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

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

CyberSecPro

D6.5
Individual Exploitation Plans

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

Related WP	WP6	Dissemination Level	PU
Lead Participant	ACEEU	Lead Author	Thorsten Kliewe, Lina Landinez (ACEEU)
Contributing Participants	LAU, TalTech, UCY, UMA, UNSPMF, UNINOVA, UPRC, FCT, AIT, C2B, ITML, SLC, SGI, FP, MAG, SINTEF, ZELUS, APIRO	Related Deliverables	D6.1, D6.3, D6.4

Abstract: This deliverable consolidates the individual exploitation plans of CyberSecPro partners, documenting how organisations are integrating and sustaining key exploitable result 1 (KER1; the modular training portfolio) beyond the funding period. It presents a comparable, partner-by-partner view of baseline educational offers and the concrete pathways through which CyberSecPro outputs are being embedded into university curricula and company training catalogues to generate long-term value for learners and labour-market stakeholders

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

Deliverable 6.5 (D6.5) captures how CyberSecPro is transitioning from consortium-level development to organisation-level exploitation, with each partner specifying how CyberSecPro results are being continued, institutionalised, and scaled after project end. The report follows a harmonised structure for all contributing partners: it first establishes a baseline by describing pre-CyberSecPro educational and training offers, then outlines which CyberSecPro modules have been (co-)implemented, and finally explains how partners are exploiting/sustaining those modules through curricular integration, recurring professional training delivery, or continued collaboration formats. This structure enables a clear "before-and-after" narrative across the consortium, highlighting where CyberSecPro is adding new sectoral coverage (e.g., health, energy, maritime), modular short-course architectures, and stronger alignment with competence frameworks relevant to employability and workforce needs.

Across Higher Education Institutions (HEIs), exploitation is primarily being realised through embedding CyberSecPro modules into accredited programmes and existing courses, in many cases as integrated content blocks, redesigned course components, or modular add-ons that can be reused across cohorts. In parallel, several partners are indicating pathways for broader reach through micro-credentials, Massive Open Online Courses (MOOCs), seasonal schools, and short-format trainings that complement degree education and support lifelong learning.

Across companies and other training providers, exploitation is being realised through productisation of modules into market-facing training offers, exercises, and workshop formats that can be repeatedly delivered to clients, often leveraging practical and scenario-based learning to meet upskilling demand.

Taken together, the individual plans show CyberSecPro's impact being sustained through recurring delivery mechanisms (degree programmes, training catalogues, and repeatable exercise formats) rather than one-off project pilots, thereby strengthening the long-term availability of job-relevant cybersecurity education for stakeholders connected to each partner's regional ecosystem.

Document information

Contributors

Name	Beneficiary
Thorsten Kliewe	ACEEU
Lina Landinez	ACEEU
Faraz Hayat	ACEEU
Jeldo Meppen	ACEEU
The main contributors of this deliverable like to highlight the crucial insights (specifically organisational information, pre-CSP training offers, CSP training offers and exploitation plans) given by the following partners: LAU, TalTech, UCY, UMA, UNSPMF, UNINOVA, UPRC, FCT, AIT, C2B, ITML, SLC, SGI, FP, MAG, SINTEF, ZELUS, APIRO	

Reviewers

Name	Beneficiary
Christos Douligeris	UPRC (Technical Lead)
Spiros Borotis	MAG (WP leader)
Cristina Alcaraz	UMA
Emmanouil Vergis	ZELUS

History

Version	Date	Contributor(s)	Comment(s)
0.1	2026-01-09	Thorsten Kliewe	1st Draft: Add ToC
0.2	2026-01-15	Thorsten Kliewe	Refine outline, first draft of Introduction
0.3	2026-01-21	Jeldo Meppen	Add pre-CSP offerings of HEI partners
0.4	2026-02-02	Jeldo Meppen	Add pre-CSP offerings of SME partners
0.5	2026-02-15	Lina Landinez	Added summaries

0.6	2026-01-20	Lina Landinez	Added exploitation tables and summary
0.7	2026-02-24	Thorsten Kliewe, Jeldo Meppen	Intergrated first level feedback
0.8	2026-02-28	Thorsten Kliewe, Lina Landinez	Final check, finalisation, approved 2nd and high-level review
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Tables

List of Acronyms

A	**ACL**	Access Control List
	AD	Active Directory
	AI	Artificial Intelligence
C	**CASP**	CompTIA Advanced Security Practitioner
	CEH	Certified Ethical Hacker
	CIA	Confidentiality, Intrulegrity, Availability (security model)
	CISSP	Certified Information Systems Security Professional
	CSRF	Cross-Site Request Forgery
	CSS	Cascading Style Sheets
	CySA	CompTIA Cybersecurity Analyst
D	**DCM**	Dynamic Curriculum Management
E	**ECSF**	European Cybersecurity Skills Framework
	ECTS	European Credit Transfer System
	ENISA	European Union Agency for Cybersecurity
	EU	European Union
	EuroTeQ	EuroTeQ Engineering University (alliance)
F	**FPCDX**	Focal Point Cyber Defense Exercise
H	**HADEA**	European Health and Digital Executive Agency
	HEI	Higher Education Institution
	HtB	Hack The Box
	HTML	HyperText Markup Language
I	**ICT**	Information and Communication Technology

	IDOR	Insecure Direct Object Reference
	IDS/IPS	Intrusion Detection System / Intrusion Prevention System
	IoT	Internet of Things
	IPICS	Intensive Programme on Information and Communication Security
	IPR	Intellectual Property Rights
	IPv6	Internet Protocol version 6
	ISACA	Information Systems Audit and Control Association
	ITSRM	IT Security and Risk Management
K	**KAs**	Knowledge Areas
	KER	Key Exploitable Result / Key Exploitable Result 1
	KQL	Kusto Query Language
L	**LAN**	Local Area Network
	LbD	Learning by Developing
	LFI/RFI	Local File Inclusion / Remote File Inclusion
	LLVM	Low Level Virtual Machine (a set of compiler and toolchain technologies)
M	**ML**	Machine Learning
	MOOC	Massive Open Online Course
	MSSP	Managed Security Service Provider
N	**NATO**	North Atlantic Treaty Organization
O	**OSINT**	Open Source Intelligence
P	**PKI**	Public Key Infrastructure
Q	**QS**	QS World University Rankings

R	**R&D**	Research and Development
S	**SCORM**	Sharable Content Object Reference Model (e-learning format)
	SEA	Partner code (full expansion not provided)
	SIEM	Security Information and Event Management
	SMB	Server Message Block (protocol)
	SME	Small and Medium-sized Enterprise
	SOC	Security Operations Centre
	SQL	Structured Query Language
	SUID	Set User ID (permission bit)
X	**XR**	Extended Reality
	XSS	Cross-Site Scripting
Y	**YUFE**	Young Universities for the Future of Europe

1 Introduction

Deliverable D6.5, "*Individual Exploitation Plans,*" represents a critical component of Work Package 6 (WP6), focusing on the sustainability and long-term impact of the CyberSecPro (CSP) project at the organisational level. While the project delivers an integrated ecosystem for European cybersecurity education, the success of this project depends on the commitment and specific exploitation plans identified by each of the 28 consortium partners. D6.5 serves as a formal collection of these customised strategies, detailing how each Higher Education Institution (HEI) and Small to Medium Enterprise (SME) will utilize, internalise, and promote the project's Key Exploitable Results (KERs) within their respective contexts. This deliverable complements the broader strategic frameworks established in D6.3 (*Overall Exploitation Plan*) and D6.4 (*Grouped Exploitation Plans*) by providing granular, partner-specific roadmaps for the post-funding era.

1.1 Background

The CyberSecPro project was launched to address a staggering misalignment between academic supply and market demand for cybersecurity skills in Europe. Existing academic programs often rely on static curricula that fail to provide the dynamic, hands-on capabilities required by the modern European Digital Single Market and critical sectors such as health, energy, and maritime.

The project has successfully developed a suite of 12 core training modules, an agile Dynamic Curriculum Management (DCM) system, and a certification schema designed to bridge the gap between degrees and working life. As the project reaches its final phase (Month 39, including extension), it is necessary to transition from consortium-wide development to individual organisational exploitation to ensure these results do not suffer from "project-end abandonment".

1.2 Purpose and Scope

The primary purpose of this deliverable is to report the specific exploitation intentions of CyberSecPro partners. Given that the overall exploitation plan already focuses on how the entire CSP modules, the DCM and the certification can be exploited, and the group exploitation plans focus on joint R&D efforts, future joint applications for a master program, and collaborative efforts to keep all CSP materials open access, the individual exploitation plans presented in this deliverable focus on the integration of the developed materials (KER1) and short- to medium-term teaching and learning activities in the partner organisations.

KER2 (CSP Certification Scheme), KER3 (DCM), and KER4 (Insight Reports and Best Practices) were not included in this planning as:

- Partners reported in the 2025 Lisbon Meeting that they plan to transfer the CSP training materials to their institutional Learning Management Systems (e.g., Moodle, Blackboard, ILIAS) rather than using the established DCM (KER3). This approach supports stronger integration into existing organisational structures, provides easier access for students (as no separate account is required), and enables faster intervention in the event of technical issues. The DCM will remain the preferred solution for individual learners and for institutions that do not wish to transfer the learning materials into their own systems.
- KER2 (the certification scheme) is strategically important, but it operates at a more cross-organisational and governance-dependent level (e.g., shared assessment logic, ECSF alignment, and potential higher-level recognition), and therefore serves as a complementary framework rather than the primary object of partner-level exploitation planning in this deliverable.
- KER4 (Insight Reports and Best Practices) was not included in the individual exploitation plans because, unlike deployable training materials or platforms, it serves primarily as a cross-project knowledge and guidance resource that supports consortium-wide learning and strategic uptake rather than direct partner-level implementation.

As outlined in the proposal, individual exploitation plans were only planned for those organisations that are not engaged in group exploitation plans. Despite this, nearly all CSP partners have outlined their exploitation intentions in this document.

1.3 Relation with other WPs and Deliverables

D6.5 is the culmination of efforts across several Work Packages and serves as a vital input for the final project evaluation. Its primary relationships include:

- **WP2 & WP3:** D6.5 draws its content foundations from D2.3 (*Programme Specifications*) and D3.1 (*DCM Setup and Syllabi*), which defined the knowledge areas and training structures that partners are now exploiting.
- **WP4:** The practical experiences and trainee feedback gathered during the operational phase (T4.3–T4.6) informed the refinement of these individual plans, identifying which modules had the highest market or academic value.
- **WP5:** A critical input for D6.5 is the evaluation analysis generated in Task 5.2 and Deliverable 5.2, which analyses trainee and trainer feedback to identify the most effective modules and tools. These results allow partners to prioritise the integration of "Best Practice" outcomes into their individual future plans, focusing resources on the highest-impact results.
- **WP6 Tasks:** This deliverable is the direct output of Task 6.3 (*IPR Management and Exploitation Planning*), which involved all partners (except SEA) in identifying and protecting foreground results.

1.4 Structure of the Report

This *Section 1* (Introduction) sets the scene for the report. It begins by outlining the broader background and context in which the report is embedded, including the rationale for the exploitation activities addressed. The introduction then clarifies the purpose and scope of the document, specifying what the report aims to achieve and which aspects are covered.

Section 2 (Individual Exploitation Planning Approach) describes the methodological approach applied to individual exploitation planning. It introduces KER1 (as the primary KER exploited), outlining its core characteristics, relevance, and potential value. This is followed by a description of the mapping approach used to link the exploitable result to institutional contexts and planned exploitation pathways, providing the analytical foundation for the institution-specific sections that follow.

Section 3 (Integration into University Curricula and Education/Training Offers) constitutes the main body of the report. It presents the individual exploitation plans of each partner HEI in a harmonised structure to ensure comparability. For each university, the section starts with a brief presentation of the relevant organisation or unit, followed by an overview of the pre-CSP educational offer. Hereafter, the CSP training offers of the respective HEI as well as the HEI's intention on how to sustain/exploit the training is detailed. A final summary highlights how CSP has enabled and will continue to enable the modernisation of the CSP HEI's curricula and education/training offers.

Section 4 (Integration into Company Training Offers) mirrors the previous section with a focus on the companies involved in the CSP project.

Ultimately, *Section 5* (Conclusion) summarises the key findings of the report. It reflects on the main contributions of the exploitation planning exercise, discusses identified limitations, and outlines a future outlook.

2 Individual Exploitation Planning Approach

This section outlines the methodological approach applied to support consortium partners in developing their individual exploitation plans. It describes KER1 (as the main input) and how baseline information on existing educational offers was translated into strategic decisions.

2.1 KER1 Description

The primary KER serving the Individual Exploitation Plans is CSP's comprehensive suite of 12 practical training modules designed to be integrated into existing university curricula and professional education offers. This repository is specifically structured to bridge the gap between static academic degrees and the dynamic, hands-on skills required by the modern European labour market.

1. Knowledge Areas and Module Composition

The training programme is founded upon ten prioritised Knowledge Areas (KAs) identified through extensive market demand analysis and alignment with existing European frameworks:

1. Penetration Testing
2. Cybersecurity Tools and Technologies
3. Cybersecurity Management
4. Cybersecurity Threat Management
5. Risk Management
6. Cybersecurity Policy, Process and Compliance
7. Incident Response
8. Network and Communication Security
9. Privacy and Data Protection
10. Human Aspects of Cybersecurity

These Knowledge Areas are operationalised through 12 core training modules:

- Module 1: Cybersecurity Essentials and Management
- Module 2: Human Factors and Cybersecurity
- Module 3: Cybersecurity Risk Management and Governance
- Module 4: Network Security
- Module 5: Data Protection and Privacy Technologies
- Module 6: Cyber Threat Intelligence
- Module 7: Cybersecurity in Emerging Technologies
- Module 8: Critical Infrastructure Security
- Module 9: Software Security
- Module 10: Penetration Testing
- Module 11: Cyber Ranges and Operations
- Module 12: Digital Forensics

To cater to varying learner maturity levels, each module is offered with both Basic (B) and Advanced (A) approaches.

2. Sector Specialisation and Capabilities

The exploitation strategy emphasises Sector Specialisation alongside Generic Modules. While the 12 generic modules provide a foundational skill set, they have been tailored into specific versions for three critical economic sectors:

- Health
- Energy
- Maritime

These modules are categorised into four distinct categories of capabilities to balance the training offer across different professional needs:

1. Cybersecurity Principles and Management: Providing foundational knowledge and oversight skills.
2. Cybersecurity Tools: Focusing on the practical application of technical instruments.
3. Emerging Technologies: Addressing security for innovations like AI, Blockchain, and IoT.
4. Offensive Cybersecurity Practices: Developing ethical hacking and penetration testing capabilities.

3. Pedagogical Delivery and Assignment Types

HEIs can exploit these materials through diverse module types and attendance formats. The programme supports heterogeneous modular learning, including:

- Course (C)
- Workshop (W)
- Seminar (S)
- Cybersecurity Exercises (CS-E)
- Summer Schools / Winter Schools (SS)
- Hackathons (H)
- Others (O)

Delivery is flexible, allowing for Physical, Virtual, or Hybrid/Mix formats to accommodate various institutional infrastructures and learning preferences. To ensure rigorous assessment and European Credit Transfer System (ECTS) credit alignment, the modules utilise a variety of assignment types:

- Programming tasks
- Essays
- Presentations
- Test exams
- Mutual peer-review among students
- Other specialised assessments (such as practical projects or lab reports)

4. Framework Alignment for University Integration

A critical factor for university exploitation is the mapping against the European Cybersecurity Skills Framework (ECSF). Each module is linked to specific ECSF job profiles, ensuring that academic programs adopting these materials provide students with recognised, job-ready competencies that meet European Union (EU) standards. This alignment facilitates the harmonisation of cybersecurity education across European HEIs.

2.2 Methodology

To document the CSP Training Modules' integration into university curricula and education/training offers, and into company training offers, a systematic and iterative methodology was employed, primarily driven by Task 6.3 (IPR Management and Exploitation Planning). This process ensured that each HEI and SME within the consortium could translate project-level results into specific, sustainable organisational roadmaps.

Steps

The methodology followed these core steps:

1. **Baseline Data Collection and Supply Analysis**
   The process began with an extensive audit of existing resources provided by the 28 consortium partners. Partners utilised templates established in WP2 and WP4 to declare their current educational offerings and technological tools. This data, documented in D2.2, provided the

baseline for the "Pre-CSP educational offer" section for each partner and was updated (if necessary) by the partner in the exploitation planning.

2. **Strategic Mapping**
   Building on the baseline data collected, the second step of the methodology focused on a structured comparison between partners' existing courses and the training modules that have been (co-)offered by each CSP partner. By systematically mapping declared courses against the CSP training module implementations (that were offered to a variety of learner groups), partners were able to identify overlaps, gaps, and areas of partial coverage.

   The results of this mapping informed two complementary strategic directions. First, it provided a clear rationale for advancing and updating existing courses, for example: through the integration of missing knowledge areas, the strengthening of practical components, or the reorientation of learning outcomes towards specific cybersecurity profiles. Second, it enabled the identification of unmet needs that could not be sufficiently addressed through course adaptation alone, thereby justifying the development of new courses or training offers within the CyberSecPro scope.

3. **Definition of Exploitation Intentions**
   Finally, each partner defined its exploitation intentions for every (co-)implemented module. As this deliverable will be made public, and as future curriculum and training portfolio planning can represent a competitive advantage, most partners have chosen to describe their plans at a strategic rather than detailed level.

Standardised Presentation Structure

To ensure a coherent and comparable overview across the consortium, each partner's plan is structured into four parts

1. **Presentation of organisation/unit:** Provides context on the partner's profile and role within the European cybersecurity landscape.
2. **Pre-CSP educational offer:** Summarises the baseline courses identified during the initial supply analysis (updated where relevant).
3. **CSP implemented modules and exploitation intentions:** Lists the CSP modules implemented by the partner and outlines how the partner intends to leverage and further develop the value generated through these modules.
4. **Summary:** Concludes the previous sections by highlighting how CSP has enabled (or will enable) the partner to modernise and strategically enhance its curriculum.

3 Integration into University Curricula and Education/Training Offers

3.1 Laurea University of Applied Sciences (LAU)

3.1.1 Presentation of organisation/unit

Laurea University of Applied Sciences (LAU) was established in 1992 in the Greater Helsinki region of Finland, operating across six campuses in Uusimaa. With approximately 9,900 students and 660 staff members, Laurea is recognised for its distinctive Learning by Developing (LbD) pedagogical model, which emphasises practical project-based education with real-world organisations and maintains the highest employment rate among Finnish universities of applied sciences. The university offers Bachelor's and Master's Degree programs in English and Finnish across fields including Business Information Technology and Cyber Security, Safety and Security Management, and Service Innovation and Design. Laurea engages in applied research and development activities focused on health and well-being, service business, and security, while maintaining strong international partnerships through programs like Erasmus+ and collaborations with institutions including the University of Cambridge and The Hague University of Applied Sciences. The university holds quality certifications from the Finnish Education Evaluation Centre and the European Consortium for Accreditation, reflecting its commitment to internationally recognised educational standards.

3.1.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
The ICT Environment and Infrastructure *ICT & Cybersecurity*	Undergraduate, Semester 1	5	Information systems development, implementation, and maintenance; system structure and operational environment; identification of information security threats.
Information Management and Databases *ICT & Cybersecurity*	Undergraduate, Semester 1	5	Database design, implementation, management and usage; query languages (SQL) for data retrieval and modification.
Data Networks and Information Security *ICT & Cybersecurity*	Undergraduate, Semester 2	5	Data network structure and operation (LAN, wireless, Internet); IP networks and protocols; Confidentiality, Integrity, and Availability (CIA) model; information security threats and safeguards for local networks.
Fundamentals of Programming *ICT & Cybersecurity*	Undergraduate, Semester 2	5	Programming fundamentals including syntax, building blocks, and best practices; planning, implementation, and

			testing of small-scale programs using Python.
Foundations of Web Development *ICT & Cybersecurity*	Undergraduate, Semester 2	5	Web site design, implementation, and publishing using HTML5, CSS3, and JavaScript; layout design according to customer needs.
Internet Infrastructure and Security *ICT & Cybersecurity*	Undergraduate, Semester 3	5	Global IP network operations and protocols; IP subnetting; security vulnerabilities in IP infrastructure; IPv6; wireless networking and cloud computing security risks.
Network Applications *ICT & Cybersecurity*	Undergraduate, Semester 3	5	LAN services development and management; network applications for companies; application security threats; secure ICT infrastructure design and implementation.
Introduction to Information Security *ICT & Cybersecurity*	Undergraduate, Semester 3	5	CIA model; threats, attacks, and vulnerabilities; security technologies and architectures; identity and access management; risk management; cryptography and PKI; cybersecurity domains.
Information Security Management *Business Information Technology*	Undergraduate, Semester 3	5	Information security program development and management; risk management, incident management, and compliance; risk assessment processes and problem-solving.
Enterprise Security and Practitioners *Business Information Technology*	Undergraduate, Semester 4/5	5	Web application and server security threats; attack tactics and hacking techniques; security controls implementation; hands-on hacking exercises in virtualized environments.
Cybersecurity Analyst *Business Information Technology*	Undergraduate, Semester 4/5	5	Network discovery, reconnaissance, harvesting, and vulnerability analysis; attack surface reduction; professional reporting of security findings.
Network and Applications Security *Business Information Technology*	Undergraduate, Semester 4/5	5	Ethical hacking in offensive and defensive security; penetration testing processes including footprinting, scanning, enumeration, and system

			hacking; security controls based on vulnerability analysis.
Systems Security *Business Information Technology*	Undergraduate, Semester 4/5	5	Organisational systems threats and risks; cryptographic methods and applications; risk assessment and management; workstation and server security controls; authentication and authorization.
Cybersecurity Project *Business Information Technology*	Undergraduate, Semester 4/5	5	Team-based cybersecurity projects (research, innovation, cyber ranges, cyber defence); project planning, implementation, and documentation; academic and professional presentation of results.
Cybersecurity Hackathon Project *Business Information Technology*	Undergraduate, Semester 4/5	3	Team-based reconnaissance and vulnerability analysis in real environments; professional presentation of findings; critical analysis using industry-standard tools (Kali Linux, Nessus, Metasploit, etc.).
Cybersecurity Working Life Practices *Business Information Technology*	Undergraduate, Semester 4/5	2	Professional working life activities including industrial visits, seminars, workshops, cyber ranges, and cyber defence exercises; networking with cybersecurity professionals.
Information and Cyber Security *Safety, Security and Risk Management*	Undergraduate, Semester 1	5	Key principles of information and cyber security; requirements and best practices; risk management; procedures and instructions related to information and cyber security.
Information and Cyber Security Management *Safety, Security and Risk Management*	Undergraduate	10	Information and cyber security requirements and best practices; risk management; administrative, operational, technical, and structural procedures; security planning, evaluation, and development.
Cyber Security Management *Security Management*	Post-graduate	5	Importance of cyber security for organisational operations; critical threats and risks from information networks; information security, risk management, and continuity management.

Risk Manager *Advanced Training in Security and Risk Management*	Professional/Executive	5	Threat identification; security of information systems; relevant standards for security and risk management.

Table 1: LAU pre-CSP educational offer

Summary of pre-CSP offering

LAU offers a comprehensive and practice-oriented educational portfolio in ICT and cybersecurity, delivered across three departments: ICT & Cybersecurity, Business Information Technology, and Safety, Security and Risk Management. The portfolio spans undergraduate to professional levels, combining technical foundations with management perspectives and hands-on practical experience, reflecting the applied sciences mission of the institution.

At the undergraduate level, the curriculum follows a well-structured progression from foundational to advanced topics. Early Semesters (1-2) establish core competencies in ICT environments, database management, data networks, programming, and web development. Students are introduced to information security principles from the outset, including the CIA model and basic threat identification. The technical foundation is delivered primarily through the ICT & Cybersecurity department and utilises industry-standard tools such as Python, SQL, and Cisco Packet Tracer.

Mid-level courses (Semester 3) deepen technical expertise in internet infrastructure, network applications, and information security management. Students engage with IP networking, security vulnerabilities, cryptography, PKI concepts, and risk management processes. The curriculum bridges technical and management perspectives, with the Business Information Technology department contributing courses on security programme development and compliance.

Advanced undergraduate courses (Semesters 4-5) are highly specialised and practice-intensive, focusing on professional cybersecurity skills. Students gain hands-on experience in ethical hacking, penetration testing, vulnerability analysis, and enterprise security through virtualized training environments aligned with industry certifications (CASP, CySA+, CEH, CISSP). Project-based learning is emphasised through dedicated cybersecurity projects, hackathons, and working life practices that connect students with industry professionals and real-world scenarios.

The Safety, Security and Risk Management department complements the technical offering with courses focused on organisational security governance, covering administrative, operational, technical, and structural procedures for information and cyber security management. These courses integrate risk management frameworks and best practices at both introductory and advanced levels.

At the post-graduate level, the Cyber Security Management course addresses strategic and organisational dimensions, focusing on the impact of cyber security on business operations, critical threats, and the integration of security with risk and continuity management. Professional and executive education is provided through the Risk Manager training programme, covering threat identification, systems security, and relevant standards.

A distinctive strength of LAU's offering is its strong applied orientation and industry alignment. The curriculum extensively uses virtualised labs, capture-the-flag platforms (PicoCTF), and industry-standard security tools (Kali Linux, Nessus, Burp Suite, Metasploit, Wireshark, Splunk). Project-based and team-based learning, including hackathons and cyber defence exercises, prepares students for professional practice. The portfolio demonstrates a balanced and vertically integrated approach, linking foundational ICT education with advanced, practice-oriented cybersecurity expertise across technical, managerial, and strategic dimensions.

3.1.3 CSP offer and exploitation plan

The following table presents LAU's (co-)implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Introduction to Penetration Testing and Nmap Tool Training CSP010_W General Basic	This training provides students with a comprehensive understanding of essential penetration testing concepts and hands-on experience with the powerful Nmap tool.	Content would be integrated into the existing course Offensive Security and Ethical Hacking (new name from 2027)
Leveraging Domain and Threat Intelligence in the Energy Domain CSP011_C_E Energy Basic	Provides knowledge and practical skills to efficiently manage digital forensics and incident response actions. The course covers incident handling fundamentals, SIEM implementation for threat detection and log analysis, and incident response strategy development.	Content would be integrated into the existing course Offensive Security and Ethical Hacking (new name from 2027)
Cybersecurity Essentials and Management for Energy Sector (v003) CSP001_C_E Energy Basic	This CSP training module provides equip trainees and professionals with the knowledge and skills needed to defend against evolving cyber threats critical energy industry.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Basic Network Vulnerability Assessment and Beyond: Nessus Hands on Training CSP010_W General Basic	This hands-on training provides participants with the skills and knowledge they need to use Nessus to perform basic and advanced network vulnerability assessments. Participants learn how to install and configure Nessus, create and run scans, interpret scan results, and generate reports.	Content would be integrated into the existing course Offensive Security and Ethical Hacking (new name from 2027)
Introduction to Analysing Network Security: Wireshark Hands on Training CSP004_W General Basic	This hands-on training introduces Wireshark, a powerful network protocol analyser that is used by cybersecurity professionals around the world. You learn how to use Wireshark to capture, filter, and analyse network traffic, and how to use this information to identify and investigate network security threats.	Content will be integrated into the existing course Offensive Security and Ethical Hacking (new name from 2027)

Name	Description	Exploitation plan
Human Aspect of Energy Cybersecurity CSP002_S_E Energy Basic	This workshop navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Penetration Testing in the Health Sector CSP010_W_H Health Advanced	This workshop focuses on penetration testing and red teaming, where students are not only taught but also provided with a demo in performing a variety of realistic attacks. The course provides in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber-attacks against background healthcare infrastructure.	Content would be integrated into the existing course Offensive Security and Ethical Hacking (new name from 2027)
Cybersecurity Essentials and Management for Maritime CSP001_W_M Maritime Basic	This training module provides a comprehensive introduction to cybersecurity for the maritime sector, equipping participants with the knowledge and skills to protect their organisations from cyber threats.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Cybersecurity Essentials and Management CSP001_W General Basic	This workshop equips participants with the fundamental knowledge and best practices to safeguard online business operations against evolving cyber threats. Through this introduction, we set the stage for the crucial role of cybersecurity in the dynamic and rapidly expanding world of e-commerce.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Human Factors in Maritime Cybersecurity CSP002_S_M Maritime Basic	This seminar navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in the energy context. Attendees uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Cybersecurity for the Critical Sectors in Europe	This intensive training equips professionals with the knowledge and strategies to safeguard Europe's vital sectors from escalating cyber	To discuss in faculty to offer it as part or separate course and in a

Name	Description	Exploitation plan
CSP001_S_M Maritime Advanced	threats. By delving into the complex interplay of technology, policy, and human factors, participants develop a comprehensive understanding of critical infrastructure's cybersecurity challenges and learn to implement robust defence mechanisms.	MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Cybersecurity in Emerging Technologies, in particular explainable AI for Healthcare CSP007_S_H Health Advanced	This comprehensive training equips participants with the knowledge and skills to navigate the complex cybersecurity landscape and protect an organisation from emerging risks. As technology evolves unprecedentedly, so do the cyber threats targeting organisations.	Content would be integrated into the existing course Cybersecurity technologies (new name from 2027)
Cybersecurity hackathon CSP011_H General Basic	12-hour hackathon implementation with Capture the Flag competition.	Content would be integrated into the existing course Cybersecurity Hackathon Project
Social Engineering and Human Factors CSP002_S General Basic	The seminar covers human-centred cybersecurity risks, manipulation techniques, behavioural vulnerabilities, and strategies to strengthen organisational awareness and resilience.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Cybersecurity Essentials and Management for Energy Sector (v002) CSP001_C_E Energy Basic	This course provides a brief overview of the main issues and measures being addressed in the energy sector CPS001_C_E, which is focused on the "Cybersecurity Essential and Management for Energy Sector".	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Foundations of networking and systems security CSP004_S General Advanced	In the modern digital landscape, understanding the fundamentals of networking and systems security is crucial for individuals and organisations alike. It is not just about keeping your personal devices secure but also about protecting sensitive data and ensuring the reliable operation of critical systems. This	Content would be integrated into the existing course Internet Infrastructure and Cloud Security (new name in 2027)

Name	Description	Exploitation plan
	CyberSecPro training examines the systems security associated with a business aspect.	
Risk Management and Risk Assessment CSP003_S_H Health Basic	Fundamental concepts on risk assessment, presenting the ITSRM methodology and examples on healthcare infrastructure.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Human Factors and Cybersecurity Energy CSP002_S_E Energy Basic	This course dives deep into the human elements of cybersecurity, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants gain insights into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Programming Foundations for CyberSecurity CSP001_C General Basic	This training module introduces students to the foundational concepts of programming while integrating essential principles of cybersecurity.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.
Human Factors and Cybersecurity CSP002_W General Basic	This workshop examines how psychological safety and information disorder intersect, using behavioural science and psychology as the lens. In an era where misinformation, disinformation, and psychological manipulation spread rapidly — especially through the Internet and AI — Western democracies face growing challenges to public trust in democratic institutions, as highlighted by the World Economic Forum.	To discuss in faculty to offer it as part or separate course and in a MOOC form in the long term. It could also be offered as part of our training catalogue targeted at companies.

Table 2: LAU offer and exploitation plan

3.1.4 Summary

Before CyberSecPro, LAU was delivering a well-structured and practice-oriented cybersecurity portfolio covering ICT foundations, network and systems security, ethical hacking, and information security management. Courses such as *Information Security Management* and *Enterprise Security and Practitioners* are demonstrating strong alignment with industry practices and applied learning approaches. LAU is already integrating hands-on laboratories, project-based work and working-life cooperation into its programmes. However, the pre-existing offer is remaining largely general in scope, with limited sector-specific differentiation and without a modular short-course architecture explicitly designed for flexible upskilling across critical domains.

CyberSecPro is significantly expanding and deepening LAU's cybersecurity ecosystem. Through newly developed modules, LAU is introducing structured sector-focused content in energy, maritime and health, for example, in *Cybersecurity Essentials and Management for Energy Sector (CSP001_C_E)* and *Penetration Testing in the Health Sector (CSP010_W_H)*. At the same time, CyberSecPro is strengthening the human-centric dimension of cybersecurity, as reflected in *Human Factors and Cybersecurity Energy (CSP002_S_E)* and *Social Engineering and Human Factors (CSP002_S)*. These modules complement LAU's existing technical strength by embedding behavioural, organisational and domain-specific risk perspectives into cybersecurity education. As a result, LAU is evolving from offering general cybersecurity education to delivering targeted competence development aligned with European critical infrastructure priorities.

CyberSecPro is also enabling structural flexibility through modularisation and integration. Several workshops and technical modules, such as Nmap and Nessus training, can be embedded into existing courses like *Offensive Security and Ethical Hacking*, while content from *Cybersecurity in Emerging Technologies (CSP007_S_H)* can be integrated into *Cybersecurity Technologies*. In parallel, selected modules can be prepared for standalone delivery, MOOC development and inclusion in LAU's professional training catalogue. Through this approach, LAU is aiming to sustain project results within accredited curricula while simultaneously expanding lifelong learning and executive education pathways.

At institutional level, CyberSecPro is strengthening LAU's strategic positioning and future programme development. LAU will be using the newly developed sector-specific modules as building blocks for expanding postgraduate education and is preparing the ground for potential new degree pathways. Cross-departmental collaboration is increasing, and cybersecurity education is becoming more coherent, specialised and future-oriented. Exploitation activities will ensure that CyberSecPro results will be embedded into formal structures and will continue beyond the funding period.

Within LAU's surrounding educational and economic ecosystem, CyberSecPro is generating targeted and lasting impact. Regional companies, public authorities and critical sector stakeholders connected to LAU will be gaining access to updated training formats such as *Cybersecurity Essentials and Management for Maritime (CSP001_W_M)* and *Risk Management and Risk Assessment (CSP003_S_H)*. Learners will acquire sector-relevant and practice-oriented skills, while employers will benefit from graduates and professionals who understand both technical and contextual cybersecurity challenges. By sustaining modules in degree programmes, MOOCs and professional training, LAU will continuously strengthen the competence base of its stakeholder network.

In conclusion, CyberSecPro will be used to transform LAU's cybersecurity offer from a strong general foundation into a specialised, modular and strategically scalable education ecosystem. Through ongoing exploitation and integration, LAU will ensure that CyberSecPro outcomes are persisting structurally and are continuously generating value for learners, employers and regional partners.

3.2 Tallin University of Technology (TalTech)

3.2.1 Presentation of organisation/unit

Tallinn University of Technology (TalTech) was founded in 1918 by the Estonian Engineering Society and is the sole technological university in Estonia, serving as the flagship institution for engineering and technology education in the country. Located in Estonia's capital city of Tallinn, TalTech enrols approximately 10,000 students, including over 1,700 international students from 100 countries, making it Estonia's most international university. The university offers over 30 degree programs in English across engineering, information technology, business, maritime studies, and natural sciences, with a particular focus on challenge-based learning and practical application. TalTech produces two-thirds of Estonia's IT professionals and maintains strong industry connections through its modern campus, which hosts over 50 high-tech companies including Skype and Starship Technologies. As a member of the EuroTeQ Engineering University alliance alongside leading European technical universities, TalTech engages in cutting-edge research focused on smart environments, cybersecurity, artificial intelligence,

and autonomous systems, while maintaining an active role in Estonia's digital innovation ecosystem and European Digital Innovation Hub initiatives.

3.2.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Introduction to Cybersecurity *Estonian Maritime Academy*	Graduate, Spring	6	Overview of cyber security concepts and terminology; cyber risks and threats to ships, organisations, and individuals; maritime sector cyber security guidelines; information society threats; cyber hygiene best practices; ethical aspects of cyber security.
Strategic Communications and Cybersecurity *IT – Department of Software Science*	Graduate, Spring	6	Cyberspace as a NATO operational domain; strategic communications, information operations, and influence activities; power projection and audience behaviour influence; hybrid warfare and asymmetric operations in the grey zone; cyber security strategy and policy development and implementation.
Cyber Incident Handling *IT – Department of Software Science*	Graduate, Autumn	6	Security Operations Centre (SOC) foundations; incident triage and response; incident handling procedures and testing; large-scale incident management; law enforcement cooperation; evidence preservation and chain of custody; tabletop exercises for capability development.
CyberDefense Monitoring Solutions *IT – Department of Software Science*	Graduate, Autumn	6	Log and event generation for firewalls, IDS/IPS, services, and applications; syslog standards (BSD, IETF) and UNIX logging tools (syslogd, rsyslog, syslog-ng); regular expressions for log monitoring; event correlation principles and techniques; network-based intrusion detection and prevention using Snort.

Table 3: TalTech pre-CSP educational offer

Summary of pre-CSP offering

TalTech offers a distinctive graduate-level educational portfolio in cybersecurity, delivered through two departments: the Estonian Maritime Academy and the Department of Software Science. The offering

reflects Estonia's strategic position in European cybersecurity and combines technical depth with strategic and operational perspectives, including a unique sectoral focus on maritime cybersecurity.

A notable feature of TalTech's portfolio is the Introduction to Cybersecurity course delivered by the Estonian Maritime Academy, which addresses cyber threats specific to the maritime sector. This course covers general cybersecurity concepts and terminology alongside maritime-specific risks, guidelines, and regulations, reflecting the growing importance of cybersecurity in critical infrastructure sectors. Students gain an understanding of cyber hygiene best practices and ethical considerations, with applicability to both ships and shore-based organisations.

The Department of Software Science contributes three courses that address cybersecurity from strategic, operational, and technical perspectives. The Strategic Communications and Cybersecurity course takes a distinctive approach by situating cybersecurity within the broader context of information warfare, North Atlantic Treaty Organization (NATO) operations, and national strategy. Students explore cyberspace as an operational domain, examining strategic communications, information operations, influence activities, hybrid warfare, and the grey zone of conflict. This course explicitly connects technical cybersecurity skills to policy development and strategic decision-making.

Operational capabilities are developed through the Cyber Incident Handling course, which provides foundational knowledge for SOC work. Students learn incident triage and response, procedure development and testing, large-scale incident management, and critically, cooperation with law enforcement agencies including evidence preservation and chain of custody requirements. The emphasis on tabletop exercises reflects best practices in developing organisational incident response capabilities.

Technical depth is provided by the CyberDefense Monitoring Solutions course, which focuses on practical monitoring infrastructure. Students gain hands-on experience with log collection standards, UNIX logging tools (syslogd, rsyslog, syslog-ng), firewall packet filtering, and event correlation techniques. The course includes practical work with network-based intrusion detection and prevention systems, particularly Snort, and emphasises the use of regular expressions for effective log analysis.

Overall, TalTech's offering demonstrates a well-integrated approach that spans strategic, operational, and technical dimensions of cybersecurity. The portfolio is distinguished by its inclusion of maritime sector cybersecurity, its explicit connection between technical skills and national strategy, and its strong emphasis on incident response and law enforcement cooperation. All courses carry 6 ECTS and are delivered at graduate level, with instruction primarily in English, positioning TalTech as an accessible option for international students seeking advanced cybersecurity education.

3.2.3 CSP offer and exploitation plan

The following table presents TalTech’s implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Human Aspect of Energy Cybersecurity CSP002_S_E Energy Basic	This workshop navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations.	Content is integrated into current courses
Penetration Testing in the Health Sector CSP010_W_H	This workshop focused on penetration testing and red teaming, where students are not only taught but also provided with a demo in performing a variety of realistic attacks. The course provides in-depth knowledge of red teaming methodologies and	Content is integrated into current courses

Name	Description	Exploitation plan
Health Advanced	techniques, empowering students to simulate real-world cyber-attacks against background healthcare infrastructure	
Cybersecurity Essentials and Management CSP001_W General Basic	This workshop equips participants with the fundamental knowledge and best practices to safeguard your online business operations against evolving cyber threats. Through this introduction, we set the stage for the crucial role of cybersecurity in the dynamic and rapidly expanding world of e-commerce.	Content is integrated into current courses
Human Factors in Maritime Cybersecurity CSP002_S_M Maritime Basic	This seminar navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations.	Content is integrated into current courses
Cybersecurity for the Critical Sectors in Europe CSP001_S_M Maritime Advanced	This intensive training equips professionals with the knowledge and strategies to safeguard Europe's vital sectors from escalating cyber threats. By delving into the complex interplay of technology, policy, and human factors, participants develop a comprehensive understanding of critical infrastructure's cybersecurity challenges and learn to implement robust defence mechanisms.	Content is integrated into current courses
Social Engineering and Human Factors CSP002_S General Basic	The seminar covers human-centred cybersecurity risks, manipulation techniques, behavioural vulnerabilities, and strategies to strengthen organisational awareness and resilience.	Content is integrated into current courses
Foundations of networking and systems security CSP004_S General Advanced	In the modern digital landscape, understanding the fundamentals of networking and systems security is crucial for individuals and organisations alike. It is not just about keeping your personal devices secure but also about protecting sensitive data and ensuring the reliable operation of critical systems. This CyberSecPro training examines the systems security associated with a business aspect.	-
Human Factors and Cybersecurity Energy	This course dives deep into the human elements of cybersecurity, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants gain insights	Content is integrated into current courses

Name	Description	Exploitation plan
CSP002_S_E Energy Basic	into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations.	
Human Aspects of Cybersecurity: Social Engineering, Personality, and Vulnerability CSP002_S_M Maritime Advanced	This course dives deep into the human elements of cybersecurity, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants gain insights into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations.	Content is integrated into current courses We will continue offering it in IPICS
The weaponization of OSINT in Maritime CSP002_S_M Maritime Basic	This course explores the tactical and strategic use of open-source intelligence within the context of maritime cybersecurity. Learners investigate how OSINT can be leveraged for data collection, threat identification, and vulnerability analysis specific to maritime operations. Emphasis is placed on understanding threat actors, legal implications, AI-driven OSINT tools, and mitigation strategies.	Content is integrated into current courses We will continue offering it in IPICS
Human Aspects of Maritime Cybersecurity CSP002_S_M Maritime Basic	As a part of the CyberSecPro project, this seminar on Human Factors in Cybersecurity examines the psychological, social, and organisational influences on security-related behaviour and decision-making.	Content is integrated into current courses
Human-AI Interactions in Cybersecurity CSP002_S General Basic	This 90-minute workshop explores the intersection of human factors and artificial intelligence in cybersecurity contexts. Participants examine how humans interact with AI-driven security tools, the cognitive and behavioural challenges that arise, and the implications for trust, decision-making, and accountability.	Content is integrated into current courses
Information and Deception CSP002_S General Basic	This workshop examines how psychological safety and information disorder intersect, using behavioural science and psychology as the lens. In an era where misinformation, disinformation, and psychological manipulation spread rapidly—especially through the Internet and AI—Western democracies face growing challenges to public trust in democratic institutions, as highlighted by the World Economic Forum.	Content is integrated into current courses

Table 4: TalTech offer and exploitation plan

3.2.4 Summary

Before CyberSecPro, TalTech was already offering a strong and well-structured graduate-level cybersecurity portfolio, primarily embedded in the Department of Software Science and the Estonian Maritime Academy. Courses such as *Introduction to Cybersecurity*, *Cyber Incident Handling*, and *CyberDefense Monitoring Solutions* were providing technical depth, operational capability development, and strategic contextualisation, including a distinctive maritime perspective. The pre-existing offer was therefore technically robust and strategically aligned with Estonia's digital ecosystem. However, the focus was predominantly on technical infrastructures, incident response, and strategic communications, with comparatively less structured attention to cross-sectoral human factors, AI-related behavioural implications, and domain-specific specialisations beyond maritime.

Through CyberSecPro, TalTech is significantly expanding and diversifying this portfolio by introducing targeted modules that deepen sectoral, behavioural, and interdisciplinary dimensions. New developments such as *Human Aspect of Energy Cybersecurity (CSP002_S_E)*, *Penetration Testing in the Health Sector (CSP010_W_H)*, *Cybersecurity for the Critical Sectors in Europe (CSP001_S_M)*, and *Human-AI Interactions in Cybersecurity (CSP002_S)* are bringing structured attention to energy, health, AI-driven systems, and European critical infrastructure protection. At the same time, specialised maritime modules such as *The Weaponization of OSINT in Maritime (CSP002_S_M)* and *Human Aspects of Maritime Cybersecurity (CSP002_S_M)* are reinforcing TalTech's established maritime expertise with new perspectives on intelligence, human vulnerability, and advanced threat analysis. CyberSecPro is therefore broadening TalTech's cybersecurity offer from a technically strong base towards a more holistic, sector-integrated and human-centred model.

In terms of exploitation, TalTech is actively planning to integrate the majority of CyberSecPro modules into existing courses, ensuring that new content is not isolated but embedded within sustainable curricular structures. Selected advanced maritime modules are continuing within IPICS, thereby institutionalising the innovation beyond project duration. This approach means that CyberSecPro outputs are not remaining as stand-alone workshops but will be continuously delivered, adapted, and scaled within TalTech's formal graduate education. Exploitation at TalTech is thus ensuring that CyberSecPro developments are becoming structurally anchored within degree programmes and specialised training formats.

The institutional impact is visible in the way TalTech is strengthening its position as a cross-sector cybersecurity hub, linking technical excellence with behavioural science, AI interaction, OSINT, and sector-specific resilience. CyberSecPro is enhancing TalTech's internal collaboration between maritime, IT, and interdisciplinary experts while reinforcing its alignment with European priorities on critical infrastructure protection and human-centric cybersecurity. TalTech is thereby expanding both its thematic scope and pedagogical depth.

Regarding the educational landscape, the impact is extending beyond TalTech itself. By continuously offering CyberSecPro-derived modules to graduate students, professionals, and sector-specific audiences, TalTech is contributing to a more resilient cybersecurity skills ecosystem around TalTech, including maritime operators, energy providers, healthcare institutions, public authorities, and high-tech companies located on campus. CyberSecPro is therefore strengthening the long-term availability of sector-aware, human-centred and AI-informed cybersecurity education that is directly benefiting learners and regional employers connected to TalTech.

3.3 University of Cyprus (UCY)

3.3.1 Presentation of organisation/unit

The University of Cyprus (UCY) was established in 1989 in Nicosia, the capital of Cyprus, and admitted its first students in 1992, growing to serve approximately 7,000 students across eight faculties and 22 departments. As Cyprus's leading research university, UCY ranks 452nd globally in the 2026 QS World University Rankings and operates 13 research centres, including three Centres of Excellence, while employing approximately 700 young scientists through external research funding. The university offers

internationally recognised degree programs based on ECTS across humanities, engineering, natural sciences, business, and social sciences, with teaching primarily conducted in Greek but with numerous programs available in English. UCY maintains an extensive international network as a member of the Young Universities for the Future of Europe (YUFE) alliance and participates in over 730 Erasmus bilateral agreements, having facilitated the exchange of more than 4,600 students since 1998. The university's state-of-the-art infrastructure includes the Stelios Ioannou Learning Resource Centre designed by Jean Nouvel, providing access to over 700,000 print and electronic book titles and extensive digital research resources.

3.3.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
System Security *Computer Science*	Undergraduate (Mandatory)	7.5	Broad introduction to systems security; applied cryptography; software vulnerabilities and memory errors; attacks and defences; mobile security; web security; network security; privacy and anonymity.
Software Analysis *Computer Science*	Undergraduate (Optional)	7.5	Fundamental concepts in software analysis; debugging, profiling, and instrumentation; binary analysis and rewriting; source-level analysis of C/C++ programs; compiler toolchain extension using LLVM.
Data Security *Computer Science*	Graduate	8	Data security fundamentals; applied cryptographic primitives and protocols for secure data transmission; system attacks and protection mechanisms; advanced attacks and defences for machine learning-based systems.

Table 5: UCY pre-CSP educational offer

Summary of pre-CSP offering

UCY offers a focused educational portfolio in cybersecurity delivered through the Computer Science Department. The offering spans undergraduate and graduate levels, with a distinctive emphasis on systems-level security and software analysis that reflects a strong research-informed approach to security education.

UCY offers a comprehensive cybersecurity curriculum spanning undergraduate and graduate levels, combining strong foundational knowledge with advanced technical specialization in systems, software, and data security. The programme equips students with both core security competencies and cutting-edge expertise, including secure system design, low-level analysis, and protection of machine learning-based systems.

Overall, UCY's offering demonstrates a coherent and technically rigorous approach to security education. The portfolio is distinguished by its systems-level focus, emphasis on low-level software analysis and binary techniques, and integration of emerging topics such as Machine Learning security.

The higher ECTS weighting compared to typical European courses highlights the substantial depth and practical engagement. While the offering is smaller in scope than most peer institutions, it provides a focused pathway for students seeking deep technical expertise in systems security and software analysis.

3.3.3 CSP offer and exploitation plan

The following table presents UCY's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Mechanics for Memory Corruption CSP009_S_E Energy Basic	This seminar provides an overview of how memory-corruption vulnerabilities work and are managed. This seminar provides an overview of how native software works, how simple bugs can be used to execute an attacker's code, and how such bugs are managed.	Content is integrated into current courses
Protecting Charging Stations Against Specific Threats CSP008_S_E Energy Advanced	The seminar provides a brief overview of the main issues being addressed in the energy field, and particularly in the area of Electric Charging Stations. This module belongs to the CPS008_S_E CSP module, which is focused on "Protecting Charging Stations Against Specific Threats."	Content is integrated into current courses

Table 6: UCY offer and exploitation plan

3.3.4 Summary

Prior to CyberSecPro, UCY was offering a focused cybersecurity portfolio anchored in systems security and software analysis, including core courses such as *System Security* and *Data Security*. These courses were already ensuring strong foundations in applied cryptography, vulnerability analysis, and emerging topics such as machine learning security. However, the portfolio was primarily structured around full-semester academic courses and did not explicitly address certain sector-specific or vulnerability-focused topics in a modular and targeted format.

Through CyberSecPro, UCY is expanding and deepening this foundation by developing and implementing specialised seminar modules, *Mechanics for Memory Corruption (CSP009_S_E)* and *Protecting Charging Stations Against Specific Threats (CSP008_S_E)*. These modules are bringing highly focused, application-oriented expertise into the curriculum, addressing concrete attack vectors and sector-specific cybersecurity challenges, particularly in the energy domain. By integrating this content into existing courses, UCY is ensuring that the new knowledge is not remaining isolated but is becoming structurally embedded within the Computer Science curriculum.

In terms of exploitation, UCY is actively embedding the CyberSecPro modules into its established courses, thereby ensuring long-term curricular sustainability. Rather than remaining stand-alone pilot activities, the developed materials will continuously be used, updated, and delivered within mandatory and elective courses. This approach will ensure that the knowledge generated through CyberSecPro is becoming part of UCY's standard educational offer and is continuously reaching new cohorts of students. Exploitation is therefore realised through curricular integration and long-term academic ownership.

At institutional level, CyberSecPro is strengthening UCY's capacity to deliver domain-specific and vulnerability-driven cybersecurity education. The project is reinforcing UCY's profile in systems-level security while extending its expertise into energy-related cybersecurity threats. This is enhancing

academic depth, enriching teaching content with cutting-edge and sector-relevant material, and further aligning research-informed teaching with real-world threat landscapes.

At the level of the educational landscape, UCY is contributing to a more specialised and industry-relevant cybersecurity offer within its ecosystem. By integrating content on memory corruption mechanics and electric charging station security, UCY is directly benefiting its surrounding stakeholders, including energy operators, technology companies, public authorities, and cybersecurity professionals. The sustained integration of these modules ensures that graduates entering the labour market are equipped with concrete, up-to-date competencies that respond to evolving sectoral risks. CyberSecPro is therefore not only strengthening UCY's internal curriculum, but is also continuously enriching the cybersecurity capacity of its regional and European stakeholder community.

3.4 Universidad de Malaga (UMA)

3.4.1 Presentation of organisation/unit

University of Málaga (UMA) was established in 1972 in southern Spain through the consolidation of existing educational institutions dating back to the 16th century, including the Seminary (1587) and the Normal School (1846). The university serves more than 39,000 students across two main campuses in Málaga, offering 65 undergraduate degrees, 64 master's programs, and 21 doctoral programs through 24 centres and 81 departments staffed by approximately 2,400 faculty members. UMA is ranked 23rd among Spanish universities and maintains a strong focus on innovation and internationalisation, participating actively in Erasmus and other international exchange programs that enhance global mobility and collaboration. The university has developed substantial research capacity through partnerships with the private sector and participation in European Union-funded projects, with particular strengths in engineering, health sciences, computer science, and humanities. UMA staff have considerable experience in international cooperation, contributing with academic excellence, strong connections to industry and the productive sector.

3.4.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Foundations of Cybersecurity *Computer Science – BSc. in Cybersecurity and Artificial Intelligence*	Undergraduate, Semester 1	6	Core cybersecurity concepts and principles; security threats, risks, and services; regulations and standards; classical, symmetric, and asymmetric cryptography; authentication and key exchange protocols; TCP/IP security and internet security mechanisms.
Digital Identity and Privacy *Computer Science – BSc. in Cybersecurity and Artificial Intelligence*	Undergraduate, Semester 2	6	Authentication mechanisms and access control policies; PKI and self-sovereign identity; identity protocols for the web; privacy-enhancing technologies; data privacy and anonymisation mechanisms.
Information Security *Computer Science – BSc. in Computer Science / Double*	Undergraduate, Semester 5/7	6	Security and privacy in computer and communications environments; symmetric and asymmetric

Degree in Computer Science and Mathematics			cryptography, hash and MAC functions; key management and access control; e-mail security and electronic payments; TCP/IP network security and wireless network security.
Security in Services and Applications *Languages and Computer Science*	Undergraduate, Semester 2	6	Security in software development and internet application deployment; threat and vulnerability identification; risk management; security requirements elicitation; SSL/TLS; web access control and identity management; web vulnerabilities and attacks; OS security.
Information Security and Computer Forensics *Computer Science – BSc. in Criminology*	Undergraduate, Semester 7	6	Cybersecurity for criminology students; cybercrimes and information security fundamentals; applied cryptography and security services; end-user security; forensic investigation; anti-forensic mechanisms; operating system forensic analysis.
Design and Configuration of Secure Networked Systems *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 1	6	Network security foundations; sources and motives of cybersecurity threats; network perimeter and protocols; switches, routers, and wireless hardening; firewall configuration; IDS/IPS and honeypots; OS hardening (Linux/Windows); SIEM systems and SOC operations.
Security and Privacy in Application Environments *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 2	4.5	Security and privacy in IoT and cloud scenarios; end-to-end encryption; cloud data security and anonymisation; online tracking and fingerprinting; HTTP security headers and certificate transparency; SSL/TLS vulnerabilities; web input validation; cryptographic primitives for privacy-enhancing technologies.
Security in Industrial and Cyber-Physical Systems *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 3	4.5	CPS security and privacy; Industrial IoT and cloud computing integration; smart infrastructures (industries, cities, homes, healthcare); threat taxonomy; secure primitives and communication channels; authentication and access control; trust, privacy, attack prevention and detection.

Malware Analysis *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 3	4.5	Malware analysis techniques and malware types; sandboxes and controlled environments; static analysis (hashing, strings, packed/obfuscated malware, PE format); dynamic analysis (monitoring, API tracing); advanced static analysis (Windows internals, reverse engineering); debugging.
Computer Forensics *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 3	4.5	Digital forensics fundamentals and international standards; anti-forensics; digital evidence identification, gathering, analysis, and presentation; tools and procedures for evidence collection and analysis; complete forensic use case.
Secure Coding *Computer Science – MSc. in Computer Engineering (Cybersecurity specialisation)*	Graduate, Semester 3	4.5	Security models, threats, and design principles; secure coding practices to minimise vulnerabilities; application security for Linux and Windows; static analysis; web security; mobile security; machine learning security.

Table 7: UMA pre-CSP educational offer

Summary of pre-CSP offering

UMA offers a comprehensive and well-structured educational portfolio in cybersecurity, delivered primarily through the Computer Science Department. The offering spans undergraduate and graduate levels, demonstrating strong vertical integration from foundational concepts to advanced specialisation, and notable horizontal breadth across technical, applied, and interdisciplinary domains.

At undergraduate level, UMA delivers cybersecurity education through both a dedicated BSc. in Cybersecurity and Artificial Intelligence and integrated courses within Computer Science, Mathematics, and Criminology programmes, covering foundations such as cryptography, network security, digital identity, secure software development, and computer forensics. At graduate level, the MSc. in Computer Engineering (Cybersecurity specialisation) provides a structured three-semester pathway progressing from secure network design and SOC operations to application, cloud, and IoT security, culminating in advanced specialisation in industrial and cyber-physical systems security, malware analysis, computer forensics, and secure coding across modern platforms.

A distinctive strength of UMA's offering is its strong applied orientation, evidenced by extensive use of industry-standard tools across all courses. Students gain hands-on experience with network simulation (GNS3), vulnerability assessment (Nmap, OpenVAS, Nessus), penetration testing (Kali Linux, Metasploit), malware analysis (REMNUX, IDA Pro), forensics (Autopsy, Volatility, FTK Imager), and secure development tools (OWASP ZAP, SonarQube). This practical emphasis ensures graduates are prepared for immediate professional engagement.

Overall, UMA's cybersecurity portfolio demonstrates a mature and comprehensive approach, combining strong cryptographic and network security foundations with advanced topics in CPS security, malware analysis, forensics, and secure development. The integration of cybersecurity across multiple degree programmes, including the interdisciplinary criminology offering, reflects a broad institutional commitment to cybersecurity education and prepares graduates for diverse professional and research pathways.

3.4.3 CSP offer and exploitation plan

The following table presents UMA's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
«ModuleName» (v001-v003) CSP003_S_E Energy Basic	This seminar provides a set of terms and concepts associated with cybersecurity risk management and its associated assessment, specifically applied to the energy sector. Within risk assessment, various topics are covered such as: risk identification in the energy sector considering assets, threats, and vulnerabilities; risk analysis and its associated methods; and risk evaluation.	Content might be integrated (partially or totally) or adapted into the existing courses, such as "Foundations of Cybersecurity", "Malware Analysis", "Secure Coding", and others related, if applicable.
Network Protection for Energy Control Systems (v001- v003) CSP004_C_E Energy Advanced	This seminar provides a clear understanding of the threats in power control networks to subsequently understand the main security weaknesses of TCP/IP protocols and their impact on critical communication networks.	Content might be integrated (partially or totally) or adapted into the existing courses, such as "Design and Configuration of Secure Networked Systems" and others related, if applicable.
Cybersecurity Essentials and Management for Energy Sector (v005) CSP001_C_E Energy Basic	This course provides a brief overview of the issues and measures being addressed in the energy sector.	Content might be integrated (partially or totally) or adapted into the existing courses. such as "Foundations of Cybersecurity", "Information Security", "Security in Services and Applications", and others related, if applicable.
Introduction to the Cybersecurity in Electric Charging Stations CSP008_S_E Energy	The seminar provides a brief overview of the main issues being addressed in the energy field, and particularly in the area of Electric Charging Stations. This module belongs to the CPS008_S_E CSP module, which is focused on the "Protecting Charging Stations Against Specific Threats".	Content might be integrated (partially or totally) or adapted into the existing courses, such as "Security in Industrial and Cyber-Physical

Name	Description	Exploitation plan
Advanced		Systems" and others related, if applicable.
Protecting Charging Stations Against Specific Threats CSP008_S_E Energy Advanced	This lecture provides an overview of cybersecurity challenges associated with electric vehicle charging infrastructures. It introduces a generic taxonomy of threats affecting these systems and delves into common cybersecurity risks specific to EV charging applications.	Content might be integrated (partially or totally) or adapted into the existing courses, such as "Security in Industrial and Cyber-Physical Systems" and others related, if applicable.

Table 8: UMA offer and exploitation plan

3.4.4 Summary

Before CyberSecPro, UMA was already offering a mature, vertically integrated cybersecurity portfolio, spanning undergraduate to graduate levels and covering foundations, network security, malware analysis, digital forensics, secure coding, and cyber-physical systems. Courses such as *Foundations of Cybersecurity*, *Information Security*, and *Security in Industrial and Cyber-Physical Systems* ensured strong theoretical and applied competencies. This pre-existing structure was demonstrating UMA's institutional commitment to cybersecurity education and its strong alignment with industry needs.

Through CyberSecPro, UMA is introducing a strategic sectoral extension of its cybersecurity expertise into the energy domain, with particular focus on critical infrastructures and electric charging ecosystems. The newly developed modules, including *Cybersecurity Risk Assessment and Management for Energy Sector (CSP003_S_E)*, *Network Protection for Energy Control Systems (CSP004_C_E)*, and *Protecting Charging Stations Against Specific Threats (CSP008_S_E)*, are bringing targeted knowledge on energy-sector risk modelling, TCP/IP vulnerabilities in power control networks, and EV charging station threat taxonomies. These modules are not standing in isolation; UMA intends to actively integrate and adapt their content into established courses such as *Design and Configuration of Secure Networked Systems* and *Security in Industrial and Cyber-Physical Systems*, thereby embedding CyberSecPro results structurally into the curriculum.

From an exploitation perspective, UMA is systematically mainstreaming CyberSecPro outputs into its accredited degree programmes, ensuring long-term sustainability beyond the project lifetime. By partially or fully integrating CSP modules into both undergraduate and MSc. courses, UMA aims to transform project-based innovation into permanent curricular assets. The energy-focused risk assessment content is enriching foundational modules (e.g., *Foundations of Cybersecurity*), while advanced energy network protection components are reinforcing specialised MSc. tracks. In doing so, UMA is ensuring that CyberSecPro materials are continuously used, updated, and delivered to new student cohorts.

The institutional impact of CyberSecPro at UMA is reflected in the expansion of sector-specific cybersecurity capacity, particularly in relation to critical energy infrastructures and smart mobility systems. CyberSecPro is strengthening UMA's positioning at the intersection of cybersecurity, industrial systems, and sustainable energy transformation. This is enhancing UMA's academic profile while reinforcing its applied orientation and collaboration potential with the productive sector.

At the level of the educational landscape, UMA is contributing to a more specialised and industry-relevant cybersecurity offer for regional and national stakeholders. By embedding energy-sector

cybersecurity into its mainstream programmes, UMA is equipping graduates with competences directly relevant to energy providers, smart grid operators, EV infrastructure companies, and public authorities in the Málaga ecosystem. This sustained offer will benefit learners through enhanced employability and support employers around UMA with professionals trained in energy-specific cyber risk management and protection strategies. In this way, CyberSecPro is generating a durable impact while UMA is actively continuing exploitation of its results.

3.5 University of Novi Sad Faculty of Sciences (UNSPMF)

3.5.1 Presentation of organisation/unit

The University of Novi Sad Faculty of Sciences (UNSPMF) is a comprehensive educational and scientific institution that conducts teaching and research across biology, ecology, chemistry, biochemistry, environmental protection, physics, astronomy, computer science, mathematics, geography, geoscience, and tourism. Established as part of the University of Novi Sad, which was founded in 1960 as Serbia's second public university, the Faculty of Sciences serves approximately 6,000 students at bachelor, master, and doctoral levels across five academic departments staffed by over 600 employees, including 400 teaching and research personnel. The faculty operates teaching and scientific activities in six lecture halls, 65 classrooms, and more than 70 well-equipped research laboratories spanning over 23,000 m², with some distinguished professors holding membership in the Serbian Academy of Sciences and Arts and Vojvodina Academy of Sciences and Arts. The faculty's mission emphasises creating state-of-the-art knowledge through education and research, safeguarding research integrity, facilitating staff career development, and attracting external funding to achieve full integration into the European Research and Higher Education Area. Faculty staff have extensive experience in international collaboration through numerous national and international research projects, academic mobility programs, and strategic partnerships focused on capacity building, interactive networking, and visibility on a global scale.

3.5.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Development of Information Systems *Department of Mathematics and Informatics*	Undergraduate, Semester 5	7	Multi-layer web application development using Spring Boot framework; Spring MVC, Spring Data, and Spring Security modules; authentication, authorisation, and JWT implementation.
Computer Networks *Department of Mathematics and Informatics*	Undergraduate, Semester 6	6	Introduction to computer networks; OSI reference model; TCP/IP stack; Linux and Windows network management tools.
Deep Learning *Department of Mathematics and Informatics*	Graduate, Semester 1	6	Introductory deep learning course; deep neural networks, gradient descent, and backpropagation; convolutional and recurrent models; autoencoders; data preprocessing techniques.

Distributed Deep Learning *Department of Mathematics and Informatics*	Graduate, Semester 2	5	Advanced deep learning with HPC focus; distributed training and optimisations; TinyML; SLURM cluster management; Linux and HPC management tools.
Distributed Optimisation with Applications *Department of Mathematics and Informatics*	Graduate, Semester 2	6	Algorithm design and convergence analysis for convex distributed optimisation and learning; gradient-based and alternating direction-based methods.

Table 9: UNSPMF pre-CSP educational offer

Summary of pre-CSP offering

UNSPMF, through its Faculty of Sciences and the Department of Mathematics and Informatics, offers a portfolio of courses that provide foundational and adjacent competencies relevant to cybersecurity education. While the offering does not include dedicated cybersecurity courses, it provides essential technical foundations in secure application development, networking, and machine learning that underpin modern security practice.

At undergraduate level, the curriculum combines secure web application development, emphasizing security-by-design principles such as authentication, authorisation, and JWT implementation, with foundational networking knowledge covering OSI, TCP/IP, and practical system administration skills. At graduate level, the focus shifts to advanced deep learning, distributed computing, and distributed optimisation, equipping students with expertise relevant to AI-driven cybersecurity applications, high-performance and edge deployment environments, and privacy-preserving data processing approaches such as federated learning.

Overall, UNSPMF's offering provides complementary technical competencies that support cybersecurity education rather than dedicated security instruction. The emphasis on secure development practices (Spring Security), networking fundamentals, and machine learning techniques positions students to apply these skills in security contexts. The portfolio would benefit from dedicated cybersecurity courses to provide explicit coverage of security concepts, threat modelling, and defence mechanisms. However, the existing courses provide a solid technical foundation upon which security specialisation can be built.

3.5.3 CSP offer and exploitation plan

The following table presents UNSPMF's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Practical Insights in Anomaly Detection CSP007_S_H Health Basic	This training module provides 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.	UNSPMF will integrate this module into existing undergraduate and master's programs in data science, and artificial intelligence. The course will support curriculum modernisation by introducing practical skills related to anomaly detection in cybersecurity. It will serve as a foundation for student research projects, master's theses, and PhD research focused on AI-driven anomaly detection, security analytics, and intelligent monitoring systems. The

Name	Description	Exploitation plan
		developed tools and datasets will also support ongoing departmental research activities.
Cyber Threat Intelligence for Health CSP006_C_H Health Basic	Comprehensive exploration of the core principles and practical applications of cyber threat intelligence. It equips students with a deep understanding of threat identification, threat actor analysis, and motives. The module emphasises hands-on training with industry-standard tools,	Course materials, case studies, and practical exercises developed within the project will be reused in regular academic teaching. The UNSPMF will promote the module through collaborations with industry partners, cybersecurity training centres, and public institutions to provide workforce upskilling in threat intelligence analysis and cyber threat monitoring.
LLM vulnerabilities CSP007_W General Basic	This module explores security vulnerabilities specific to Large Language Models (LLMs) and AI-driven systems. Learners will learn how adversarial inputs, prompt injection, data poisoning, model extraction, and privacy leakage attacks can compromise LLM-based applications. The module covers both theoretical foundations and practical techniques for identifying, analysing, and mitigating risks in generative AI systems	The module will be integrated into artificial intelligence and data science study programs at the Faculty of Sciences, University of Novi Sad. Developed teaching materials, laboratory exercises, and case studies will support undergraduate and graduate courses.

Table 10: UNSPMF offer and exploitation plan

3.5.4 Summary

Before CyberSecPro, UNSPMF was delivering a technically strong portfolio rooted in secure software engineering, networking fundamentals, and advanced machine learning, yet without explicitly dedicated cybersecurity modules. Courses such as *Development of Information Systems* (Spring Security, JWT implementation), *Computer Networks*, and *Deep Learning* were already providing essential building blocks for secure system design and intelligent data processing. However, cybersecurity was addressed implicitly through technical enablers rather than through targeted, application-oriented security education. In this context, UNSPMF was positioning students with strong computational and analytical competencies, while the explicit connection to cyber threat analysis, anomaly detection, and AI-specific vulnerabilities was still emerging.

Through CyberSecPro, UNSPMF is transforming complementary technical strengths into explicit cybersecurity capacity. The introduction of modules such as *Practical Insights in Anomaly Detection*, *Cyber Threat Intelligence for Health*, and *LLM Vulnerabilities* is operationalising cybersecurity as a structured learning pathway embedded within data science and artificial intelligence curricula. These modules are not isolated additions; UNSPMF is integrating them directly into undergraduate and master's programmes, thereby aligning anomaly detection, threat intelligence analysis, and generative AI security with existing expertise in distributed learning and optimisation. In practical terms, UNSPMF

is embedding hands-on laboratories, real-world case studies, and applied research components into formal teaching structures, while connecting them to thesis work and doctoral research pipelines.

Exploitation is being embedded institutionally and academically. UNSPMF is sustaining the new courses by incorporating CyberSecPro materials into regular curricula, reusing laboratory environments and datasets, and linking modules to ongoing departmental research in AI-driven security analytics. The module on anomaly detection is becoming a foundation for student research projects, while the threat intelligence module is being promoted through collaboration with industry partners and public institutions. At the same time, the LLM security module is strengthening UNSPMF's strategic positioning at the intersection of artificial intelligence and cybersecurity, ensuring that emerging risks such as prompt injection or data poisoning are systematically addressed in formal education.

The impact on the educational landscape around UNSPMF is being realised through continuity and stakeholder engagement. By sustaining these CyberSecPro modules within accredited study programmes, UNSPMF is expanding the regional offer in applied cybersecurity education, particularly for stakeholders in health, AI-driven industries, public administration, and cybersecurity training centres. Learners are gaining access to practice-oriented competencies in anomaly detection and threat intelligence, while employers in the UNSPMF ecosystem are benefiting from graduates who are combining advanced machine learning expertise with explicit security awareness. In this way, UNSPMF is contributing to a more resilient regional skills base, where cybersecurity is not an add-on, but an integrated and continuously evolving component of digital education.

3.6 Instituto de Desenvolvimento de Novas Tecnologias (UNINOVA)

3.6.1 Presentation of organisation/unit

UNINOVA (Instituto de Desenvolvimento de Novas Tecnologias) is a multidisciplinary, independent, non-profit research institute founded in 1986 in the Lisbon metropolitan area by the Faculty of Sciences and Technology of NOVA University of Lisbon, industrial associations, and over 30 companies. Employing approximately 180 researchers and staff, UNINOVA comprises two main research units: CEMOP (Centre of Excellence in Microelectronics, Optoelectronics and Processes) and CTS (Centre of Technology and Systems), which together address microelectronic and optoelectronic technologies, cyber-physical engineering systems, intelligent manufacturing, and advanced materials characterisation. The institute pursues excellence in scientific research, technical development, and advanced training while working closely with industry and universities to transfer technological innovations into profitable business concepts and develop existing products to match new industrial requirements. UNINOVA has managed and participated in numerous national and international research programs, securing over €33 million in Horizon 2020 and Horizon Europe funding, with particular expertise in system interoperability, standards-based platforms, data fusion and harmonisation, and open systems integration. As an active partner of Madan Parque business facilitator and accelerator, UNINOVA staff have extensive experience in supporting entrepreneurial activity, managing EU-funded research projects across digital innovation, robotics, energy systems, and advanced manufacturing technologies.

3.6.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Strategic Leadership and Governance *Cybersecurity Executive Program*	Executive	-	Strategic understanding of cybersecurity for executives; leading cybersecurity initiatives; informed decision-making; communicating cybersecurity risks and investments to stakeholders.

Incident Response and Risk Management *Cybersecurity Executive Program*	Executive	-	Cybersecurity preparedness and response; effective incident response; crisis management; vendor and third-party risk mitigation; integrating cybersecurity into business continuity planning.
Emerging Trends and Collaboration *Cybersecurity Executive Program*	Executive	-	Emerging cybersecurity trends and technologies; ethical and legal implications; international cooperation; cyber threat intelligence; security operations; impact of emerging technologies on cybersecurity.

Table 11: UNINOVA pre-CSP educational offer

Summary of pre-CSP offering

UNINOVA offers a focused Cybersecurity Executive Program designed specifically for senior leaders and decision-makers. Unlike traditional academic programmes, this offering is structured as executive education, targeting professionals who need strategic cybersecurity competencies rather than technical implementation skills.

The programme integrates three complementary modules that equip executives with strategic, operational, and forward-looking cybersecurity leadership capabilities, covering governance and board-level decision-making, incident response oversight and risk management embedded in business continuity, and emerging trends including legal considerations, international cooperation, threat intelligence, and the security implications of new technologies.

Overall, UNINOVA's offering fills an important niche in the cybersecurity education landscape by targeting executive-level competencies rather than technical skills. The programme addresses the recognised need for cybersecurity literacy among senior leadership and board members, who must make strategic decisions about cybersecurity investments, risk acceptance, and organisational governance without necessarily possessing technical expertise. This executive focus complements the more technical offerings available at other institutions and addresses a critical gap in organisational cybersecurity capability.

3.6.3 CSP offer and exploitation plan

The following table presents the implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Foundations of networking and systems security CSP004_S General Advanced	In the modern digital landscape, understanding the fundamentals of networking and systems security is crucial for individuals and organisations alike. It is not just about keeping your personal devices secure but also about protecting sensitive data and ensuring the reliable operation of critical systems. This CyberSecPro training examines the systems security associated with a business aspect.	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a Cybersecurity Executive Program. We plan to promote the training materials for self-study.

Name	Description	Exploitation plan
Cyber Threat Intelligence in the Energy Network CSP006_C_E Energy Advanced	This training module explains the underlying properties and principles associated with cyber threats within an energy organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence.	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a Cybersecurity Executive Program. We plan to promote the training materials for self-study.
Cybersecurity in Emerging Technologies for Energy CSP007_C_E Energy Advanced	This training module explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, equipping participants with the knowledge and skills needed to protect their environments.	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a Cybersecurity Executive Program. We plan to promote the training materials for self-study.
Cybersecurity in Emerging Technologies for the Energy Network CSP007_S_E Energy Basic	This seminar explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, providing the participants with an overview of how to protect their energy environments. It introduces the learner to energy securing various technologies like the IoT, cloud computing, blockchain, and AI.	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a Cybersecurity Executive Program. We plan to promote the training materials for self-study.
Critical Energy Infrastructure Security CSP008_C_E Energy Advanced	The training module provides participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge energy technologies. As the energy business embraces innovations, this module provides a comprehensive understanding of the cybersecurity landscape within the energy context.	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a Cybersecurity Executive Program. We plan to promote the training materials for self-study.
Digital Forensics for Energy CSP012_S_E Energy	This seminar provides a set of terms and concepts associated with digital forensics, specifically applied to the energy sector. It introduces the learner to digital forensics and techniques for	We plan to discuss with NOVA FCT faculty to offer it jointly as part of a

Name	Description	Exploitation plan
Advanced	conducting forensic examinations in energy infrastructures.	Cybersecurity Executive Program. We plan to promote the training materials for self-study.

Table 12: UNINOVA offer and exploitation plan

3.6.4 Summary

UNINOVA is building on an established executive cybersecurity portfolio and is significantly expanding its scope through CyberSecPro by integrating sector-specific and technically advanced content into its offer. Prior to CyberSecPro, UNINOVA was delivering a focused Cybersecurity Executive Program structured around strategic leadership, governance, incident response, risk management, and emerging trends. This portfolio was primarily addressing decision-makers and senior leaders, equipping them with high-level competencies in modules such as *Strategic Leadership and Governance* and *Incident Response and Risk Management*. The emphasis was clearly on strategic oversight rather than domain-specific or sector-oriented technical depth.

Through CyberSecPro, UNINOVA intends to introduce a new layer of specialised and energy-focused modules that complement and strengthen the existing executive framework. New courses such as *Foundations of Networking and Systems Security (CSP004_S)*, *Cyber Threat Intelligence in the Energy Network (CSP006_C_E)* and *Critical Energy Infrastructure Security (CSP008_C_E)* can bring structured, advanced content directly linked to energy systems and emerging technologies into the portfolio. In addition, seminars such as *Cybersecurity in Emerging Technologies for the Energy Network (CSP007_S_E)* and *Digital Forensics for Energy (CSP012_S_E)* can broaden the thematic range and create a bridge between strategic leadership and operational cybersecurity in critical sectors.

UNINOVA aims to exploit CyberSecPro results by integrating the new modules into the Cybersecurity Executive Program and by promoting them as stand-alone and self-study learning opportunities. By discussing joint delivery with NOVA FCT and embedding the CyberSecPro modules into the executive framework, UNINOVA is ensuring institutional anchoring and academic recognition. At the same time, promoting training materials for self-study is increasing flexibility and accessibility, thus extending the reach beyond traditional classroom-based executive education. This dual exploitation pathway is strengthening UNINOVA's long-term capacity to offer both structured executive programmes and modular, scalable learning formats.

At institutional level, CyberSecPro is expanding UNINOVA's educational profile from a strategic executive focus towards a sector-specific, technically informed, and innovation-driven cybersecurity portfolio. The integration of energy-oriented content aligns strongly with UNINOVA's research expertise in cyber-physical systems, intelligent manufacturing and energy systems, thereby reinforcing coherence between research, innovation and advanced training. As a result, UNINOVA is strengthening its positioning as a bridge between research excellence and applied executive education.

Regarding the broader educational landscape, UNINOVA is contributing to a more specialised and industry-aligned cybersecurity offer for stakeholders in the energy and industrial ecosystem. By sustaining the new CyberSecPro modules, UNINOVA will continuously benefit regional energy operators, technology providers, industrial partners, and executive learners connected to its innovation network. The persistent availability of courses such as *Cyber Threat Intelligence in the Energy Network* and *Digital Forensics for Energy* will increase the cybersecurity maturity of organisations within UNINOVA's ecosystem and support employers in addressing sector-specific cyber risks. In this way, CyberSecPro is not only strengthening UNINOVA's internal capacity, but is actively shaping a more resilient and competence-driven cybersecurity training landscape around UNINOVA.

3.7 University of Piraeus Research Centre (UPRC)

3.7.1 Presentation of organisation/unit

The University of Piraeus Research Centre (UPRC) was founded in 1989 as an independent legal entity within the University of Piraeus to provide administrative and legal support for basic and applied research conducted by university staff in national and international contexts. Located in Piraeus, Greece, UPRC facilitates research activities across multiple departments, with particular strength in the Department of Digital Systems, which has actively coordinated significant numbers of EU-funded R&D projects, national projects funded by the Greek Ministry of Development and General Secretariat of Research and Technology, and collaborative projects with international and national enterprises. Since its inception, UPRC has completed over 1,000 research projects, educational programs, and development initiatives encompassing basic and applied research, postgraduate programs, infrastructure development, continuing training, conferences, and student internships. The centre focuses on research areas including healthcare information systems, electronic health records, cybersecurity, cloud computing, Internet of Things, energy efficiency in buildings, maritime security, supply chain management, and advanced distributed computing systems. UPRC staff have extensive experience in managing European research projects and maintain strong collaborations with public and private sector organizations, contributing to the modernization and development of Greek economy and society through cutting-edge research and technology transfer activities.

3.7.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Web Technologies *Informatics*	Undergraduate, Semester 1	5	Internet and WWW technologies and protocols; TCP/IP stack; HTML5, CSS3, JavaScript, jQuery, AJAX; PHP, Node.js; XML and JSON; client-side and server-side application development.
Cryptography *Informatics*	Undergraduate, Semester 5	5	Basic algorithms (monoalphabetic substitution, One-Time-Pad, Caesar, Vigenère, Hill); symmetric algorithms (DES, AES, cipher modes); stream ciphers (LFSR, RC4); public key algorithms (RSA, elliptic curves); homomorphic encryption; hash functions; digital signatures; cryptanalysis.
Security Governance *Informatics*	Undergraduate, Semester 6	5	System and application vulnerabilities; vulnerability discovery methods and tools; exploitation and persistence; digital forensics; information risk analysis; security plans, policies, and processes; regulatory frameworks and

			standards; continuity and recovery plans.
Information Systems Security *Informatics*	Undergraduate, Semester 7	5	Information system security concepts; security management systems; cryptographic systems and PKI; access control and privacy; security technologies; secure electronic and mobile services; network security introduction.
Network Security *Informatics*	Undergraduate, Semester 8	5	Network security at all protocol layers; routing security; firewall design; VPNs; IPSec; SSL/TLS.
Maritime ICT Systems *Informatics*	Undergraduate, Semester 7	5	Maritime database and information systems; maritime monitoring systems; threats and attacks on maritime technologies; standards and regulatory frameworks for maritime security; port ICT risk management.
E-Business and Innovation *Informatics*	Undergraduate, Semester 8	5	E-business and e-commerce fundamentals; trustworthy e-business infrastructure; e-environment analysis; e-business strategy; supply chain management; digital marketing; CRM; secure e-business service design and implementation.
Security Policies and Security Management *Digital Systems*	Undergraduate, Semester 5	5	Information security management systems; ISO 27k standards; risk analysis and ISO 27005; security policies and policy hierarchy; incident management and lifecycle; business continuity and disaster recovery; security assurance and metrics.
Network Security *Digital Systems*	Undergraduate, Semester 5	5	Security at lower, network, and application layers; key and identity management protocols; firewalls; trust management; distributed authentication and intrusion detection systems.
Information Systems Security *Digital Systems*	Undergraduate, Semester 6	5	Identification, authentication, and biometrics; identity management; access control mechanisms; OS security (Unix, Windows NT); database security and multi-level databases; malware

			classification; system and product security assurance.
Internet Protocols *Digital Systems*	Undergraduate, Semester 6	5	OSI and TCP/IP models; application layer protocols (DHCP, HTTP, FTP, SMTP, DNS); client-server architecture and socket programming; TCP and UDP; IP addressing and routing protocols; ARP; multimedia networking and VoIP.
Privacy Enhancing Technologies *Digital Systems*	Undergraduate, Semester 6	5	Privacy definition and legal framework; privacy attacks and impact assessment; anonymity, unlinkability, and undetectability; pseudo-anonymity; identity management; PETs (Anonymizer, LPWA, Onion Routing, Crowds, MixNets); privacy in ubiquitous computing, IoT, and health systems; privacy economics.
Cryptography *Digital Systems*	Undergraduate, Semester 7	5	Information security concepts; symmetric and public key cryptography; digital signatures; authentication; hash functions; integrity checking; key management and random number generators.
Mobile and Wireless Communications Security *Digital Systems*	Undergraduate, Semester 8	5	Wireless security fundamentals; IEEE 802.11 security and authentication; RADIUS and EAP methods; IEEE 802.1x; WEP vulnerabilities; IEEE 802.11i, WPA, WPA2 (TKIP, CCMP).
Privacy on the Internet *Digital Systems*	Undergraduate, Semester 8	5	Privacy protection (technical, legal, regulatory, ethical); ISO/IEC 29100, 29101, 29134, 27701 standards; Privacy by Design; privacy impact assessment; cloud privacy (ISO 27018); GDPR and ISO 27001 synergies; social media privacy.
Information Systems *Industrial Management & Technology*	Undergraduate, Semester 5	5.5	Information systems fundamentals; IT strategy; databases and file management; business information systems; e-commerce; decision support systems; collaboration technologies; information security and privacy.

Management Information Systems *Business Administration*	Undergraduate, Semester 7	7	Information systems from business viewpoint; IT management responsibilities; understanding and harnessing IT for business functions.
E-Commerce *Business Administration*	Undergraduate, Elective	3	E-business introduction; e-commerce categories and models; B2C and B2B systems; ERP and CRM; supply chain information systems; security considerations.
Network Security *Hellenic Air Force Academy (with UPRC)*	Undergraduate, Semester 8	2	Cryptography principles; message integrity and digital signatures; key management; end-point authentication; secure e-mail; SSL; wireless LAN security; firewalls and IDS; malware.
Computer Networks & Network Security *Hellenic Air Force Academy (with UPRC)*	Undergraduate, Semester 6	2	Application, transport, network, and data link layers; TCP/IP protocols; routing algorithms; network security fundamentals.
Information Security of Public Services and Blockchain *MSc. in Digital Culture, Smart Cities, IoT*	Graduate, Semester 2	6	Web application security vulnerabilities; secure password storage; encryption functions; blockchain building blocks; Proof of Work/Stake; blockchain applications and tokenisation; smart contracts; distributed storage and IPFS.
Cryptography *MSc. in Informatics*	Graduate, Semester 3	5	Private and public key algorithms; hash functions; digital signatures; cryptographic applications (IPSec, SSL, SSH, e-voting); cryptanalysis.
Information Security *MSc. in Informatics*	Graduate, Semester 4	5	Information system security methodologies; cryptographic tools and techniques; access control; security technologies for the web.
Maritime Informatics *MSc. in Informatics*	Graduate, Semester 4	5	Port critical information infrastructure protection; trustworthy e-port and e-maritime services; surveillance and monitoring technologies; autonomous vessels and AI attacks; routing algorithms.

Network and Communications Security *MSc. in Cybersecurity and Data Science*	Graduate, Semester 1	6	TCP/IP security vulnerabilities analysis; network security policy design; firewalls, IDS/IPS, and VPN implementation; data-link, network, transport, and application layer security.
Information Security Governance *MSc. in Cybersecurity and Data Science*	Graduate, Semester 1	6	Risk assessment standards and methodologies (CRAMM, eBIOS, MITIGATE); security policies and procedures; auditing and certification; legal and policy requirements; business continuity; incident handling; supply chain security.
Applied Cryptography *MSc. in Cybersecurity and Data Science*	Graduate, Semester 1	3	Symmetric and asymmetric encryption; hash functions; digital signatures; key generation and exchange; homomorphic encryption; cryptographic protocols; secure computations.
Penetration Testing *MSc. in Cybersecurity and Data Science*	Graduate, Semester 2	6	Penetration testing methodology; reconnaissance and scanning techniques; exploitation, brute forcing, client-side attacks; persistence (trojans, rootkits, backdoors); AV/EDR bypass; post-exploitation; lateral movement; network pivoting.
Digital Forensics *MSc. in Cybersecurity and Data Science*	Graduate, Semester 2	3	Incident handling process; Windows forensics (memory, registry, file system, application); log file analysis; Linux forensics; network forensics.
Malware Analysis *MSc. in Cybersecurity and Data Science*	Graduate, Semester 2	3	Malware types; C&C servers and protocols; obfuscation techniques; static and dynamic malware analysis; machine learning for malware detection.
Software Security *MSc. in Cybersecurity and Data Science*	Graduate, Semester 2	6	Security best practices in software development; vulnerability identification in open-source and closed-source software; vulnerability demonstration and rating; vulnerability management; state-of-the-art identification methods and proactive mitigation.

Advanced Cryptographic and Security Technologies (Blockchain) *MSc. in Cybersecurity and Data Science*	Graduate, Semester 2	3	Blockchain fundamentals; consensus algorithms (PoW, PoS, BFT); transaction traceability; smart contract development in Ethereum/Hyperledger.
Network Security *MSc. in Digital Systems Security*	Graduate, Semester 1	7.5	Security requirements and attacks; cryptography and PKI; authentication and trust management; PGP; IPSec; SSL/SSH/SET; firewalls; malware; intrusion detection; DoS attacks; DNS and ARP attacks.
Applied Cryptography *MSc. in Digital Systems Security*	Graduate, Semester 1	7.5	Cryptographic history and foundations; PRNGs and one-way functions; stream and block ciphers; El Gamal, RSA, elliptic curves; hash functions and MACs; digital signatures (DSS); key distribution (Diffie-Hellman, Kerberos); e-voting, e-payments, MPC.
Mobile Internet Security *MSc. in Digital Systems Security*	Graduate, Semester 2	7.5	WLAN security and IEEE 802.11i; ad hoc networks and IoT security; GSM, GPRS, UMTS security; WiMAX and LTE security; wireless community networks; Android and iOS security.
Distributed Systems and Cloud Computing *Cross-institutional (with Univ. Western Macedonia)*	Graduate, Semester 1	5	Modern distributed systems and cloud computing design; NFV, SDN, edge and fog computing; heterogeneity and scaling; quality assurance; fault tolerance.
Security of Information and Network Systems – GDPR *Cross-institutional (with Univ. Western Macedonia)*	Graduate, Semester 1	5	Identification and authentication; identity management; access control; OS and database security; malware; system assurance and assessment; GDPR compliance.
Cybersecurity *Open University of Cyprus / Hellenic Air Force Academy*	Graduate	-	Network security essentials; cryptography; user authentication; database and cloud security; malware; DoS attacks; intrusion detection; firewalls; buffer overflow and software security; OS security; IT security management and controls.

CCNA Security V1.0 *MSc. in Digital Systems Security (Summer Course)*	Seminar	-	Cisco security technologies; modern network threats; network device security; AAA; ACLs; IPS; LAN security; cryptographic systems; VPN implementation; ASA and ASDM.
CyberHOT Summer School *UPRC*	Seminar	-	Threat and attack monitoring; strategy and tool evaluation; system administration; network monitoring; attack detection and response.
Cybersecurity Policies and Practices in the EU *UPRC (for non-IT experts)*	Seminar	-	Legal and policy aspects of EU cybersecurity; risk assessment; cybersecurity management and governance; crisis communication; business continuity and disaster recovery.
AIS/GNSS Spoofing *UPRC*	Seminar	-	Risks and threats to GNSS and AIS; use cases; securization of AIS and GNSS; secure AIS transponders.

Table 13: UPRC pre-CSP educational offer

Summary of pre-CSP offering

UPRC offers one of the most extensive and comprehensive cybersecurity educational portfolios in European higher education, delivered across multiple departments (Informatics, Digital Systems, Industrial Management & Technology, Business Administration) and through collaborations with the Hellenic Air Force Academy and the University of Western Macedonia. The offering spans undergraduate to graduate levels, with additional summer schools and seminars, demonstrating exceptional breadth, depth, and institutional commitment to cybersecurity education.

At the undergraduate level, UPRC provides approximately 20 courses across multiple departments. The Informatics and Digital Systems departments offer parallel and complementary security curricula, with courses progressing from foundational topics (web technologies, internet protocols, cryptography) through intermediate topics (security governance, information systems security, network security) to advanced specialisations (privacy enhancing technologies, mobile and wireless security, internet privacy). This dual-department structure provides extensive coverage with some beneficial redundancy, allowing students to access security education through multiple degree pathways.

A distinctive feature of the undergraduate offering is its strong coverage of privacy topics. Two dedicated courses address Privacy Enhancing Technologies (anonymity systems, Onion Routing, MixNets) and Privacy on the Internet (ISO privacy standards, Privacy by Design, GDPR), providing depth that is relatively rare at undergraduate level. The maritime security focus (Maritime ICT Systems) reflects Greece's strategic importance in maritime industries and provides unique sector-specific security education.

The collaboration with the Hellenic Air Force Academy extends security education into defence contexts, with courses on network security and computer networks tailored to military requirements. The Business Administration department contributes courses on management information systems and e-commerce, ensuring that security considerations are integrated into business-oriented education.

At the graduate level, UPRC offers multiple dedicated cybersecurity master's programmes. The MSc. in Cybersecurity and Data Science provides a comprehensive curriculum covering network and

communications security, security governance, applied cryptography, penetration testing, digital forensics, malware analysis, software security, and blockchain technologies. The MSc. in Digital Systems Security offers parallel depth with higher credit weighting (7.5 ECTS courses) in network security, applied cryptography, and mobile internet security. The MSc. in Informatics contributes additional courses in cryptography, information security, and maritime informatics.

Cross-institutional collaboration with the University of Western Macedonia extends the graduate offering to include distributed systems, cloud computing, and GDPR compliance. The collaboration with the Open University of Cyprus and Hellenic Air Force Academy provides a comprehensive cybersecurity course accessible to military and distance learning students.

Professional development is supported through summer schools and seminars, including CCNA Security certification preparation, the CyberHOT summer school on threat monitoring and incident response, EU cybersecurity policy training for non-IT professionals, and specialised training on AIS/GNSS spoofing for maritime applications.

The portfolio demonstrates extensive use of industry-standard tools across all levels, including CrypTool, John the Ripper, Nmap, OpenVAS, OWASP ZAP, Wireshark, Snort, Metasploit, Kali Linux, Burp Suite, IDA Pro, Autopsy, and Volatility. The Hack-the-Box platform is used for penetration testing training, and risk assessment tools (CRAMM, eBIOS, MITIGATE) support governance education.

Overall, UPRC's cybersecurity portfolio is distinguished by its exceptional scale (40+ courses), comprehensive coverage across technical, governance, legal, and sector-specific domains, multiple dedicated graduate programmes, strong privacy focus, unique maritime security specialisation, military collaboration, and extensive professional development offerings. The portfolio prepares graduates for diverse career pathways in technical security, governance and compliance, privacy engineering, maritime security, and defence contexts.

3.7.3 CSP offer and exploitation plan

The following table presents UPRC’s implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Penetration Testing in the Health Sector CSP010_W_H Health Advanced	This workshop focused on penetration testing and red teaming, where students are not only taught but also provided with a demo in performing a variety of realistic attacks. The course provides in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber-attacks against background healthcare infrastructure	Incorporation into the 'Health Informatics and Data Protection' courses. The lab exercises (via Hack-the-Box) will be used for hands-on training of medical staff and IT administrators in hospitals.
Penetration Testing in Energy Sector CSP010_S_E Energy Advanced	The binary penetration testing in the energy sector seminar is a concise, intensive introduction aimed at equipping participants with the foundational skills and knowledge needed to begin addressing binary vulnerabilities within the energy sector.	Utilisation of the modules in Professional Training Programs (KEDIVIM) focused on Critical Infrastructure Protection. Use of the risk management frameworks in future research projects and industrial consulting.
Cybersecurity Essentials and	This training module provides a comprehensive introduction to cybersecurity for the maritime sector,	Integration into the Maritime Security specialisation of the MSc. in Cybersecurity. Use of

Name	Description	Exploitation plan
Management for Maritime CSP001_W_M Maritime Basic	equipping participants with the knowledge and skills to protect their organisations from cyber threats.	the materials in specialised workshops for port authorities and shipping companies to enhance personnel resilience.
Cyber Ranges and Operations in Maritime CSP011_S_M Maritime Basic	The CyberPort training program specifically addresses the unique cybersecurity challenges in port environments. It brings together world-renowned experts to enhance technical skills in key areas of cybersecurity, with a special focus on ports. The program covers ethical hacking, risk management, incident handling, and practical cybersecurity issues specific to maritime ports.	Integration into the Maritime Security specialisation of the MSc. in Cybersecurity. Use of the materials in specialised workshops for port authorities and shipping companies to enhance personnel resilience.
Healthcare sector cyber security CSP008_S_H Health Basic	The module provides the learner with the ability to understand and manage vulnerabilities, threats, and risks with a particular focus on the healthcare system. It offers systemic risk management practice and supports critical evaluation of the protection mechanisms used to enhance the security and resilience of the healthcare sector.	Integration into systemic risk management coursework to evaluate protection mechanisms in healthcare.
Network and IoMT Security CSP006_S_H Health Basic	Analysis of network security at various layers. Integration of the emerging field of Internet of Medical Things. Comprehensive knowledge on securing data transmission. Understanding potential vulnerabilities in network layers. Implementation of robust security policies with detailed analyses of real-world medical case studies focused on IoMT communication protocols.	Mainstreaming the content into the annual CyberHOT summer school and providing the modules as Open Educational Resources (OER) for the UPRC student community.
Critical infrastructure Security in Maritime CSP008_C_M Maritime Advanced	The Critical Infrastructure Security for Maritime MODULE aims at describing cybersecurity risks for critical infrastructure and operators of essential services in the maritime. A focus is placed on the Maritime Systems and specificities, as well as on international regulation. Common vulnerabilities of systems and applications that be detailed.	Focused training on international maritime regulations and common vulnerabilities in maritime systems.

Name	Description	Exploitation plan
Cybersecurity Essentials and Management CSP001_C_E Energy Basic	A comprehensive overview of the critical importance of cybersecurity within the energy industry. It presents the fundamental cybersecurity principles and strategies specifically to address the unique challenges faced by the energy sector.	Addressing sector-specific challenges for energy industry trainees to build fundamental defence skills.
Secure Healthcare Software Development CSP009_S_H Health Basic	This module provides specialised knowledge and skills for developing secure software specifically for the healthcare sector. Participants learn to understand the unique security challenges in healthcare software development. The course covers secure coding practices, threat modelling, and the integration of security into the software development lifecycle.	Integration into software engineering courses, covering secure coding and threat modelling for health apps.
Cybersecurity Essentials and Management CSP001_W General Basic	CyberSecPro Training Module on Cybersecurity Essentials and Management for the Business. This workshop equips you with the fundamental knowledge and best practices to safeguard your online business operations against evolving cyber threats. Through this introduction, we set the stage for the crucial role of cybersecurity in the dynamic and rapidly expanding world of e-commerce.	Integration into security certifications and vocational training for personnel.
Human Factors in Maritime Cybersecurity CSP002_S_M Maritime Basic	This seminar navigates through the human aspects of energy cybersecurity, examining the psychological, social, and organisational influences on security practices and decisions in an energy context. Attendees uncover insights into human vulnerabilities that cyber attackers target in energy operations and acquire methods to cultivate a cybersecurity-aware culture within energy organisations.	Seminar-based delivery to foster a cybersecurity-aware culture within maritime organisations.
Maritime Cybersecurity Risk Management and Governance CSP003_S_M Maritime	This module provides the basic principles, phases and methodologies for risk assessment of maritime systems and their supply chains.	Teaching basic principles and methodologies for risk assessment in maritime supply chains.

Name	Description	Exploitation plan
Basic		
Cyber Threat Intelligence and sharing in the SeaPort CSP006_S_M Maritime Advanced	The module provides an understanding of the underlying properties and principles associated with cyber threats within a maritime organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence.	Advanced module on current threat landscapes and hunting specifically for port environments.
Cybersecurity for the Critical Sectors in Europe CSP001_S_M Maritime Advanced	This intensive training equips professionals with the knowledge and strategies to safeguard Europe's vital sectors from escalating cyber threats. By delving into the complex interplay of technology, policy, and human factors, participants develop a comprehensive understanding of critical infrastructure's cybersecurity challenges and learn to implement robust defence mechanisms.	Integration into professional certification pathways for Critical Infrastructure Protection (CIP). The module will be offered as a high-level seminar for security officers in transport sectors to enhance cross-sectoral resilience
Human Factors and Cybersecurity Energy CSP002_S_E Energy Basic	This course dives deep into the human elements of cybersecurity, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants gain insights into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations.	Integration into professional certification pathways for Critical Infrastructure Protection (CIP). The module will be offered as a high-level seminar for security officers in energy sectors to enhance cross-sectoral resilience
Network and IoMT Security CSP006_S_H Health Basic	Cyber Threat Intelligence	Incorporation into the advanced 'Cyber Operations' lab. The materials will be used to train students and professionals in proactive threat hunting and the use of intelligence sharing platforms (e.g., MISP) in real-world scenarios
Software Security for Maritime CSP009_S_M Maritime Advanced	This training module dives deep into the essential principles and practices of maritime software security. Participants gain hands-on experience identifying, understanding, and mitigating software vulnerabilities of the maritime applications throughout the development lifecycle.	Direct exploitation through specialised training for maritime software developers and vendors. The module will be integrated into the 'Secure Software Development Lifecycle' (S-SDLC) course, focusing on maritime-specific protocols.

Name	Description	Exploitation plan
Cybersecurity Essentials and Management for Health Sector CSP001_W_H Health Basic	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.	Utilisation as a mandatory training component for Healthcare IT administrators and medical staff. The content will be adapted into a 'Micro-credential' for health professionals to comply with NIS2 directive requirements
Cybersecurity Essentials and Management CSP001_S General Basic	Introduction to Cybersecurity. Foundational Knowledge of Cybersecurity Taxonomy. Cybersecurity Body of Knowledge. Importance of Cybersecurity. Common Cyber Threats and Types of Cyber Attacks. Understand Hackers Mindset. Cybersecurity Best Practices: CIA, Risk Management, Security Policies & Procedures, Security Awareness Programmes, Incident Response.	Usage as a 'Bridge Module' for non-IT students and entry-level professionals. The taxonomy and foundational knowledge will serve as the standardized introductory course for all new CyberSecPro-related training cycles.

Table 14: UPRC offer and exploitation plan

3.7.4 Summary

Prior to CyberSecPro, **UPRC** was already delivering an extensive and vertically integrated cybersecurity portfolio across undergraduate, graduate, and professional levels, with strong expertise in cryptography, network security, governance, privacy, maritime ICT, and sectoral applications. The baseline offer demonstrated academic depth and disciplinary breadth, including advanced modules such as *Penetration Testing*, *Malware Analysis*, *Information Security Governance*, and sector-oriented courses like *Maritime ICT Systems*. This foundation positioned UPRC as a mature cybersecurity education provider with solid research-to-teaching transfer mechanisms. Through CyberSecPro, UPRC is introducing a decisive sector-specific and operational reinforcement of its portfolio, transforming existing strengths into highly contextualised, practice-oriented, and infrastructure-focused training pathways. New modules such as *Penetration Testing in the Health Sector (CSP010_W_H)*, *Cyber Ranges and Operations in Maritime (CSP011_S_M)*, *Software Security for Maritime (CSP009_S_M)*, and *Cybersecurity Essentials and Management for Health Sector (CSP001_W_H)* are embedding realistic attack simulations, cyber range environments, IoMT security scenarios, and critical infrastructure governance frameworks directly into curricula and professional training formats. This is not merely expanding content; CyberSecPro is operationalising sectoral cybersecurity through red teaming exercises, threat intelligence platforms (e.g., MISP), and compliance-driven micro-credentials aligned with NIS2 requirements.

At institutional level, UPRC is strengthening its exploitation capacity by mainstreaming CyberSecPro modules into MSc. specialisations, summer schools (e.g., CyberHOT), professional certification pathways (CIP), and KEDIVIM training programmes. CyberSecPro content will be embedded within existing courses (e.g., integration into *Health Informatics and Data Protection* and *Secure Software Development Lifecycle*), while simultaneously generating new stand-alone seminars for port authorities, energy operators, hospital IT administrators, and maritime software vendors. This dual academic-professional integration ensures that exploitation is continuing beyond the project lifecycle through formal curricula, micro-credentials, Open Educational Resources, and executive-level sector training.

CyberSecPro is reshaping the educational landscape around UPRC by systematically addressing the needs of its immediate stakeholder ecosystem. For healthcare providers and hospitals in the UPRC

network, sector-specific penetration testing and secure health software modules are strengthening operational resilience. For port authorities, shipping companies, and maritime regulators, cyber range exercises and risk governance training are enhancing preparedness against supply chain and operational technology threats. For energy operators and critical infrastructure managers, dedicated essentials and human-factor modules are building compliance-ready security cultures. Employers in these sectors are gaining access to graduates and professionals trained in realistic, domain-specific threat environments rather than generic cybersecurity theory.

Overall, UPRC is consolidating its role as a sector-driven cybersecurity competence hub, with CyberSecPro enabling the transition from broad academic excellence to targeted, infrastructure-aligned capability building. The new modules are persisting within formal programmes and professional pathways, ensuring that learners, industry partners, and public authorities continue benefiting from specialised, compliance-oriented, and practice-intensive cybersecurity education.

3.8 Universidade Nova De Lisboa, Faculty of Science and Technology (FCT)

3.8.1 Presentation of organisation/unit

Universidade NOVA de Lisboa (NOVA) was founded in 1973 as Portugal's youngest public university in the Lisbon metropolitan area, adopting from its inception an innovative departmental and interdisciplinary structural model considered new in the Portuguese university context. With nine academic units, more than 22,000 students, 2,500 teachers and researchers, and over 3,400 international students from 110 nationalities, NOVA operates campuses in Lisbon, Almada, Oeiras, and Cascais, delivering comprehensive education across sciences, technology, health sciences, business, economics, social sciences, and humanities. The university ranks consistently among the top young European universities in international rankings and is the only Portuguese institution in the QS Top 50 Under 50, with its School of Business and Economics holding triple crown accreditation (AMBA, EQUIS, AACSB) and ranking 30th among European business schools in Financial Times rankings. NOVA hosts 42 Research and Development Units, 75% of which received "Exceptional," "Excellent," or "Very Good" evaluations from the Portuguese Foundation for Science and Technology, contributing approximately 10% of Portugal's research papers indexed in Web of Science and securing 10 European Research Council grants since 2009. University staff have substantial experience in international collaboration through partnerships with MIT, Carnegie Mellon University, University of Texas at Austin, and extensive participation in Erasmus+ mobility programs, cooperative agreements with Portuguese-speaking countries, and involvement in prestigious academic networks including the Young European Research Universities Network (YERUN).

3.8.2 Pre-CSP educational offer

Course name and department	Level	ECTS	Content summary
Networks and Computer Systems Security *Informatics (NOVA FCT)*	Undergraduate , Semester 1-2	6	Security fundamentals; applied computational cryptography and cryptographic tools; authentication and access control; TCP/IP stack security; systems security.
Software Security *Informatics (NOVA FCT)*	Undergraduate , Specialisation	6	Security properties and threat modelling; secure software design principles (least privilege, fail-safe defaults, complete mediation);

			authorisation and access control models; information flow and non-interference; web application security (injection, XSS, CSRF); unsafe language exploitation (buffer overruns); data security, provenance, and differential privacy.
Cybersecurity and Governance *MSc. in Law and Security (NOVA School of Law)*	Graduate, Semester 1	6	Information security and cybersecurity concepts; hackers and cyberspace actors; cyberspace regulation; fight against cybercrime; incident response and crisis management; algorithms and future technologies.
Data Protection and Management Law *MSc. in Law and Security (NOVA School of Law)*	Graduate, Semester 1	6	Rights to privacy and data protection in European law; GDPR legal background and practical application; critical assessment of GDPR.
Cybercrime *MSc. in Law and Security (NOVA School of Law)*	Graduate, Semester 1	6	Online threats and cybercrime typologies; cyber-criminology and victimisation; financial cybercrime (extortion, fraud, cryptocurrency laundering); cyber-terrorism; attacks against information systems; AI-generated evidence; algorithmic criminal justice; EU cybersecurity policies.
Cybersecurity *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 2	7.5	Information security in organisations; legal and normative frameworks; cyberspace actors and threats; risk assessment and management; security technologies, policies, and organisation; governance, compliance, and reporting.
Globalisation and Security Risks *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 2	7.5	Globalisation and securitisation; human and cooperative security concepts; response tools for global risks and threats; international alliances and cooperation; strategic analysis and public policy decision support.
Intelligence Services and Political Regimes *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 2	7.5	Concepts of democratisation; contributions of information services to the establishment.

Social Network Intelligence *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 1	7.5	Data, information, and knowledge management in a knowledge-based society; social networks and geographic information in intelligence and information management.
Regional Dynamics of Security and Defence *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 1	7.5	Security and defence dynamics in different world regions; analytical and critical skills for regional security analysis.
Economic and Competitive Intelligence *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 1	7.5	Competitive intelligence and its relation to strategy and marketing; tools and methodologies for competitor analysis; strategic decision-making support.
Methodology and Techniques for Analysis and Prospection *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 1	7.5	Foresight concepts and tools; scenario building methodologies; geoeconomic and geopolitical analysis; alternative evolution scenarios.
Structured Analytical Techniques for Information Analysis *Post-Grad in Information Management and Security (NOVA IMS)*	Post-graduate, Semester 2	7.5	Intelligence analysis specificity; structured analytic techniques for intelligence matters; technique selection for specific situations.
Digital Transformation in a Cybersecurity Context *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	Cybersecurity in digital transformation; enabling factors and technologies; organisational preparedness; transformation and risk management methodologies.
Cybersecurity, IT Asset Management, and Governance *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	IT asset management policies, mapping, and governance; risk identification and mitigation; IoT vulnerabilities and risk minimisation.

GDPR: Governance, Implementation, Maintenance and Control *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	GDPR governance and privacy policies; compliance monitoring and auditing; data subject rights procedures; incident management response.
The Legal Framework of the Digital Ecosystem (TMT) *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	Constitutional and criminal limits in digital context; computer crime and cybercrime definitions; GDPR and CNPD supervision; sanctions and software legal protection.
How to Implement an ISMS with ISO/IEC 27001 *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	Security policy definition for ISMS implementation; information system security architecture; risk assessment, control, and management mechanisms.
Cybercrime - Prevention and Forensic Techniques *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	Digital information safeguarding for evidence; forensic best practices; crisis management interconnection; criminal law considerations.
Competitive and Counter Intelligence *Executive Seminar: Cybersecurity and Data Privacy (NOVA IMS)*	Executive	-	Competitive intelligence for actionable insights; navigating data overload and misinformation; protection against social engineering and competitor activities.

Table 15: NOVA FCT pre-CSP educational offer

Summary of pre-CSP offering

NOVA offers an exceptionally broad and interdisciplinary educational portfolio in cybersecurity and information security, delivered across multiple schools and departments: the Faculty of Science and Technology (NOVA FCT), the NOVA School of Law, and the NOVA Information Management School (NOVA IMS). The offering spans undergraduate to executive education levels, demonstrating a comprehensive institutional approach that integrates technical, legal, governance, and strategic intelligence perspectives.

NOVA FCT delivers a comprehensive and multidisciplinary cybersecurity portfolio spanning technical, legal, strategic, and executive dimensions: at undergraduate level, rigorous Informatics courses address cryptography, network and software security, secure design principles, threat modelling, and advanced topics such as differential privacy; at graduate level, specialised programmes combine legal and criminological perspectives on cybersecurity governance, data protection, and cybercrime with strategic intelligence-oriented education in security management and analysis; and executive seminars further strengthen governance, compliance, ISO/IEC 27001 implementation, digital transformation, and forensic competencies for professionals and decision-makers.

Overall, NOVA's portfolio is distinguished by its breadth and interdisciplinary integration. The combination of deep technical content (software security, cryptography), legal and regulatory expertise (GDPR, cybercrime), strategic intelligence (competitive intelligence, foresight), and practical governance (ISO 27001, risk management) creates a uniquely comprehensive offering. This multi-school approach prepares graduates for diverse career pathways spanning technical security, legal and compliance, policy and governance, and strategic intelligence roles.

3.8.3 CSP offer and exploitation plan

The following table presents NOVA's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Leveraging Domain and Threat Intelligence in the Energy Domain CSP011_C_E Energy Basic	Provides knowledge and practical skills to efficiently manage digital forensics and incident response actions. The course covers incident handling fundamentals, SIEM implementation for threat detection and log analysis, and incident response strategy development.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Mechanics for Memory Corruption CSP009_S_E Energy Basic	This seminar provides an overview of how memory-corruption vulnerabilities work and are managed. This seminar provides an overview of how native software works, how simple bugs can be used to execute an attacker's code, and how such bugs are managed.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Foundations of networking and systems security CSP004_S General Advanced	In the modern digital landscape, understanding the fundamentals of networking and systems security is crucial for individuals and organisations alike. It is not just about keeping your personal devices secure but also about protecting sensitive data and ensuring the reliable operation of critical systems. This CyberSecPro training examines the systems security associated with a business aspect.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Cyber Threat Intelligence in the Energy Network CSP006_C_E Energy Advanced	This training module explains the underlying properties and principles associated with cyber threats within an energy organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering.

Name	Description	Exploitation plan
		We plan to promote the training materials for self-study.
Cybersecurity in Emerging Technologies for Energy CSP007_C_E Energy Advanced	This training module explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, equipping participants with the knowledge and skills needed to protect their environments.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Cybersecurity in Emerging Technologies for the Energy Network CSP007_S_E Energy Basic	This seminar explores the unique cybersecurity challenges and best practices associated with energy emerging technologies, providing participants with an overview of how to protect their energy environments. It introduces the learner into energy securing various technologies like the IoT, cloud computing, blockchain, and AI.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Critical Energy Infrastructure Security CSP008_C_E Energy Advanced	The training module equips participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge energy technologies. As the energy business embraces innovations, this module provides a comprehensive understanding of the cybersecurity landscape within the energy context.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.
Digital Forensics for Energy CSP012_S_E Energy Advanced	This seminar provides a set of terms and concepts associated with digital forensics, specifically applied to the energy sector. It introduces the learner to digital forensics and techniques for conducting forensic examinations in energy infrastructures.	We plan to integrate the content into the existing Master's in Electrical and Computer Engineering. We plan to promote the training materials for self-study.

Table 16: NOVA FCT offer and exploitation plan

3.8.4 Summary

NOVA entered CyberSecPro with a **s**trong and highly interdisciplinary cybersecurity portfolio, combining technical depth at NOVA FCT (e.g., *Networks and Computer Systems Security*), legal-regulatory expertise at NOVA School of Law (e.g., *Cybercrime*), and governance and intelligence-oriented education at NOVA IMS. This pre-existing offer demonstrates that NOVA was already addressing cybersecurity from multiple disciplinary angles, spanning undergraduate to executive levels. However, before CyberSecPro, the portfolio was primarily generalist in scope and not sector-specific, with limited dedicated focus on critical infrastructures such as energy systems

Through CyberSecPro, NOVA is significantly expanding this foundation by introducing sector-focused, practice-oriented, and infrastructure-specific cybersecurity modules, particularly in the energy domain. New modules such as *Cyber Threat Intelligence in the Energy Network (CSP006_C_E)*, *Critical Energy Infrastructure Security (CSP008_C_E)*, and *Digital Forensics for Energy (CSP012_S_E)* are operationalising advanced threat intelligence, incident response, and forensic methodologies within energy infrastructures. In parallel, foundational seminars such as *Mechanics for Memory Corruption (CSP009_S_E)* and *Cybersecurity in Emerging Technologies for the Energy Network (CSP007_S_E)* are strengthening technical depth in vulnerability exploitation and emerging technology protection, explicitly contextualised to energy systems.

The exploitation strategy of NOVA is clearly embedding CyberSecPro results into institutional structures. By integrating the new modules into the existing Master's in Electrical and Computer Engineering, NOVA is ensuring that CyberSecPro content is not remaining project-bound but is becoming structurally anchored within accredited degree programmes. At the same time, NOVA is promoting the training materials for self-study, thereby extending exploitation beyond enrolled students and enabling continuous professional development. This dual pathway is strengthening sustainability while broadening access.

As a result, NOVA is transforming its cybersecurity portfolio from a broad interdisciplinary offer into a strategically specialised and sector-relevant ecosystem, with a strong focus on critical energy infrastructures. CyberSecPro is enabling NOVA to bridge advanced technical cybersecurity (e.g., memory corruption, SIEM implementation, threat hunting) with real-world operational environments in the energy sector. This is increasing the applied character of programmes and reinforcing alignment with European resilience priorities.

In terms of impact, NOVA is strengthening the cybersecurity capacity of its surrounding stakeholders, including energy companies, public authorities, technology providers, and SMEs in the Lisbon metropolitan area. By continuously delivering energy-focused cybersecurity competencies, NOVA is supporting employers with graduates and professionals trained in infrastructure protection, threat intelligence, and incident response within energy contexts. In this way, NOVA is actively shaping the regional educational landscape, ensuring that specialised cybersecurity skills remain available beyond CyberSecPro and continue benefiting learners, industry partners, and public sector actors.

4 Integration into Company Training Offers

4.1 Austrian Institute of Technology (AIT)

4.1.1 CSP offer and exploitation plan

The following table presents AIT's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Network Protection for Energy Control Systems CSP004_C_E Energy Advanced	This seminar provides a clear understanding of the threats in power control networks to subsequently understand the main security weaknesses of TCP/IP protocols and their impact on critical communication networks.	The practical activities developed in this course are planned to be reused for our future trainings.
Cascading Effects in Complex Health Networks CSP008_S_H Health Advanced	Initially, the importance and characteristics of Critical Infrastructures be discussed, based on the EU's NIS2 and CER directives. Then, it focuses 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.	The created slides are planned to be used as part of our future trainings to increase cybersecurity awareness in critical infrastructure.
Protecting Charging Stations Against Specific Threats CSP008_S_E Energy Advanced	This lecture provides an overview of cybersecurity challenges associated with electric vehicle charging infrastructures. It introduces a generic taxonomy of threats affecting these systems and delves into common cybersecurity risks specific to EV charging applications.	We plan to include topics such as cascading effects analysis in our future training course plan to highlight the significance in critical infrastructure protection and resilience as well as to facilitate the simulation using the CASSANDRA tool.
Security Aspects for Maritime Networks - Session 3: Cryptography and encryption CSP004_S_M Maritime	This lecture provides an overview of cryptography and its history. It discusses the main features of cryptography and its various types. It also includes a description of cryptanalysis and brute-force attacks, then delves into the differences between symmetric and asymmetric encryption techniques.	The created slides are planned to be used as part of our future efforts to increase cybersecurity awareness in the maritime domain.

Name	Description	Exploitation plan
Advanced		
Network Protection for Energy Control Systems - Session 4: Web security CSP004_C_E Energy Advanced	This lecture delves into details related to web security and its associated protocols. It provides an overview of the IP and TCP protocols and explains how TCP/IP works. The discussion then highlights the importance of TCP/IP and explores the structure of this protocol.	The slides are intended for use in our future training with industry and critical infrastructure from the energy domain.
Security Aspects for Maritime Networks CSP004_S_M Maritime Advanced	In the beginning, the participants get a general overview on communication networks and how they are used in the maritime domain. This be accompanied by a selection of recent or most prominent attacks that happened in the maritime domain, i.e., on port infrastructures or vessels, together with a description of the attack vector and the consequences in the maritime sector.	We plan to reuse the practical activities related to threat modelling, particularly those involving ThreatGet, in our future training materials. This will help demonstrate threat analysis in the maritime sector and provide a strategy for mitigating cyber risks.
Cascading Effects in Complex Maritime Networks and Supply Chains CSP008_S_M Maritime Advanced	Initially, the importance and characteristics of Critical Infrastructures be discussed, based on the EU's NIS2 and CER directives. Then, it focusses on the different types of dependencies within a CI from the maritime sector and among CIs and other organisations from different sectors along the maritime supply chain.	We planned to include topics such as cascading effects analysis in our future training course plan with companies from the maritime sector to highlight the significance in complex maritime ecosystems.
Cyber Threat Intelligence and Threat Hunting in the Energy Domain CSP006_S_E Energy Advanced	The seminar provides critical infrastructure operators from the energy sector with an overview of threat intelligence and management. It enables participants to analyse the known and unknown threats in the energy domain and determine a course of action to tackle them.	We plan to reuse the ThreatGet section in our future training materials with industry and critical infrastructure from the energy domain.

Name	Description	Exploitation plan
Essential Protection for Energy Control Networks: Topic-3: Essential Protection for Energy Control Networks CSP004_C_E Energy Advanced	The session includes an overview and discussion of common network protocols, Additionally, the session provide an introduction to the energy domain and highlight the most common cybersecurity vulnerabilities within this sector.	The created slides are planned to be used as part of our future trainings to increase cybersecurity awareness in critical infrastructure.
Cyber Threat Intelligence and Threat Hunting in the Energy Domain CSP006_S_E Energy Advanced	The seminar provides critical infrastructure operators from the energy sector with an overview of threat intelligence and management. It enables participants to analyse the known and unknown threats in the energy domain and determine a course of action to tackle them.	We plan to reuse the ThreatGet section in our future training materials with industry and critical infrastructure from the energy domain.

4.2 C2B Consulting (C2B)

4.2.1 CSP offer and exploitation plan

The following table presents C2B's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Pentesting for Maritime CSP010_W_M Maritime Basic	This module can be operated on a physical installation operated by an end-user. The training should be as realistic as possible and aims at providing a training on AIS devices detained by an entity willing to improve the training of its personnel. It helps to identify spoofing or jamming of AIS and GNSS.	Contact has been taken with a French Company[1] developing AIS transponders and C2B co-developed cybersecurity functions for this system.
Cyber range and operations on SCADA CSP011_S_E Energy Basic	Attacks, countermeasures, mitigations, privacy on energy control systems.	The development of a basic SCADA simulator could be further developed to propose a future PENTEST platform

[1] ATHANOR ENGINEERING - https://athanor-engineering.com/

Name	Description	Exploitation plan
Digital Forensic for Maritime CSP012_C_M Maritime Basic	A part of a broader Maritime Cybersecurity Seminar, this module on Digital Forensic for Maritime is an adaptable module dedicated to the specific threats for administrations operating at sea and the capacity to access to Automated Information Systems Forensics.	The digital forensic module for maritime will be proposed to Coastguards, once C2B has gained its certification.
Critical infrastructure Security in Maritime CSP008_C_M Maritime Advanced	The Critical Infrastructure Security for Maritime MODULE aims at describing cybersecurity risks for critical infrastructure and operators of essential services in the maritime. A focus is done on the Maritime Systems and specificities as well as on international regulation. Common vulnerabilities of systems and applications that be detailed.	Module delivered as part of the Multimodal Transportation Master 2 of the University of Dunkirk

Table 17: C2B offer and exploitation plan

4.3 Information Technology for Market Leadership (ITML)

4.3.1 Presentation of organisation/unit

Information Technology for Market Leadership IKE (ITML) is a fast-growing ICT and software company founded in 2011 and headquartered in Athens, Greece, with additional offices in Cyprus and the United Kingdom. ITML specialises in the design and delivery of cybersecurity solutions and services, with strong expertise in AI-driven data analytics, secure software development, and trustworthy data management. The company actively participates in EU research and innovation projects, delivering scalable, reliable, and market-oriented technologies.

4.3.2 Pre-CSP educational offer

Before the start of the CyberSecPro project, ITML's educational activities, as an SME, were primarily focused on internal training sessions aimed at upskilling employees in areas such as cybersecurity, secure software use and development, and data management. Participation in CyberSecPro provided the opportunity to expand educational activities through the design and delivery of structured cybersecurity training courses for external stakeholders, including SMEs, universities, and medical institutions.

4.3.3 CSP offer and exploitation plan

The following table presents ITML's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Network Security & Health: Endpoint Protection Strategies CSP004_S_H Health Basic	This course provides participants with practical knowledge and skills to enhance the security of healthcare networks. With a strong focus on endpoint protection, the course covers fundamental concepts, the cybersecurity threat landscape in healthcare, and best practices for securing critical systems.	The course will be exploited through professional training sessions and workshops targeting healthcare organisations and SMEs. The materials will also be reused in future cybersecurity training initiatives and potential

Name	Description	Exploitation plan
		future EU-funded research and innovation projects.
Alerting, Reporting, & Monitoring Strategies for Cybersecurity in Healthcare Sector CSP011_S_H Health Basic	This module focuses on cybersecurity strategies for the healthcare sector, emphasizing alerting, reporting, and monitoring. It covers the following topics: an introduction to cybersecurity in healthcare,	The module will be reused in external training activities for healthcare stakeholders and SMEs, and integrated into ongoing cybersecurity capacity-building and awareness programmes.
Digital Forensics for Health Sector CSP012_S_H Health Basic	This seminar focuses on equipping healthcare professionals with digital forensic skills to investigate and prevent cybersecurity incidents. Through hands-on use of tools like Security Infusion, participants learn how to analyse data, reconstruct events, and implement security measures to safeguard patient data.	The materials will be exploited through hands-on workshops and academic training activities in healthcare and educational institutions, supporting digital forensics skills development.
Alerting, Reporting, & Monitoring Strategies for Cybersecurity in the Energy Sector CSP011_S_E Energy Basic	This module covers Alerting, Reporting, and Monitoring Strategies for Cybersecurity in the Energy Sector. It builds upon the syllabus, with a focus on vulnerability management, real-time threat notifications, and continuous infrastructure monitoring using cloud-based tools.	The module will be exploited through targeted training activities for energy sector SMEs and public organisations and reused in future professional training and research initiatives.

Table 18: ITML offer and exploitation plan

4.3.4 Summary

Before CyberSecPro, ITML's educational engagement was primarily inward-looking and strategically aligned with operational excellence. As a fast-growing ICT SME, ITML was focusing on internal capacity-building activities, delivering structured in-house training sessions to upskill staff in cybersecurity, secure software development, and data management. These activities were strengthening ITML's internal expertise but were not yet formalised as externally accessible courses. CyberSecPro is transforming ITML's educational role from an internal training provider into an outward-facing cybersecurity capacity builder for sectoral stakeholders.

Through CyberSecPro, ITML is developing and implementing a portfolio of structured, market-oriented training modules tailored to specific sectors, notably health and energy. Courses such as *Network Security & Health: Endpoint Protection Strategies (CSP004_S_H)*, *Digital Forensics for Health Sector (CSP012_S_H)* and *Alerting, Reporting & Monitoring Strategies for Cybersecurity in the Energy Sector (CSP011_S_E)* are introducing new thematic depth and sector-specific specialisation that did not exist in ITML's pre-project offer. These modules are combining practical, tool-based training with applied cybersecurity strategies, directly reflecting ITML's technological expertise. CyberSecPro is enabling ITML to formalise, package and externalise its know-how into scalable, reusable learning products.

The exploitation of these modules is actively continuing beyond the project lifetime. ITML aims to deliver professional workshops for healthcare organisations, SMEs and public bodies, while also integrating the developed materials into future training initiatives and potential EU-funded research and innovation projects. The reuse of course materials and their adaptation to different target groups is ensuring sustainability and continuous value creation. ITML is embedding CyberSecPro outcomes into its long-term service portfolio, ensuring that the newly developed courses remain operational, market-relevant and revenue-generating.

The impact on ITML is structural and strategic. CyberSecPro is strengthening ITML's positioning not only as a technology provider but also as a recognised contributor to cybersecurity skills development. The project is expanding ITML's stakeholder engagement, fostering closer collaboration with healthcare institutions, energy-sector organisations, SMEs and academic actors. This shift is reinforcing ITML's role within the broader cybersecurity ecosystem, enhancing visibility, credibility and innovation capacity.

On the educational landscape surrounding ITML, the impact is targeted and practice-oriented. By continuing to offer specialised sectoral courses, ITML is enriching the regional and cross-sectoral cybersecurity training ecosystem with applied, industry-driven content. Healthcare providers, energy-sector organisations and SMEs connected to ITML are gaining sustained access to up-to-date training in endpoint protection, digital forensics and real-time monitoring strategies. CyberSecPro is thus contributing to a more resilient skills environment around ITML, directly benefiting employers, professionals and learners through the continued availability of high-quality, sector-specific cybersecurity education.

4.4 Security Labs Consulting Ltd (SLC)

4.4.1 Presentation of organisation/unit

Security Labs Consulting Ltd (SLC) has strong experience in leading and contributing to European projects. SLC already developed a broad portfolio of unique and specialised products and services which are underpinned by AI techniques, including in Cyber Security Risk Assessment and Management Platform, Cyber Threat Management, Secure Software Systems Lifecycle, and Privacy-by-Design. Dissemination and communication are one of the key activities of SLC for the wider adoption and showcase of the solutions. Specifically, SLC's dissemination and communication approach aims to adopt the innovative solutions across the sectors in various domains such as Health Care, Banking, Public Administration, Maritime, Critical Infrastructures and Telecommunications, and explore through showcase in security and privacy challenges in technologies such as Internet of Things, Cloud Computing, AI and Big Data. SLC members are also frequently invited speakers at company-sponsored training events, public organisation meetings, and well-known security conferences and seminars such as ISACA, ENISA and NATO. Hence, SLC is active in the scientific and industry community by publishing research outputs and participating in showcase events like cybersecurity demos, workshops and posters.

4.4.2 CSP offer and exploitation plan

The following table presents the implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Cybersecurity Risk Management and Governance in the Energy sector CSP003_S_E Energy	The module provides an understanding of the underlying properties and principles associated with cybersecurity risk management with particular focus on the energy sector. It offers learners the opportunity to	Multi-channel exploitation strategy will follow to disseminate this workshop, including contact made to targeted groups such as SME owners, University graduates, LinkedIn channel. This workshop will be considered as a part of the

Name	Description	Exploitation plan
Advanced	understand and adopt the relevant standard for risk management and governance to the energy domain.	cybersecurity awareness programme and aims to offer, through different EU events, invited talks by the SLC members as standalone workshops or in combination with other training programmes.
Healthcare sector cyber security CSP008_S_H Health Basic	The module provides learner with the ability to understand and manage vulnerabilities, threats, and risks with a particular focus on the healthcare system. It offers systemic risk management practice and supports critical evaluation of the protection mechanisms used to enhance the security and resilience of the healthcare sector.	The workshop materials will be updated based on the expertise of the SLC team. SLC follows a multi-channel exploitation strategy and will disseminate this workshop and consider this workshop as a part of the training portfolio. This workshop will be considered as part of the cybersecurity awareness programme and aims to offer, through different EU events, invited talks by the SLC members as standalone workshops or in combination with other training programmes.
Data Protection and Privacy Technologies for Maritime CSP005_S_M Maritime Basic	This module provides a comprehensive understanding and teaches practices of cyber risk, vulnerabilities and data protection and privacy technologies. The training module empowers both individuals and organisations to navigate the evolving landscape of data protection and privacy with confidence and compliance for maritime sector.	The workshop materials will be updated based on the expertise of the SLC team. This workshop will be considered as part of the data protection awareness programme and will be disseminated to the targeted sectoral audience.

Table 19: SLC offer and exploitation plan

4.4.3 Summary

Before CyberSecPro, SLC has been actively contributing to European projects and has been developing advanced AI-driven cybersecurity solutions, while dissemination has been taking place primarily through conference presentations, invited talks and sectoral showcase events. However, SLC has not been operating a structured, modular educational portfolio comparable to the CyberSecPro offer. Educational activities have largely been embedded in project-related communication, industry events and awareness sessions rather than formalised, stand-alone training modules.

With CyberSecPro, SLC is formalising and expanding its educational engagement by developing and implementing sector-specific training modules that translate its technical expertise into structured learning offers. New offers, such as *Cybersecurity Risk Management and Governance in the Energy Sector (CSP003_S_E)*, *Healthcare Sector Cyber Security (CSP008_S_H)* and *Data Protection and Privacy Technologies for Maritime (CSP005_S_M),* are operationalising SLC's applied knowledge in risk management, governance and privacy-by-design into targeted, competency-oriented learning experiences. Through these modules, SLC is embedding cybersecurity risk methodologies and sectoral

compliance practices directly into dedicated training formats, moving from dissemination-based knowledge sharing to structured capacity building.

CyberSecPro is therefore enabling SLC to transition from project-based knowledge transfer to a sustainable training portfolio model. The exploitation strategy will help to position the new modules within SLC's broader cybersecurity awareness and data protection programmes, using multi-channel dissemination, targeted outreach to SME owners, graduates and sectoral stakeholders, and integration into EU events and invited workshops. By continuously updating content based on in-house expertise and market developments, SLC will ensure that these courses remain relevant and aligned with evolving regulatory and technological landscapes.

At institutional level, CyberSecPro is strengthening SLC's role as a sector-focused cybersecurity capacity builder. SLC will be integrating the new modules into its long-term service portfolio, reinforcing its visibility across energy, healthcare and maritime ecosystems. The project is also enhancing internal capabilities in structured curriculum design, learner targeting and modularisation of expert knowledge, thereby professionalising SLC's educational dimension beyond ad-hoc dissemination activities.

On the educational landscape, CyberSecPro is broadening the specialised cybersecurity offer available to stakeholders around SLC. SMEs in the energy and healthcare sectors, maritime operators, recent graduates and professional networks connected to SLC are gaining continued access to sector-specific risk management and privacy training. By sustaining these modules, SLC will continuously contribute to raising cybersecurity maturity and compliance awareness within its surrounding industry communities, while employers will benefit from learners who are better equipped to manage sector-specific risks and governance challenges.

4.5 Serious Games Interactive (SGI)

4.5.1 Presentation of organisation/unit

Serious Games Interactive (SGI) is a forward-thinking SME dedicated to developing innovative game-based learning solutions that combine game mechanics and game technology to create solutions with engagement, and impact. SGI specialises in transforming complex training and educational content into interactive digital experiences that enhance understanding, retention, and real-world application. By integrating storytelling, simulations, and scenario-based learning, SGI enables individuals and organisations to learn through active participation rather than passive instruction.

Through innovation, creativity, and a strong commitment to learning impact, Serious Games Interactive aims to deliver effective, engaging, and future-ready training experiences that drive performance improvement and long-term organisational growth.

4.5.2 Pre-CSP educational offer

SGI offered development of bespoke cybersecurity training games for major corporations but did not have a ready-made offer in the marketplace.

4.5.3 CSP offer and exploitation plan

The following table presents SGI's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Leveraging Domain and Threat Intelligence in the Energy Domain	Provides knowledge and practical skills to efficiently manage digital forensics and incident response actions. The course covers incident handling fundamentals,	1) Higher education: Make SCORM Package available for HE. 2) Corporations: Make an event package for use once and a yearly

Name	Description	Exploitation plan
CSP011_C_E Energy Basic	SIEM implementation for threat detection and log analysis, and incident response strategy development.	subscription for larger organisations 3) Individuals: Make a package for the biggest digital games platform (Valve's Steam) to create a new channel for individuals to buy one license, and from the inside, create interest.
Cybersecurity Essentials and Management for Energy Sector (v003) CSP001_C_E Energy Basic	Cybersecurity Essential and Management for Energy Sector CSP training module provides equip trainees and professionals with the knowledge and skills needed to defend against evolving cyber threats critical energy industry.	Same as above
RxB - Cyber security management game CSP001_CS-E_H Health Basic	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.	Same as above
RxB - Cyber security management game CSP001_CS-E_M Maritime Basic		
RxB - Cyber security management game CSP001_CS-E_E Energy Basic		

Table 20: SGI offer and exploitation plan

SGI will use different ways to reach the three audiences: HE, Corporations and individuals.

1. **HE**: SGI will make direct contact to program leaders in cybersecurity faculty, and to coordinators for educational offerings.
2. **Corporations**: SGI will target medium or large enterprises with direct sales to senior staff, security head or training department
3. **Individuals**: SGI will use Steam organic, curators within Steam within cybersecurity games, and our own Social Media channels,

Across all channels, SGI will use the network built up through CyberSecPro.

4.5.4 Summary

SGI is transforming from a bespoke development provider into a scalable cybersecurity training actor through CyberSecPro. Before CyberSecPro, SGI focused on tailor-made cybersecurity training games for large corporate clients without offering standardised, ready-to-market courses. This model ensured high-quality solutions but limited scalability, visibility, and systematic outreach to higher education (HE) and individual learners. With CyberSecPro, SGI aims to implement structured, modular training offers such as *Leveraging Domain and Threat Intelligence in the Energy Domain (CSP011_C_E)* and *Cybersecurity Essentials and Management for Energy Sector (CSP001_C_E)*, alongside sector-specific versions of the *RxB – Cyber Security Management Game* for Health, Maritime and Energy. These courses are translating SGI's game-based learning expertise into replicable, licensable educational products.

CyberSecPro is enabling SGI to operationalise a multi-channel exploitation strategy that is currently expanding its market presence and long-term sustainability. SGI will make SCORM packages available to HE institutions, offer event-based and subscription models to corporations, and enter the individual learner market through digital distribution platforms such as Steam. Through these differentiated exploitation pathways, SGI is systematically embedding CyberSecPro modules into formal curricula, corporate training programmes, and self-directed professional development. At the same time, SGI will leverae the CyberSecPro network to strengthen partnerships and visibility, ensuring that the newly developed courses are continuously reaching programme leaders, security managers, and independent learners.

The institutional impact is significant, as SGI is consolidating a sustainable product portfolio that extends beyond project funding. By converting project outputs into market-ready, sector-specific modules (e.g., RxB variants across Energy, Health and Maritime), SGI will strengthen its positioning as a provider of immersive, domain-focused cybersecurity training. This is ensuring that the CyberSecPro results are not remaining isolated pilot activities but are becoming an integrated and continuously exploited part of SGI's business model.

The impact on the educational landscape around SGI is emerging through the sustained availability of practice-oriented, gamified cybersecurity training for key stakeholders. HE partners are integrating CyberSecPro modules into their curricula, corporations are embedding them into professional training pathways, and individual learners are accessing high-quality sector-specific simulations via digital platforms. As a result, learners are benefiting from interactive, scenario-based training that strengthens applied skills, while employers in Energy, Health and Maritime sectors are gaining access to talent with practical red-versus-blue experience. Through ongoing exploitation, SGI is contributing to a more resilient regional and sectoral cybersecurity skills ecosystem, ensuring that CyberSecPro outcomes are continuously supporting workforce development and organisational preparedness.

4.6 Focal Point (FP)

4.6.1 Presentation of organisation/unit

Focal Point SPRL (FP) is a Belgian cybersecurity consultancy and research company specializing in cyber defence, operational security, and advanced training programs for security professionals. Founded with extensive experience in NATO exercises and European security frameworks, FP transforms EU-funded cybersecurity research projects into operational platforms, including LLM-powered detection assistants, cyber range environments, and attack surface mapping tools. The company has contributed to over 21 peer-reviewed publications in cybersecurity research and actively participates in European research initiatives including Ai4HealthSec and CYRENE projects funded through Horizon 2020 and Horizon Europe programs. FP delivers hands-on blue team, purple team, and SOC training programs developed by field-tested operators, with particular expertise in red teaming, defensive scenarios, and real-world attack simulation through proprietary cyber range tools. The company's staff have substantial experience in managing European cybersecurity projects, conducting research in areas including healthcare cybersecurity, natural language processing for threat assessment, supply chain risk

management, and advancing cybersecurity education in higher education institutions across critical sectors.

4.6.2 Pre-CSP educational offer

Course Name / Department	Level	ECTS	Content Summary
Tabletop Exercise *Focal Point*	Professional Training	N/A	Interactive, gamified exercise providing high-level understanding of business impacts from cyber-attacks. Covers foundational cyber hygiene concepts through group scenarios. Designed for students and low to mid-level employees with no prior knowledge required. Serves as awareness-raising and team-building activity for training events.
FP_CDX (Cyber Defense Exercise) *Focal Point*	Professional Training	N/A	Hands-on SIEM training using Microsoft Sentinel with KQL queries for log analysis. Covers Active Directory attack scenarios: enumeration attacks, user spraying, SMB share vulnerabilities, Zerologon exploitation, ASREPRoast, Kerberoasting, and AD ACL abuse. Develops skills in threat detection, incident response, and defensive strategies.
FP Training Lab *Focal Point*	Professional Training	N/A	Comprehensive red teaming course with hands-on offensive security training. Covers reconnaissance, network enumeration, privilege escalation, and lateral movement. Students perform simulated attacks including injections, buffer overflows, brute-forcing, and misconfiguration exploitation to understand attacker methodologies.
HtB Enterprise Labs: Introduction To Penetration Testing *Focal Point*	Professional Training	N/A	Introductory penetration testing using “Hack The Box enterprise labs”. This covers web application attacks (injections, LFI/RFI, IDOR, CSRF, XSS, command injection) and Linux privilege escalation techniques (SUID exploitation). It develops foundational vocabulary and understanding of common attack vectors.

Table 21: FP pre-CSP educational offer

Summary of pre-CSP offering

Focal Point offers a portfolio of four professional training courses focused on practical cybersecurity skills. All courses are delivered in English and operate outside the formal ECTS credit system,

positioning them as industry-oriented training rather than academic programs. The portfolio spans from awareness-level exercises to advanced offensive security techniques.

FP's programme offers a layered cybersecurity training pathway, beginning with a gamified Tabletop Exercise that introduces cyber hygiene and awareness to non-technical participants, and progressing to advanced technical training in both defensive and offensive security. The FP_CDX cyber defence exercise develops hands-on blue team capabilities in SIEM monitoring, Active Directory attack detection, and threat analysis, while the FP_Training Lab and HtB Enterprise Labs provide comprehensive red team and penetration testing experience, covering the full attack lifecycle and practical exploitation techniques.

The portfolio demonstrates a balanced approach between defensive and offensive training, with strong emphasis on hands-on practical exercises over theoretical instruction. The use of industry-standard platforms (Sentinel, Hack The Box) ensures training relevance to real-world security operations. This combination makes Focal Point's offerings well-suited for upskilling security professionals and preparing practitioners for both blue team and red team roles.

4.6.3 CSP offer and exploitation plan

The following table presents FP's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Software Security - OWASP Top 10 CSP009_W General Basic	Throughout this workshop, students are introduced to the architecture of web applications, as well as to their common bugs.	FP will utilise this workshop as a foundational technical course for junior web developers and security auditors. It will be offered as a "Security by Design" training service for corporate IT departments.
Detection Engineering **on a Cyber Range of a Maritime IT infrastructure- Active Directory** CSP010_W_M Maritime Advanced	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 course provides hands-on experience and in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber-attacks against an Active Directory environment.	Exploitation involves offering this as an advanced, high-tier training for enterprise security teams. FP will use the Active Directory simulation environment to provide hands-on "Attack & Defence" corporate retreats.
Detection Engineering on a Cyber Range -Active Directory CSP011_W General Advanced	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.	This module will be integrated into FP's Managed Security Service Provider (MSSP) training portfolio, helping clients' internal teams build robust SOC detection capabilities.
Securing Healthcare Web Applications	Throughout this workshop, students explore the architecture of modern web applications and the most	Specific exploitation through "Medical Device & Hospital Security" consulting. FP will use

Name	Description	Exploitation plan
CSP009_W_H Health Basic	common categories of web vulnerabilities. Each topic is introduced through a concise theoretical overview and then reinforced with hands-on demonstrations that illustrate how specific flaws can be identified and exploited in real-world scenarios. Participants are provided with the necessary tools and resources to replicate the exercises on their own laptops, ensuring practical understanding and direct applicability to live web environments.	this to train Healthcare IT administrators to identify vulnerabilities in critical patient-care environments.
Penetration Testing for Healthcare IT Infrastructures CSP010_W_H Health Advanced	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 course provides 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	Integration into FP's specialized healthcare compliance services (e.g., NIS2 for Health). It will be used to help hospitals implement automated threat detection tailored to medical protocols.
Detection Engineering on a Cyber Range of a Healthcare IT infrastructure-Active Directory CSP011_W_H Health Advanced	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.	Integration into FP's specialised healthcare compliance services (e.g., NIS2 for Health). It will be used to help hospitals implement automated threat detection tailored to medical protocols.
Securing Maritime Web Applications CSP009_W_M Maritime Basic	Throughout this workshop, students explore the architecture of modern web applications and the most common categories of web vulnerabilities. Each topic is introduced through a concise theoretical overview and then reinforced with hands-on demonstrations that illustrate how specific flaws can be identified and exploited in real-world scenarios. Participants are provided with the necessary tools and resources to replicate the exercises on their own	Usage as a standardized entry-level module for FP’s vocational training academy, serving as a prerequisite for more advanced sectoral cybersecurity certifications.

Name	Description	Exploitation plan
	laptops, ensuring practical understanding and direct applicability to live web environments.	
Penetration Testing for Maritime IT Infrastructures CSP010_W_M Maritime Advanced	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.	FP will exploit this as a high-end "Red Team Assessment" training for financial and government institutions, focusing on replicating the tactics of sophisticated threat actors.
Detection Engineering on a Cyber Range of a Maritime IT infrastructure-Active Directory CSP011_W_M Maritime Advanced	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.	Exploitation through the development of a "Blue Team Certification" path, allowing FP to certify professionals in modern defensive engineering and incident response.
Penetration Testing in the Health Sector CSP010_W_H Health Advanced	This workshop focused on penetration testing and red teaming, where students are not only taught but also provided with demo in performing a variety of realistic attacks. The course provides in-depth knowledge of red teaming methodologies and techniques, empowering students to simulate real-world cyber-attacks against background healthcare infrastructure	Provision of "Executive Cybersecurity Demos" for healthcare board members. FP will use the demos to visualize the impact of cyber-attacks and upsell security infrastructure upgrades.
CSP010_W_H CSP010_W_H Health Advanced	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. All these stages are highly applicable to background Healthcare IT infrastructure.	FP will use this curriculum to establish a long-term "Cyber Resilience Program" specifically for the Health sector, providing continuous training as attackers' techniques evolve.
CSP010_W_M CSP010_W_M Maritime Advanced	Under the guidance of instructors, students learn the intricacies of red teaming, starting with the fundamentals and gradually progressing to more advanced	Exploitation through FP's maritime division. This module will be used to train Vessel IT managers and port operators to defend Ship-to-Shore

Name	Description	Exploitation plan
	techniques. The curriculum covers a wide range of offensive security topics. All these stages are highly applicable to background Maritime IT infrastructure used for operations.	communication systems and Operational Technology (OT).

Table 22: FP offer and exploitation plan

4.6.4 Summary

Before CyberSecPro, FP was already delivering a strong portfolio of professional, non-ECTS cybersecurity trainings focused on hands-on operational skills, including awareness-level exercises (e.g., *Tabletop Exercise*), defensive SIEM-based blue team training (*FP_CDX*), and offensive security programs (*FP_Training Lab*, *HtB Enterprise Labs: Introduction to Penetration Testing*). These offerings were technically robust and industry-oriented, yet primarily horizontal in scope and not sector-specialised. CyberSecPro is significantly expanding FP's portfolio by introducing structured, sector-specific and cyber-range-based modules that deepen both technical sophistication and strategic relevance.

Through CyberSecPro, FP is implementing a coherent set of new modules that address software security, red teaming, and detection engineering across general, maritime, and healthcare contexts (e.g., *CSP009_W – Software Security: OWASP Top 10*, *CSP011_W_M – Detection Engineering on a Cyber Range of a Maritime IT Infrastructure*, *CSP010_W_H – Penetration Testing for Healthcare IT Infrastructures*). These modules will not only extend existing expertise but are embedding it into simulated sectoral infrastructures, enabling realistic attack-and-defence scenarios tailored to critical domains. CyberSecPro is therefore operationalising sector-focused cyber range environments and translating EU-funded research into deployable, revenue-generating training services.

FP intends to actively exploit these new courses by integrating them into corporate training services, managed security service provider portfolios, compliance consulting (e.g., NIS2 for Health), executive demonstrations, and the development of structured certification paths such as a "Blue Team Certification". In doing so, FP is moving from standalone technical training toward long-term resilience programmes and recurring sectoral engagement models.

At institutional level, CyberSecPro is strengthening FP's positioning as a provider of advanced cyber range–based training and as a bridge between European research and operational cybersecurity practice. FP is consolidating its role as a sector-aware cybersecurity capability builder, expanding from general red/blue team training into targeted healthcare and maritime resilience programmes. The project is enhancing FP's strategic capacity, service diversification, and long-term sustainability.

At ecosystem level, the impact is materialising in the sustained availability of specialised, practice-oriented training for stakeholders surrounding FP, including hospitals, maritime operators, port authorities, IT departments, and enterprise SOC teams. Through continued exploitation of modules such as *Securing Healthcare Web Applications (CSP009_W_H)* and *Penetration Testing for Maritime IT Infrastructures (CSP010_W_M)*, FP is strengthening the regional and European cybersecurity skills pipeline. CyberSecPro is therefore contributing to a more resilient educational landscape by ensuring that sector-specific cybersecurity competencies remain accessible to professionals, employers, and critical infrastructure operators connected to FP.

4.7 Maggioli SPA (MAG)

4.7.1 Presentation of organisation/unit

Maggioli S.p.A. is a leading Italian system integrator and technology provider founded in 1896, serving as the primary ICT solutions provider for local public administrations in Italy with over 6,000 municipalities out of 8,048 running approximately 100,000 modules provided by Maggioli Informatica,

the company's IT division. Headquartered in Santarcangelo di Romagna near Rimini, Maggioli operates through multiple business areas including Information Technology, Services & Technologies, Publishing, Training and Education, Document Management, and Museums, Art and Culture, employing over 2,000 staff across Italy and international offices in Brussels, Madrid, Athens, and Bogotá. The company has maintained a Brussels representative office for over 20 years to ensure visibility within European institutions, conduct research and development activities, and participate in European projects, with particular expertise in Cloud computing, Big Data analysis, AI, Internet of Things, cybersecurity, and system architecture. Maggioli holds certifications including UNI EN ISO 9001:2008, UNI CEI ISO/IEC 27001:2014, and UNI EN ISO 14001:2015, and serves as coordinator or partner in numerous EU-funded Horizon 2020 and Horizon Europe projects including VOXReality (AI-enabled XR solutions), AI4Gov (AI supporting policy making), CyberSecDome (VR in security, privacy), CYberSynchrony (cybersecurity), CyberNEMO (AI IoT), INCISIVE (cancer imaging AI toolbox), CYRENE (cybersecurity and privacy assessment), PolicyCLOUD (data-driven policy management), and COMFORTage (AI in healthcare). The company's extensive experience spans digital transformation of public administration processes, interoperable health data spaces, federated data sharing, and development of AI-based solutions for both public and private sectors across Europe and Latin America.

4.7.2 Pre-CSP educational offer

Course Name / Department	Level	ECTS	Content Summary
The Application Consultant *Maggioli Academy*	Professional Training	N/A	Training for recent graduates providing general understanding of public administration and related services. Serves as the delivery training ground. Duration: 160 hours.
Junior Full Stack Developer *Maggioli Academy*	Professional Training	N/A	Cloud development training for graduates in three-year scientific subjects. Serves as the developers' training ground. Duration: 160 hours.
Data Science Basic and Advanced *Maggioli Academy*	Professional Training	N/A	Data Science program (5th edition) for those investing in future-critical skills. Covers data analysis and navigation through records, numbers, information, and data sets aligned with job market demands.
Project Management *Maggioli Academy*	Professional Training	N/A	Advanced skills training with business professionals as instructors. Emphasises practical, directly applicable skills for the workplace, reflecting Maggioli's philosophy of companies as places of higher education.
Cyber Security Specialist *Maggioli Academy*	Professional Training	N/A	First edition program training professional profiles for public administration and private sector. Develops specialised technical skills with cross-functional vision across

			technology, organisational, procedural, legal, and legislative domains.
Bootcamp Maggioli Academy *Maggioli Academy*	Seminar	N/A	Intensive 3-day immersive training initiative (2nd edition) involving final-year classes from 'Business Information Systems' course at Rino Molari Technical Institute in an innovative artificial intelligence project.
H-Greenovation *Maggioli Academy*	Seminar	N/A	Team-based project marathon from collaboration between Higher Institutes and Maggioli Group. The 2022 initiative involved 48 students from 'Einaudi - Molari' high schools in challenges dedicated to #GreenMobility and #GreenPackaging.
Girls Code it Better *Maggioli Academy*	Seminar	N/A	All-female initiative promoted by Officina Futuro Fondazione W-Group encouraging girls to pursue STEM studies. Set national record hosting 44 students from Franchini Institute in Santarcangelo di Romagna, divided into two clubs.

Table 23: MAG pre-CSP educational offer

Summary of pre-CSP offering

MAG, through its Maggioli Academy division, delivers a portfolio of five professional training courses and three seminars, all conducted in Italian. Operating outside the formal ECTS system, the offerings serve as corporate training grounds for workforce development, with particular focus on bridging education and employment for recent graduates and secondary school students.

MAG delivers 160-hour professional training programmes aligned with specific career pathways, including Application Consultant (public administration), Junior Full Stack Developer (cloud development), Data Science (now in its fifth edition), Project Management, and the newly launched Cyber Security Specialist programme, which adopts a cross-functional approach integrating technical, organisational, and legal competencies for both public and private sector contexts. Complementing these are socially impactful seminar initiatives such as the Bootcamp Maggioli Academy (AI projects for technical students), H-Greenovation (sustainability challenges for high schools), and Girls Code it Better, which promotes gender diversity in STEM through large-scale coding clubs.

Maggioli Academy's portfolio reflects a distinctive industry-education integration model, positioning the company as a site of higher learning while maintaining strong connections with regional technical institutes. The offerings combine workforce development for recent graduates with pipeline-building initiatives that introduce younger students to technology careers, creating a comprehensive talent development ecosystem rooted in the Emilia-Romagna region.

4.7.3 CSP offer and exploitation plan

The following table presents MAG’s implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Software Security for Maritime CSP009_S_M Maritime Advanced	This training module dives deep into the essential principles and practices of maritime software security. Participants gain hands-on experience identifying, understanding, and mitigating software vulnerabilities of the maritime applications throughout the development lifecycle.	The content may be integrated into existing course "Cyber Security Specialist" (under discussion)
Data Protection and Privacy Technologies for Maritime CSP005_S_M Maritime Basic	This module provides a comprehensive understanding and practices of the cyber risk, vulnerabilities and data protection and privacy technologies. The training module empowers both individuals and organisations to navigate the evolving landscape of data protection and privacy with confidence and compliance for the maritime sector.	The content may be integrated into existing course "Cyber Security Specialist" or delivered as a standalone course (under discussion)

Table 24: MAG offer and exploitation plan

4.7.4 Summary

MAG is building on an already well-established corporate training ecosystem delivered through Maggioli Academy, which prior to CyberSecPro has been focusing on professional upskilling and talent pipeline development in areas such as cloud development, data science, project management and cybersecurity (e.g., *Cyber Security Specialist*). These offers have been positioned outside the formal ECTS framework and have primarily addressed workforce integration and reskilling needs in Italian, with strong links to public administration and regional secondary education. As documented in the Individual Exploitation Report, MAG has already been acting as a bridge between education and employment, combining technical depth with applied business relevance.

With CyberSecPro, MAG is significantly extending its cybersecurity portfolio by embedding sector-specific and European-level content into its training landscape. The newly implemented modules, *Software Security for Maritime (CSP009_S_M)* and *Data Protection and Privacy Technologies for Maritime (CSP005_S_M)*, are introducing a focused maritime dimension that has not previously been present in MAG's educational offer. These modules are going beyond generic cybersecurity training by addressing software vulnerabilities in maritime applications across the development lifecycle and by integrating compliance-oriented data protection and privacy technologies tailored to the maritime sector. Through the planned integration of these modules into the existing *Cyber Security Specialist* programme, or through potential standalone delivery, MAG is ensuring that CyberSecPro results are being structurally embedded into its long-term training architecture.

The key added value of CyberSecPro for MAG lies in the sectoral specialisation and the Europeanisation of its cybersecurity training content. While MAG has already been offering cross-functional cybersecurity education combining technical, legal and organisational perspectives, CyberSecPro is enabling MAG to refine this approach with concrete maritime use cases, risk scenarios and compliance requirements. This is strengthening MAG's positioning as a provider of advanced, sector-aware cybersecurity competence development for both public administration and private sector actors. The ongoing exploitation is therefore ensuring that CyberSecPro content is not remaining project-bound, but is being integrated into revenue-generating and recurring training formats.

At institutional level, CyberSecPro is reinforcing MAG's strategic role as an ICT system integrator that is simultaneously acting as a competence hub. By incorporating the maritime-focused modules into its Academy portfolio, MAG is aligning its training activities more closely with its European R&D engagement and its expertise in cybersecurity and data governance. This alignment is strengthening

internal knowledge transfer between project teams and training units, while also expanding the thematic depth of its Academy.

At ecosystem level, CyberSecPro is positively shaping the educational landscape around MAG by introducing persistent, sector-specific cybersecurity competences that will continue benefiting regional and international stakeholders. Learners are gaining access to advanced maritime cybersecurity skills embedded within established training pathways at MAG. Employers – including municipalities, public bodies and private maritime actors connected to MAG – are benefiting from a workforce trained in software security and privacy technologies aligned with European standards and sector-specific risk profiles. Through this sustained offer, MAG will contribute to a more resilient cybersecurity skills base in its surrounding innovation and public administration ecosystem.

Overall, CyberSecPro is enabling MAG to transform project-based knowledge into durable educational assets, ensuring that exploitation is actively strengthening both institutional capacity and stakeholder-oriented impact.

4.8 SINTEF AS (SINTEF)

4.8.1 Presentation of organisation/unit

SINTEF (Stiftelsen for industriell og teknisk forskning - The Foundation for Industrial and Technical Research) was established in 1950 by the Norwegian Institute of Technology (NTH, now part of NTNU) in Trondheim, Norway, and has grown into one of Europe's largest independent research organisations with approximately 2,000 employees from 75 countries. As a not-for-profit foundation, SINTEF reinvests all financial surplus into scientific equipment, skills, and expertise, having invested over NOK 1 billion in laboratories and equipment since 2007, including world-leading facilities such as the world's largest laboratory for multiphase transport of oil and gas and the world's largest marine laboratory. The organisation is structured into five specialized research institutes covering Community (sustainable buildings and infrastructure), Energy Research (renewable energy and power technology), Ocean (marine technology and biomarine research), Industry (materials technology, biotechnology, and applied chemistry), and Digital (artificial intelligence, cybersecurity, and digital health), conducting several thousand research projects annually for approximately 3,800 customers across Norwegian and international industries. SINTEF maintains a strategic partnership with the Norwegian University of Science and Technology (NTNU), sharing approximately 200 laboratories and nearly 30 long-term research centres, with extensive collaboration including joint teaching assignments and research projects. SINTEF holds ISO 9001:2015, ISO 14001:2015, and OHSAS 18001:2007 certifications and operates offices across Norway in Trondheim, Oslo, Bergen, Tromsø, Ålesund, and other cities, as well as in Brussels and Hirtshals, Denmark, with staff having substantial experience in European research collaborations, EU-funded Horizon programs, and participation in strategic research agendas through euRobotics, BDVA (Big Data Value Association), and ADRA (AI, Data and Robotics Association).

4.8.2 Pre-CSP educational offer

Course Name / Department	Level	ECTS	Content Summary
Introduction to Cyber Security *SINTEF Digital / NTNU*	Postgraduate	2.5	Basic introduction to digital system construction, addressing criticality, complexity and diversity (human, technological, organisational dimensions). Covers dependencies between digital systems, integration into critical infrastructure, and potential impacts of attacks and errors on society's basic needs.
Introduction to Cyber Security: Risk Management *SINTEF Digital / NTNU*	Postgraduate	2.5	Risk-based approach to digital security covering ISO/IEC 27005 risk assessment methodology, threat profiling, consequence and vulnerability assessment, and risk management practices.
Thinking Like an Attacker *SINTEF Digital*	Seminar	N/A	Introduction to offensive security mindset for organisational defence. Covers security testing methodology with hands-on exercises on common web application flaws. Requires programming background and basic web

			understanding; no prior security knowledge needed. Delivered on demand.
Digital TORC Training *SINTEF Digital*	Seminar	N/A	Training for Operational Resilience (TORC) using board-game-based learning approach. Helps organisations reveal, understand and develop resilient performance capabilities for unexpected deviations and disturbances. Captures training outcomes as input for technological, human, organisational, and managerial resilience priorities. Delivered on demand.

Table 25: SINTEF pre-CSP educational offer

Summary of pre-CSP offering

SINTEF offers a focused portfolio of four cybersecurity education offerings through its SINTEF Digital division. The portfolio combines two ECTS-credit postgraduate courses delivered in partnership with the Norwegian University of Science and Technology (NTNU) and two on-demand seminars for professional development.

4.8.3 CSP offer and exploitation plan

The following table presents SINTEF's implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
AI and Cybersecurity Research in Maritime CSP007_S_M Maritime Advanced	It covers various aspects of research in AI. The course focuses on building expertise in AI-driven penetration testing, enhancing IDS and SIEM with AI, and defending against adversarial AI attacks.	We plan to continue offering this through collaboration with partners as part of winter or summer schools such as IPICS, and to reuse material in regular academic teaching. We also plan to use the training material and guidelines in the recently started EU project WARRaNT (WAterborne fedeRated systems and models for secuRe and resilieNt operations, Grant agreement ID: 101202581). SINTEF is in charge of the training activities related to Waterborne Digital System methodology, which covers robust cybersecurity assurance and AI for maritime operations.
Threat landscape in healthcare CSP006_S_H Health Basic	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	We plan to continue offering this through collaboration with partners as part of winter or summer schools such as IPICS.

Name	Description	Exploitation plan
	various sources within healthcare systems.	

Table 26: SINTEF offer and exploitation plan

4.8.4 Summary

Before CyberSecPro, SINTEF was offering a focused yet relatively compact cybersecurity education portfolio anchored in foundational and risk-oriented perspectives. The pre-existing offer, delivered through SINTEF Digital in collaboration with NTNU, was primarily addressing general cybersecurity principles and standards-based risk management (e.g., *Introduction to Cyber Security* and *Introduction to Cyber Security: Risk Management*). In addition, SINTEF was providing applied professional seminars such as *Thinking Like an Attacker* and *Digital TORC Training*, which were strengthening practitioner skills in offensive security thinking and organizational resilience. Overall, the portfolio was building strong foundations in systems thinking, risk assessment, and resilience, but was not yet addressing sector-specific and AI-driven cybersecurity challenges at advanced level.

Through CyberSecPro, SINTEF is significantly expanding and deepening this offer by implementing new, domain-specific and research-integrated modules. The course *AI and Cybersecurity Research in Maritime (CSP007_S_M)* is introducing advanced competencies in AI-driven penetration testing, AI-enhanced IDS/SIEM systems, and defence against adversarial AI in maritime contexts. In parallel, *Threat Landscape in Healthcare (CSP006_S_H)* is addressing the application of cyber threat intelligence within healthcare systems, linking intelligence principles with sector-specific operational realities. CyberSecPro is therefore bringing a clear shift from generic cybersecurity foundations to AI-enabled, sector-focused and research-driven specialisation, aligned with European strategic priorities**.**

The exploitation strategy developed by SINTEF ensures that these new modules are not one-off pilot activities but are becoming embedded in long-term educational and research structures. SINTEF intends to continue to offer the modules through international winter and summer schools such as IPICS, is reusing materials in regular academic teaching, and is integrating content into new EU-funded initiatives such as WARRaNT. By embedding training material and guidelines into ongoing research and innovation projects, SINTEF is ensuring that CyberSecPro outputs remain alive, continuously updated, and directly linked to cutting-edge developments. Exploitation is thus taking place through institutionalisation, curricular integration and cross-project reuse, reinforcing sustainability beyond the project lifetime.

In terms of impact, CyberSecPro is strengthening SINTEF's role as a bridge between research, education and sectoral application. SINTEF is expanding its advanced training capacity in AI-driven cybersecurity for maritime and healthcare domains, directly benefiting researchers, industry partners, public authorities and professionals collaborating with SINTEF. The sustained offer is providing learners with specialised, research-informed competences that meet concrete labour market needs, while employers around SINTEF are gaining access to upskilled talent and updated methodologies. CyberSecPro is therefore contributing to a more resilient and innovation-oriented educational landscape in SINTEF's ecosystem, where advanced cybersecurity expertise in critical sectors is continuously being developed, exploited and transferred into practice.

4.9 Zelus P.C. (ZELUS)

4.9.1 Presentation of organisation/unit

Zelus is a Greek digital innovation company committed to building a sustainable circular economy through advanced technologies, offering secure and innovative IT solutions for businesses ranging from micro SMEs to large industries with a security-by-design approach. The company specialises in AI-powered analytics, data-driven intelligence, and user-centred digital products that empower businesses, municipalities, and industry leaders to reduce waste, optimise resources, and comply with evolving EU

regulations around sustainability and digital product passports. Core solution offerings include VÒNG (dual-sided platform for sustainable fashion combining digital wardrobe organisation with AI-powered outfit recommendations for consumers and AI-driven shopping experiences for businesses), MindFactor (AI-powered manufacturing platform processing up to 10,000 measurements per second for real-time operational intelligence), and specialised sustainability consulting services for circular transition and regulatory readiness. Zelus maintains deep expertise in cybersecurity with an innovative toolset for digital forensics analysis and threat hunting, supporting complete IT project management services across the entire software lifecycle, including design, development, deployment, optimisation, and maintenance. The company actively participates in major EU-funded initiatives including CYRENE (supply chain security and conformity assessment), MARVEL (smart city decision-making toolkit with multimodal audio-visual intelligence), KYKLOS 4.0 (circular manufacturing and digital product passports via ROCTex textile waste management experiment), ERMIS (cybersecurity assurance and insurance-as-a-service), FAITH (trustworthy AI framework coordination), ClimaBorough (smart urban planning), GRECO (circular resource optimization), and 3D-CIRCULAR (workforce reskilling for digital and green transition), with pilot deployments across Greece, Italy, Portugal, and partnerships with CRF (Stellantis Group), textile and fashion SMEs, urban innovation labs, and municipalities including Patras, Amarousion, Elliniko-Argyroupoli, and Cascais.

4.9.2 Pre-CSP educational offer

Course Name / Department	Level	ECTS	Content Summary
SmartViz Cybersecurity Training *Zelus*	Professional Training	N/A	Comprehensive cybersecurity training using SmartViz visualisation tool. Covers incident response and decision-making, threat intelligence analysis (logs, network traffic, IoC identification), defensive analysis techniques, and penetration testing/ethical hacking. Emphasises practical skills for vulnerability assessment and security posture improvement.

Table 27: ZELUS pre-CSP educational offer

Summary of pre-CSP offering

Zelus delivers a specialised professional training course centred on its proprietary SmartViz cybersecurity visualisation tool, targeting security professionals seeking applied, operational skills beyond the formal ECTS framework. The programme integrates incident response, threat intelligence analysis, defensive security testing, and penetration testing into a cohesive curriculum, enabling participants to translate technical indicators into structured decision-making and effective incident management.

By combining defensive monitoring techniques with offensive simulation exercises, the course develops a balanced understanding of organisational security posture, while SmartViz functions as the core analytical platform for visualising and interpreting cybersecurity data. This tool-centric and practice-oriented approach ensures immediate applicability in security operations environments where data-driven analysis enhances detection, response efficiency, and strategic decision-making.

4.9.3 CSP offer and exploitation plan

The following table presents ZELUS' implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Introduction to Penetration Testing and Nmap Tool Training CSP010_W General Basic	This training provides students with a comprehensive understanding of essential penetration testing concepts and hands-on experience with the powerful Nmap tool. Penetration testing is the process of evaluating the security of a computer system or network by simulating the attacks of a malicious actor.	ZELUS integrates CSP modules into its commercial training portfolio and custom in-house training programmes for public and private organisations under future commercial agreements and existing EU-funded projects. Modules are to be reused as stand-alone workshops, blended learning courses, and executive training sessions, with adaptation to sectoral regulatory and operational contexts.
Digital Forensics in the Health Sector CSP012_W_H Health Basic	Digital Forensics in the Health Sector is a specialised module that explores the application of digital forensic techniques within healthcare environments. It covers the investigation of cyber incidents, data breaches, and unauthorised access to sensitive medical information.	Based on the existing cybersecurity expertise, ZELUS exploits this module as awareness programmes, table-top exercises, and management-level workshops. ZELUS integrates CSP modules into its commercial training portfolio and custom in-house training programmes for public and private organisations under future commercial agreements and existing EU-funded projects. Modules are to be reused as stand-alone workshops, blended learning courses**,** and executive training sessions**,** with adaptation to sectoral regulatory and operational contexts**.**
Data Protection and Privacy Technologies for healthcare. CSP005_S_H Health Basic	This seminar provides in-depth knowledge and practical skills in safeguarding healthcare data. It covers a comprehensive range of topics from foundational principles of data privacy to advanced technologies and practices specific to the healthcare industry.	
Forensic Investigation CSP006_H_H Health Advanced	This session provides an introduction to understanding malware using forensic analysis tools. Participants are aware of the types and the impact of malware attacks along with the importance of the malware sample analysis. Specific case studies are introduced to participants to leverage their skills on the topic.	

Table 28: ZELUS offer and exploitation plan

4.9.4 Summary

Prior to CyberSecPro, ZELUS is operating a focused, tool-driven professional training offer, centred on the proprietary *SmartViz Cybersecurity Training*, which is addressing incident response, threat intelligence analysis, defensive techniques and penetration testing in an integrated format. This pre-existing offer is practice-oriented, commercially positioned, and tailored to security professionals operating outside the ECTS framework and closely aligned with operational cybersecurity needs. The

emphasis is on applied skills development, data visualisation for enhanced threat detection, and immediate applicability in professional environments.

Through CyberSecPro, ZELUS is significantly expanding and structuring its educational portfolio with modular, thematically differentiated short courses, introducing new content depth and sector-specific specialisation. The implementation of modules such as *CSP010_W – Introduction to Penetration Testing and Nmap Tool Training*, *CSP012_W_H – Digital Forensics in the Health Sector*, *CSP005_S_H – Data Protection and Privacy Technologies for Healthcare*, and *CSP006_H_H – Forensic Investigation* is broadening the scope from a single integrated training product to a flexible portfolio of stand-alone, stackable learning units. These modules are introducing structured learning pathways, sectoral contextualisation (notably in healthcare), and differentiated levels (basic to advanced), thereby complementing and strengthening the existing SmartViz-based training.

Exploitation is actively taking place through systematic integration of CyberSecPro modules into ZELUS's commercial training portfolio and EU-funded project activities. ZELUS is reusing the modules as stand-alone workshops, blended learning formats, executive seminars, awareness programmes, and table-top exercises. By adapting content to sector-specific regulatory and operational contexts, ZELUS is ensuring long-term sustainability under commercial agreements with public authorities, healthcare organisations, and private enterprises. The modular design is enabling ZELUS to continuously embed CyberSecPro outputs into customised in-house training programmes, thereby institutionalising the results beyond the project lifecycle.

At organisational level, CyberSecPro is strengthening ZELUS's positioning as a specialised cybersecurity capacity builder with sector-specific expertise, particularly in digital forensics and data protection in healthcare environments. The structured CSP modules are enriching ZELUS's service portfolio, enhancing market differentiation, and reinforcing its credibility in EU-funded and commercial engagements. The project is not replacing existing training; rather, it is deepening specialisation, expanding thematic coverage, and increasing flexibility of delivery formats.

Within the broader educational landscape surrounding ZELUS, CyberSecPro is generating a sustained increase in targeted, practice-oriented cybersecurity training offers that continue benefiting learners and employers in the regional and EU innovation ecosystem. SMEs, healthcare providers, municipalities, and industrial partners collaborating with ZELUS are gaining access to specialised short courses aligned with operational and regulatory needs. By embedding CyberSecPro modules into ongoing commercial and EU project activities, ZELUS will ensure that new cybersecurity competences in penetration testing, digital forensics, and healthcare data protection are continuously disseminated.

4.10 APIROPLUS Solutions Ltd. (APIRO)

4.10.1 Presentation of organisation/unit

APIROPLUS Solutions Ltd. (APIRO) is a Cypriot information security and cybersecurity consultancy founded in May 2019 and headquartered in Limassol, providing holistic consulting and training services to organisations in Cyprus and internationally across information security, cybersecurity, business continuity, privacy, quality management, IT service management, corporate governance, and digital transformation. With over 25 years of combined experience among its founding members Apostolos Karras and Argyro Chatzopoulou, the company has completed over 2,000 security audits and assessments, developing extensive industry knowledge of organisational strengths and weaknesses in relation to information and cybersecurity through hands-on implementation experience, leadership of international projects, and expertise in education, training, and certification of skills. APIRO implements a unique Capability Maturity Model-based solution to assess organisational security posture, identify and quantify relevant risks, and propose treatment actions, having already supported an EU member state in implementing monitoring and assessment mechanisms for the NIS Directive. The company provides practical, expert, and innovative training programs in information security and cybersecurity that bridge theory with practice through interactive exercises, holding experience in leading international information security certifications for over 10 years each. APIRO actively participates in major EU-funded initiatives including PHOENI2X (Horizon Europe Grant Agreement 101070586, July 2022-June

2025, €4.82M total budget), a cyber resilience framework providing AI-assisted orchestration, automation, and response capabilities for business continuity, incident response, and information exchange tailored to Operators of Essential Services across energy, transport, and healthcare sectors with 16 consortium partners, and REWIRE (Cybersecurity Skills Alliance), developing innovative courses and certification schemes based on the European Cybersecurity Skills Framework in partnership with European University Cyprus and Cyprus Certification Company, with presentations at ENISA's European Cybersecurity Skills Conference contributing to discussions on capacity building and the European Cybersecurity Certification Framework.

4.10.2 Pre-CSP educational offer

Course Name / Department	Level	ECTS	Content Summary
ISO 27001 Auditor / Lead Auditor Course (IRCA Approved) *APIROPLUS Solutions & LRQA Hellas*	Seminar	N/A	40-hour IRCA-approved auditor qualification course. Covers ISO/IEC 27001:2022 structure and requirements, PDCA cycle correlation, risk management principles, Annex A controls, audit processes per ISO 19011 and ISO 17021, audit team management, and findings reporting. Enables participation in IRCA certification exams.
Introduction to the new ISO/IEC 27001 version *APIROPLUS Solutions*	Seminar	N/A	8-hour introduction to ISO/IEC 27001:2022 requirements and operations. Covers standard structure, risk management principles, Annex A connection, mandatory documentation, and detailed comparison of changes between 2013 and 2022 versions for both core requirements (clauses 4-10) and Annex A controls. Includes IAF transition period guidance.
Cybersecurity Maturity Models Requirements / Auditing Practices *APIROPLUS Solutions*	Seminar	N/A	8-hour course on cybersecurity maturity models. Covers maturity model concepts, different types and scales, well-known cybersecurity maturity model examples, and assessment processes and methods for evaluating organisational compliance against specific maturity level requirements.

Table 29: APIRO pre-CSP educational offer

Summary of pre-CSP offering

APIRO delivers a specialised portfolio of three seminars focused on information security management standards and auditing practices, offered in English and Greek outside the formal ECTS system but aligned with internationally recognised certification pathways. The 56-hour portfolio spans governance, compliance, and maturity assessment, with the 40-hour ISO 27001 Auditor/Lead Auditor course (delivered in partnership with LRQA Hellas and IRCA-approved) serving as the flagship programme,

covering the full audit lifecycle and the complete scope of ISO/IEC 27001:2022 requirements and Annex A controls.

Complementing this, the Introduction to ISO/IEC 27001 seminar provides up-to-date foundational training on the 2022 revision and transition requirements, while the Cybersecurity Maturity Models seminar addresses capability-based assessment approaches increasingly adopted by regulators and industry. Overall, the portfolio reflects strong expertise in governance, risk, and compliance (GRC) education, with particular depth in auditor development and standards-based security assessment.

4.10.3 CSP offer and exploitation plan

The following table presents the implemented CSP modules and the planned exploitation.

Name	Description	Exploitation plan
Cybersecurity Risk Management and Governance in the Energy sector CSP003_S_E Energy Advanced	The module provides an understanding of the underlying properties and principles associated with cybersecurity risk management with particular focus on energy sector. It offers learners the opportunity to understand and adopt the relevant standard for risk management and governance to the energy domain.	APIROPLUS Solutions aims to exploit these training modules as follows: 1. Use the module material to create and offer relevant training courses to the market. 2. Collaborate with other partners (HEI) to provide the training courses as part of their academic portfolio. 3. Especially for CSP003_S_H, APIROPLUS Solutions shall provide the Seminar as part of a joined Master with other project partners. 4. Collaborate with the National Standardisation Organisation and the National Digital Security Authority to continue the provision of these and other modules to interested parties of their choosing. 5. Finally, courses will continue to be offered in collaboration with partners as part of winter or summer schools.
Cybersecurity Risk Management and Governance in the Healthcare sector CSP003_S_H Health Advanced	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 customised to fit the healthcare domain.	

Table 30: APIRO offer and exploitation plan

4.10.4 Summary

Prior to CyberSecPro, APIRO demonstrated a strong and focused expertise in governance, risk and compliance (GRC) education, particularly in ISO/IEC 27001 and cybersecurity auditing. The educational offer consisted of high-level professional seminars such as the *ISO 27001 Auditor / Lead Auditor Course (IRCA Approved)* and *Cybersecurity Maturity Models Requirements / Auditing Practices*, operating outside the formal ECTS framework but closely aligned with industry certification pathways. These seminars were primarily standards-driven and audit-oriented, addressing cross-sector information security management and compliance needs. The portfolio positioned APIRO as a

specialised provider in professional upskilling, with strong links to certification bodies and regulatory developments.

Through CyberSecPro, APIRO is significantly expanding this foundation by introducing sector-specific, advanced modules that integrate risk management and governance principles into critical domains, notably energy (CSP003_S_E – *Cybersecurity Risk Management and Governance in the Energy sector*) and healthcare (CSP003_S_H – *Cybersecurity Risk Management and Governance in the Healthcare sector*). These new courses move beyond general ISO-based compliance and contextualise standards, governance models, and risk methodologies within highly regulated, mission-critical environments. In doing so, CyberSecPro is enabling APIRO to translate its GRC expertise into domain-adapted, practice-oriented learning experiences that are directly aligned with sectoral resilience and operational security needs.

From an exploitation perspective, APIRO is actively transforming these modules into sustainable market offerings. The new courses will be integrated into commercial training services, joint Master programmes with HEIs, and seasonal schools. At the same time, APIRO is strengthening strategic collaborations with national authorities such as the National Standardisation Organisation and the National Digital Security Authority, ensuring that the CyberSecPro modules are being embedded into broader national capacity-building initiatives. Through these actions, APIRO is not only maintaining but continuously scaling the exploitation of CyberSecPro results within both academic and professional ecosystems.

CyberSecPro is reinforcing APIRO's profile from a standards-focused training provider to a sector-specialised cybersecurity education actor with the capacity to address critical infrastructure domains. The new modules are diversifying APIRO's portfolio, enabling access to new learner segments, including energy operators, healthcare organisations, and postgraduate students. The structured integration of these modules into joint academic programmes is strengthening APIRO's positioning within formal education pathways while maintaining its professional training identity.

The impact on the educational landscape surrounding APIRO is being realised through the persistent availability of advanced, sector-specific cybersecurity governance courses that were previously not systematically offered in Cyprus and the wider region. Learners are benefiting from structured, domain-adapted risk management education, while employers in the energy and healthcare sectors are gaining access to professionals trained in governance frameworks tailored to their operational realities. Through CyberSecPro, APIRO is contributing to a more resilient regional cybersecurity skills ecosystem, ensuring that specialised expertise in critical sectors continues to be available, evolving, and aligned with regulatory and market needs.

5 Conclusion

This report consolidates the partner-level pathway from CyberSecPro development to post-project value creation by translating a shared set of Key Exploitable Results (the training modules) into concrete, organisation-specific exploitation intentions. Across both HEIs and SMEs, the evidence compiled in this report shows a clear shift from "one-off delivery" to structural embedding: CSP modules are being integrated into accredited curricula, packaged into recurring professional training offers, and adapted into flexible formats such as workshops, short courses, seasonal schools, and (in several cases) MOOCs. Taken together, the individual plans demonstrate that CyberSecPro is not only expanding content coverage (e.g., sector-specific variants for health, energy, and maritime), but is also strengthening delivery models that are continuing beyond the funding period through re-use, adaptation, and integration into existing teaching and training pipelines.

A key contribution of this report is that it provides a **comparative baseline-to-change narrative** for each partner by documenting what existed pre-CSP and what CyberSecPro is bringing into sustained practice. This makes the exploitation progress tangible: partners are not merely listing modules, but are linking them to specific internal "homes" (courses, programmes, training catalogues) where the material is being continuously used, updated, and delivered. In addition, D6.5 contributes a practical "sustainability map" for KER1 by showing how different partner types exploit the same assets in distinct ways: HEIs primarily through curriculum integration and credit-bearing structures, and SMEs primarily through market-facing training products and client-oriented delivery. Together this strengthens the overall ecosystem logic described in the wider exploitation framework.

The main limitation of D6.5 is that it captures exploitation intentions at a largely strategic level, which is appropriate for a public deliverable but limits comparability regarding implementation depth (e.g., exact credit recognition decisions, pricing models, detailed business forecasts, or internal staffing allocations). A second limitation is that exploitation maturity differs across partners: some plans describe immediate integration into existing courses, while others depend on future institutional decisions (e.g., faculty approvals, programme redesign cycles) or market validation steps, meaning that timing and certainty vary. Finally, because partners understandably protect competitive advantages, plans refrain from specifying target volumes, revenue expectations, or partner-specific commercial agreements, which constrains the report's ability to quantify projected outcomes across the consortium.

Looking ahead, the durability of CyberSecPro exploitation is likely to be strongest where partners are continuing to anchor modules in recurring structures, such as degree courses, annual training catalogues, joint programmes, and repeatable exercise formats, supported by ongoing updates through the project's curriculum management logic and competence mapping. As sector-focused cybersecurity needs continue evolving (notably in energy, health, and maritime), the exploitation trajectories documented in D6.5 indicate a pathway toward progressive specialisation: partners are continuing to refine offerings toward stakeholder-specific demands, combining technical depth with governance, human factors, and operational readiness. In this way, the individual plans presented here position CyberSecPro results to remain actively exploited as a living educational supply that is continuously benefiting learners, employers, and regional ecosystems connected to each partner, rather than becoming static outputs at project end.