CYBERSEC PRO

Professional Cybersecurity Training Programme

CYBERSECPRO-PROJECT.EU

This brochure provides a overview of how the CyberSecPro professional training programme evolved from professional market analyses to curricula portfolio design, training implementation, its evaluation and benchmarking.

CyberSecPro supports the implementation of the European Cybersecurity Skills Framework (ECSF) by delivering targeted modules that equip professionals with the essential skills and competencies aligned with key ECSF professional roles needed by the market.

CYBERSEC PRO

CyberSecPro Professional Programme Analysis

CYBERSECPRO-PROJECT.EU

This phase involves several activities, including identifying the cybersecurity skills, knowledge, and values required in the workforce; analysing university and industry cybersecurity programmes, courses, and ECTS grading; assessing partner technologies and teaching suitability; designing the CyberSecPro programme; and proposing actions to integrate its modules and improve the ECTS system.

Cybersecurity practical skills gap in Europe

The key activity in this task involved desktop research. Its deliverable outlines the cybersecurity skills needed by the market, those offered by EU academic and industry programmes, and the gaps between them. The CybeSecPro D2.1 report analyses practical skill shortages across Europe, focusing on essential knowledge areas and core skills. Recognising variation across EU countries, it adopts a practitioner-focused and applied research approach in developing cybersecurity education. The report gives special attention to the health, energy, and maritime sectors and reflects outcomes from tasks T2.1 and T2.2.

Read more

Blended CyberSecPro technological training interactive technologies and academic practice

This is a market-driven analysis of EU cybersecurity existing academic programmes. It includes an overview of 81 CSP partner courses and 64 cybersecurity laboratory hands-on tools. Courses are categorised by type and mapped to high-demand knowledge domains. ECSF alignment highlights both strengths and gaps in role coverage. Recommendations focus on course diversity, ECSF alignment, certification standards, and better access to learning resources. The report also suggests regular content updates and stronger collaboration between students, professionals, and industry.

Read more

CyberSecPro programme specification

This deliverable provides a general structure of the programme, as well as the needs and requirements for its adoption by Higher Education Institutions (HEIs).

A key outcome of this deliverable is the rigorous and systematic analysis and prioritisation of cybersecurity knowledge areas, ensuring the quality and success of the training programme. The knowledge areas are as follows:

- *Cybersecurity management (short descriptions needed)*
- *Human aspects of cybersecurity*
- *Cybersecurity policy, process and compliance*
- *Cybersecurity risk management*
- *Network and communication security*
- *Privacy and data protection*
- *Cybersecurity threat management*
- *Cybersecurity tools and technologies*
- *Penetration testing*
- *Incident response*
- *Emerging technologies*

Read more

Curricula Portfolio
Design, Management & Certification

This phase focuses on developing the training programme and its modules. It defines all modules, integrates an agile Dynamic Curriculum Management System (DCM) to track market needs, and generates curricula for basic and advanced competency levels. Sector-specific curricula for maritime, health, and energy were adapted and stored in the DCM.

CyberSecPro programme main components and procedures

This includes the professional training modules, the DCM system, and a general-purpose CyberSecPro curriculum.

CyberSecPro cybersecurity certification schema

This deliverable proposed a certification schema for the practical training programme.

Read more

CyberSecPro portfolio of cybersecurity curricula targeted to health sector

This deliverable provides a cybersecurity curricula for health sector training needs, customised from the general-purpose curricula.

Read more

CyberSecPro portfolio of cybersecurity curricula targeted to the energy sector

This deliverable provides a cybersecurity curricula for energy sector cybersecurity training needs, customised from the general-purpose curricula.

Read more

CyberSecPro portfolio of cybersecurity curricula targeted to maritime sector

This deliverable provides a cybersecurity curriculum tailored to maritime cybersecurity training needs, customised from the general-purpose curriculum.

Read more

Operating CyberSecPro Professional Training Programme

CYBERSECPRO-PROJECT.EU

This phase involves planning the scalable delivery of CyberSecPro training.
Engaging over 530 trainees in three years, training professionals across various industries, gathering feedback from trainees and trainers, and offering modules that cover cybersecurity principles, tools, emerging technologies, and offensive practices.

Read more

Reports and training material on the emerging technologies modules

This deliverable encompasses all training documentation, including hosting site details, enrolment information, learner backgrounds, evaluations, income records, and sponsorships, covering training modules on emerging technologies and related capabilities.

Reports and training material on Cybersecurity offensive practices modules

This deliverable encompasses all training documentation, including hosting site details, enrolment information, learner backgrounds, evaluations, income records, and sponsorships, covering training modules on offensive practices-related capabilities.

CyberSecPro training operational plan

This provides logistical details as well as templates for reporting and evaluation forms.

Reports and training material on the Cybersecurity Principles and Management training modules

This deliverable encompasses all training documentation, including hosting site details, enrolment information, learner backgrounds, evaluations, income records, and sponsorships concerning modules covering Cybersecurity Principles and Management capability.

Reports and training material on Cybersecurity tools modules

This deliverable encompasses all training documentation, including hosting site details, enrolment information, learner backgrounds, evaluations, income records, and sponsorship in relation to modules covering cybersecurity tools.

CYBERSEC PRO

Multi-facet Evaluation and Benchmarking of CyberSecPro Professional Training Programme

CYBERSECPRO-PROJECT.EU

In this phase, the project developed an evaluation and benchmarking methodology for CyberSecPro training, assessing performance, effectiveness, quality, and sustainability. It also establishes best practices, policy guidelines, and a certification schema for practical cybersecurity training.

CyberSecPro evaluation methodology

This deliverable outlines the evaluation and benchmarking methodology for CyberSecPro. It is based on international standards and cybersecurity training frameworks and incorporates best practices from EU initiatives. The methodology defines relevant KPIs and includes tools for assessing performance, usability, impact, and overall quality. It also provides templates and procedures to support consistent data collection, trainer and trainee feedback, and continuous improvement across the project.

CyberSecPro evaluation and best practices

This deliverable analyses the effectiveness of CyberSecPro's training modules using a set of defined KPIs and evaluation criteria. It includes feedback from over 250 trainees and trainers, with both qualitative and quantitative insights. Findings are benchmarked against international standards to ensure relevance and quality. The report also highlights best practices in cybersecurity skills development and outlines efforts to promote these across academia, industry, and certification bodies.

CyberSecPro certification schema

This deliverable outlines the CyberSecPro certification schema for hands-on cybersecurity training. It reviews the current certification landscape across international, EU, and national levels, and highlights ongoing EU efforts and challenges in harmonising certification. It defines relevant standards, criteria, and evaluation scales. The document also presents the CyberSecPro certification schemas, including principles, objectives, and three schema types: a general professional training framework, module descriptions, and detailed syllabi.

CYBERSEC PRO

Summary of Developed and Implemented Cybersecurity Modules per Targeted Sector

CYBERSECPRO-PROJECT.EU

In addition to the knowledge areas, each cybersecurity module falls under one or more CyberSecPro targeted cybersecurity capabilities, including Cybersecurity Principles and Management, Cybersecurity Tools and Technologies, Cybersecurity Emerging Digital Technologies, and Offensive Cybersecurity Practices. A module can be a course, seminar, workshop, hackathon, summer school, winter school, or other.

CSP001: Cybersecurity Essentials and Management

Basic Level

This training module provides a foundational understanding of cybersecurity essentials and management principles, equipping participants with the knowledge and skills to manage information and cybersecurity in an organisation.

CSP002: Human Factors and Cybersecurity

Basic and Advanced Levels

This training module provides participants with the necessary knowledge and skills about human aspects of cybersecurity at the individual and organisational levels as well as at the strategic, operational, and tactical levels.

CSP003: Cybersecurity Risk Management and Governance

Basic and Advanced Levels

This course focuses on acquainting participants with the principles and requirements for Information Systems (IS) security and privacy. The main phases of an Information Security Management System (ISMS) implementation are described as defined within ISO/IEC 27001. Risk Management and Risk Assessment methodologies are introduced based on standards and best practices. Security Management will involve the development of security reports (e.g. Risk Treatment Plan, Security Policy, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and Security Procedures)

CSP004: Network Security

Advanced Level

This module will provide participants with the necessary knowledge to identify and address the possible security problems and threats associated with the emergence of various types of communication networks and their implicit protocols. In this training process, participants will also learn how these protocols can be used to the benefit of attackers and what can be done to prevent their exploits. The module will also provide ways of post-attack policies in case of a successful attack and measures to ensure privacy and anonymity in communication systems.

CSP005: Data Protection and Privacy Technologies

Advanced Level

This module will provide policies and practices for data protection in terms of security flaws and disastrous events. Further, this comprehensive training module equips individuals and organisations with the knowledge and skills to navigate the ever-evolving landscape of data protection and privacy.

CSP006 - Cyber Threat Intelligence

Advanced Level

The module aims to provide learners with an overview of threat intelligence and management. It allows the learners to analyse the known and unknown threats and determine a course of action to tackle them.

CSP007 - Cybersecurity in Emerging Technologies

Advanced Level

The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge technologies in various industries. As businesses embrace innovations such as the Internet of Things (IoT), artificial intelligence (AI), blockchain, and 5G, robust cybersecurity measures become paramount. This module aims to provide a comprehensive understanding of the cybersecurity landscape within the context of emerging technologies.

CSP008 - Critical Infrastructure Security

Advanced Level

All aspects of Critical Infrastructure Security that includes different perspectives: technology, policy, and legal.

CSP009 - Software Security

Advanced Level

This CSP delves into the intricacies of software security, building upon foundational cybersecurity knowledge. It provides students with specialized skills and strategies for securing software throughout its entire lifecycle, from design and development to deployment and maintenance.

CSP010 - Penetration Testing

Advanced Level

The objective of this module is to provide trainees with knowledge and skills for penetration testing to uncover any form of vulnerability ranging from small implementation bugs to major system design flaws resulting from coding errors, system configuration faults, design flaws or other operational deployment weaknesses. This course complements and expands upon foundational cybersecurity knowledge, preparing students for real-world security assessments and ethical hacking scenarios.

CSP011 - Cyber Ranges and Operations

Advanced Level

Advanced hands-on network security educational scenario, including simulated cyber environments, deploying countermeasures, and responding to real-world attack scenarios.

CSP012 - Digital Forensics

Advanced Level

The module introduces learners to digital forensics to equip them with the knowledge and skills to undertake cybercriminal investigations that produce digital evidence that may prove a malicious activity.

All Modules