.12.2.2 Adapted Syllabus

Table 45: Module 12.2 Syllabus

Main topics	Suggested Content
1.Core Principles of Digital Forensics in Healthcare	• **Introduction to Digital Forensics**: Exploring the significance of digital forensics in safeguarding healthcare information systems and patient data. • **Cyber Threats and Vulnerabilities**: Overview of the landscape of cyber threats facing healthcare, along with common vulnerabilities.
2.Forensic Investigation Methodologies	• **Analytical Techniques:** Methodologies for collecting, analysing, and interpreting digital evidence in healthcare settings. • **Event Reconstruction Theories:** Theoretical frameworks for reconstructing the sequence of events leading up to security incidents, focusing on understanding the methodologies.
3.Strategies for Incident Response and Prevention	• **Incident Management Frameworks**: Discussion on the theoretical models for developing effective incident response strategies to cybersecurity breaches. • **Preventive Strategies and Best Practices**: Theoretical approaches to implementing preventive measures based on

	insights derived from forensic analysis, aimed at enhancing the cybersecurity posture of healthcare systems.
4.Analyse digital evidence using scientifically validated methods	**Standardised procedures:** ● Repeatability: Others can replicate the analysis and obtain similar results. ● Reliability: The methods consistently yield accurate outcomes. ● Validity: The techniques align with accepted forensic principles. ● Transparency: The process is well-documented and transparent.
5.Building Cybersecurity Resilience in Healthcare	● **Cybersecurity Infrastructure Strengthening**: Theoretical perspectives on enhancing the resilience of healthcare systems against cyber threats through improved cybersecurity practices.

3.11.1.3 Planning for Preparedness

Students need to download the corresponding material from the DCM platform, have a laptop and an internet connection to either attend remotely or physically. The seminar can be either delivered online or/and with physical presentation and suitable time should be allocated for the availability of suitable tutors, location (in case it is a physical seminar). Trainers should just define a time schedule for teaching the course.

3.11.1.4 Materials and Exercises

The training seminar is supported by the following material:

- Presentations that will be used during the course and be provided digitally to the learners from the DCM platform.

3.11.1.5 Verification of Learning Outcomes, and Skills

Multiple assessments will be conducted throughout the course to ensure the full integration of all participants with the course content and to support the overall evaluation of the course.

4 Conclusions

This chapter outlines the detailed syllabus for each of the 12 CyberSecPro (CSP) Health Modules, designed to address the cybersecurity needs within the healthcare sector. These modules are developed to equip healthcare professionals with the essential skills and knowledge to safeguard sensitive health information and infrastructure against cyber threats. Each module's syllabus is crafted considering the templates of D3.1 and the Cybok framework, ensuring relevance and applicability to the health sector's unique challenges.

The overall operational plan for the CSP Health Modules acknowledges the challenges of integrating new courses into rigid Higher Education Institution (HEI) programs. To overcome these barriers, CSP partners have introduced seminars, workshops, and exercises that can be incorporated as additional topics in existing curricula. This flexible approach allows for the inclusion of cutting-edge cybersecurity topics in healthcare education without the need for comprehensive curriculum overhauls. Additionally, these modules can be integrated into summer schools and conferences, offering further opportunities for healthcare professionals to enhance their cybersecurity knowledge and skills.

This strategy ensures that the CSP Health Modules are not only academically rigorous but also practically applicable, providing healthcare professionals with the tools they need to address the evolving cybersecurity challenges within the health sector.