Project No. 101083594 Project start: 2022-12-01

Call: DIGITAL-2021-SKILLS-01 Project duration: 39 months

CyberSecPro

D6.3
Overall Exploitation, Sustainability and Business Plans

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

Related WP	WP6	Dissemination Level	PU/SEN
Lead Participant	ZELUS	Lead Author	Emmanouil Vergis (ZELUS)
Contributing Participants	ACCEU, LAU, UPRC, MAG, ITML, UMA, UNINOVA	Related Deliverables	D6.4 Grouped exploitation plans D6.5 Individual exploitation plans

Abstract: This deliverable defines the exploitation, sustainability, and business framework for the CyberSecPro project beyond its funded duration under the DIGITAL-2021-SKILLS-01 programme. It consolidates the project's four Key Exploitable Results (KERs), sector-specific cybersecurity training modules, structured MOOC pathways, the Moodle-based Dynamic Curriculum Management (DCM) platform and a certification-oriented skills validation approach aligned with the European Cybersecurity Skills Framework (ECSF). The document presents a structured exploitation model based on three progressive deployment scenarios. The deliverable integrates market positioning, competitive analysis, business modelling logic, and indicative financial envelopes to define the operational conditions required for sustainable post-project continuation. The financial analysis focuses on minimum operational sustainability thresholds rather than speculative growth projections. Long-term sustainability is framed around institutional adoption, governance clarity, structured content maintenance, and defined operational responsibilities. The document provides a decision-support framework enabling the consortium to determine the most appropriate continuation model after project closure.

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.

Executive Summary

This deliverable defines the exploitation, business, and sustainability framework for the CyberSecPro project results beyond the project lifetime. It consolidates the Key Exploitable Results (KERs), analyses their market positioning, and presents structured exploitation scenarios supported by indicative financial assumptions and operational considerations.

CyberSecPro delivers four interconnected exploitable results: (i) sector-specific cybersecurity training modules, (ii) structured MOOC learning pathways, (iii) the Moodle-based Dynamic Curriculum Management (DCM) platform, and (iv) a certification-oriented skills validation approach aligned with European competence frameworks. These results can be exploited individually or as an integrated ecosystem, depending on the adoption pathway selected by institutional or enterprise users.

Three exploitation scenarios are defined. Scenario 1 focuses on individual or platform-supported module delivery, targeting individual learners and educational institutions. Scenario 2 expands toward scalable MOOC-based learning and enterprise licensing. Scenario 3 introduces certification-enabled deployment models supported by credential validation services. Each scenario builds upon the technical and educational outputs of the project and assumes gradual, sustainable adoption rather than rapid commercial scaling.

The financial analysis provides indicative annual cost envelopes and revenue logic to illustrate the sustainability requirements of post-project continuation. The analysis does not constitute audited financial forecasting but outlines realistic operational conditions necessary for platform maintenance, content updates, and governance continuity.

Sustainability depends on the establishment of a clear post-project operational structure, ongoing content refresh cycles, and the progressive adoption of institutional licensing models. The deliverable therefore presents both the strategic logic and the operational considerations required to ensure the long-term continuation of CyberSecPro results within the European cybersecurity skills ecosystem.

Document information

Contributors

Name	Beneficiary
George Bolpasis	ZELUS
Eleni Alimperti	ZELUS
Emmanouil Vergis	ZELUS
Michalis Vakallelis	ZELUS
Paulinus Ofem	LAUREA
Christos Douligeris	UPRC
Spiros Borotis	MAGGIOLI
George Kliafas	MAGGIOLI
Vina Roboti	ITML
Thorsten Kliewe	ACEEU
Ruben Costa	UNINOVA
Cristina Alcaraz	UMA

Reviewers

Name	Beneficiary
Vaia Gousdova	FOCAL POINT
Nektaria Kaloudi	SINTEF

History

Version	Date	Contributor(s)	Comment(s)
0.1	2025-06-26	George Bolpasis	1st Draft: Creation of ToC

0.2	2025-09-15	George Bolpasis	2nd Draft with ZELUS contributions
0.3	2025-10-30	Michalis Vakalelis	3rd Draft
0.4	2025-12-01	Eleni Alimperti	4th Draft with UMA, LAU contributions
0.5	29/01/2026 2026-01-29	Eleni Alimperti	5th Draft with ACCEU, ITML, UNINOVA contributions
0.6	2026-02-09	Eleni Alimperti	6th Draft with MAG, UPRC contributions
0.7	2026-02-20	Emmanouil Vergis	7th Draft with introduction, summary and finalizations
0.8	2026-02-26	Vaia Gousdova	1st Review
0.9	2026-02-26	Nektaria Kaloudi	2nd Review
0.91	2026-02-27	Emmanouil Vergis, Michalis Vakalelis	Final document with reviewer comments and high level review
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
	AIS	Automatic Identification System
B	**BMC**	Business Model Canvas
C	**CC BY-NC-SA 4.0**	Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License
	CISO	Chief Information Security Officer
D	**DCM**	Dynamic Curriculum Management
E	**ECSF**	European Cybersecurity Skills Framework
	ENISA	European Union Agency for Cybersecurity
G	**GDPR**	General Data Protection Regulation
	GNSS	Global Navigation Satellite System
H	**HEI**	Higher Education Institution
	HR	Human Resources
I	**IIoT**	Industrial Internet of Things
	IP	Intellectual Property
	IPR	Intellectual Property Rights
	IoE	Internet of Energy
	IoMT	Internet of Medical Things
	IoT	Internet of Things
K	**KA**	Knowledge Area
	KER	Key Exploitable Result
L	**L&D**	Learning and Development
	LMC	Lean Model Canvas
M	**ML**	Machine Learning
	MOOC	Massive Open Online Course
N	**NIS2**	Network and Information Security Directive (EU) 2022/2555

	NCCC	National Coordination Centre
O	**OT**	Operational Technology
S	**SCADA**	Supervisory Control and Data Acquisition
	SIEM	Security Information and Event Management
	SME	Small and Medium-sized Enterprise
	SaaS	Software as a Service
T	**ToC**	Table of Contents
U	**UVP**	Unique Value Proposition
V	**VPC**	Value Proposition Canvas
W	**WP**	Work Package
X	**XAI**	Explainable Artificial Intelligence

Glossary of Terms

A **Adoption Pathway**

The structured process through which institutions, organisations, or individual learners progressively integrate and deploy CyberSecPro training modules, MOOCs, or platform services.

B **Break-even Point**

The level of revenue at which total operational costs are fully covered, ensuring financial sustainability without generating deficit.

Business Model Canvas (BMC)

A strategic management framework used to describe, design, and analyse a business model across nine building blocks, including value proposition, customer segments, revenue streams, and cost structure.

C **Certification-as-a-Service**

A structured service model enabling assessment, credential issuance, validation, and lifecycle management of certifications aligned with defined competence frameworks.

Competence Framework Alignment

The structured mapping of learning outcomes, modules, and assessment criteria to recognised professional skills frameworks, such as the European Cybersecurity Skills Framework (ECSF).

Content Governance

The structured process of reviewing, updating, validating, and maintaining training materials to ensure accuracy, regulatory alignment, and sector relevance.

Cost Envelope

An indicative range of annual operational costs required to sustain platform hosting, content updates, governance activities, and administrative functions.

D **Digital Twin**

A virtual representation of a physical system used to simulate scenarios, including cybersecurity attack and defence modelling, without affecting live infrastructure.

Dynamic Curriculum Management (DCM)

A Moodle-based platform architecture supporting modular training delivery, learner tracking, certification workflows, and curriculum extensibility.

E **Exploitation Scenario**

A structured deployment configuration combining CyberSecPro assets (modules, MOOCs, platform, certification) under defined operational and revenue models.

I **Institutional Licensing**

A structured agreement allowing universities or organisations to deploy CyberSecPro modules or platform services under predefined governance and access conditions.

K **Key Exploitable Result (KER)**

A tangible project outcome with potential for structured post-project deployment, sustainability, or revenue generation.

Knowledge Area (KA)

A defined thematic domain of cybersecurity competence identified through market analysis and aligned with workforce needs.

L **Learning Pathway**

A structured sequence of modules or MOOCs designed to progressively develop competence aligned with specific professional profiles.

M **Micro-credential**

A certification format validating the completion of a defined learning unit or competence set, typically shorter than a full academic qualification.

Modular Training Architecture

A curriculum structure composed of independent yet combinable learning units that allow flexible deployment and scalability.

O **Operational Sustainability**

The ability to maintain technical, financial, and governance continuity of project results beyond funded duration.

P **Platform Uptime**

The percentage of time during which the DCM platform remains operational and accessible within a defined reporting period.

Post-Project Governance Model

The defined allocation of roles, responsibilities, and decision-making processes for the continuation of CyberSecPro activities after project closure.

O **Revenue Prognosis**

Indicative estimation of potential revenue under alternative adoption scenarios, based on assumed uptake levels.

S **Sector-Specific Cybersecurity Training**

Training tailored to operational environments such as healthcare, maritime, and energy, incorporating sector-relevant technologies, risks, and regulatory requirements.

Skills Gap

The measurable difference between workforce demand for cybersecurity competences and the available supply of trained professionals.

Sustainability KPI

Key Performance Indicator used to monitor operational, financial, technical, and educational sustainability after project completion.

V **Value Proposition**

A clear statement describing the functional, strategic, and operational value delivered to specific customer segments.

Value Proposition Canvas (VPC)

A structured analytical tool mapping customer needs (jobs, pains, gains) against product features (pain relievers, gain creators).

W **Workforce Upskilling**

Structured training aimed at enhancing the competences of existing professionals to meet evolving market or regulatory demands.

1 Introduction

1.1 Purpose of the Document

The purpose of this document is to define the structured exploitation and sustainability framework for the CyberSecPro project outputs. It builds upon the market analysis conducted in D2.1 and the training development and implementation results of Work Packages 3 and 4. The document outlines how the Key Exploitable Results (KERs) can be maintained, positioned, and operationalised beyond the funded project duration.

The document does not define legally binding commercial arrangements or final contractual terms between partners. Instead, it presents the operational logic, potential revenue models, indicative cost assumptions, and governance considerations required to support informed post-project decision-making. It serves as a structured reference for partners when defining future cooperation models or institutional continuation pathways.

1.2 Methodology for exploitation, sustainability and business planning

The development of the CyberSecPro exploitation and sustainability framework followed a structured and progressive methodology designed to translate project results into operational and financially sustainable post-project pathways. The approach was grounded in evidence generated within the project, particularly the market demand analysis conducted in D2.1 and the training design and implementation outcomes of Work Packages 3 and 4.

The methodological process consisted of three consecutive analytical layers. First, the Key Exploitable Results (KERs) were clearly defined and functionally separated in order to distinguish between educational content assets (training modules and MOOCs), technical infrastructure (DCM platform), and certification-oriented recognition mechanisms. This separation enabled structured assessment of operational requirements and sustainability dependencies for each asset.

Second, customer segments and adoption contexts were identified based on the skills gap analysis and observed participation patterns during project implementation. The primary segments considered include higher education institutions, training providers, sector-specific organisations, and individual learners. Rather than assuming immediate large-scale commercial uptake, the methodology prioritised realistic institutional adoption pathways and gradual scaling through structured deployment models.

Third, business model logic was developed using standard business modelling frameworks as internal structuring tools. The Lean Model Canvas was used at an early stage to examine problem–solution alignment and identify the value proposition for each KER. These insights were then consolidated into scenario-based Business Model Canvas structures to analyse value delivery mechanisms, cost components, potential revenue streams, and resource dependencies. The Value Proposition Canvas supported refinement of the alignment between identified customer needs and the functional characteristics of the CyberSecPro assets. These frameworks were used to organise reasoning and decision logic rather than as standalone outputs.

The sustainability dimension was incorporated through the identification of recurring operational costs, governance requirements, and risk factors affecting post-project continuation. Financial sustainability envelopes were constructed to illustrate the minimum conditions required to maintain platform functionality, content relevance, and administrative oversight. These financial illustrations are indicative and are intended to inform strategic planning rather than provide audited forecasts.

Overall, the methodology emphasises operational realism, progressive adoption, and structured governance considerations. It does not assume the creation of a new commercial entity within the project

scope but instead provides a decision-support framework that enables partners to define appropriate continuation models prior to project closure.

1.3 Document Structure

This deliverable is structured to progressively present the exploitation logic of CyberSecPro. Section 2 describes the Key Exploitable Results and defines the exploitation scenarios. Section 3 analyses the relevant market context and positioning considerations. Section 4 presents the business logic and scenario-based business models. Section 5 defines the go-to-market approach and adoption pathway. Section 6 provides indicative financial assumptions and sustainability calculations. Section 7 defines governance and long-term sustainability considerations. The final sections consolidate conclusions and forward-looking recommendations.

2 Overall Exploitation Plan

2.1 Exploitable results and their value proposition

The **CyberSecPro project** delivers a cohesive set of four Key Exploitable Results (KERs) that collectively form a scalable and sustainable ecosystem for cybersecurity education and workforce development. Each KER has commercial potential on its own and creates amplified value when integrated with the others.

2.1.1 Overview of Key Exploitable Results

- **KER 1 - Cybersecurity Training Modules:** Sector-specific, practical training modules delivering hands-on skills through online, hybrid, or in-person formats. Modules are aligned with job-market needs and developed by EU academic experts.
- **KER 2 - Cybersecurity MOOCs**: Structured learning paths that combine multiple modules into comprehensive, sector-focused tracks. Delivered via the CyberSecPro Platform for scalable, certification-ready training for individual and enterprise users.
- **KER 3 - CyberSecPro Platform (DCM System):** A Moodle-based Dynamic Curriculum Management system serving as the core technical infrastructure for content delivery, user tracking, and certification management. Customizable for universities, training providers, and enterprises.
- **KER 4 - Certification Scheme:** A proposed certification system recognizing practical skills acquired through CyberSecPro training modules and MOOCs, linked to ECSF competency frameworks and EU recognition standards.

2.1.2 Strategic Value Proposition

CyberSecPro's exploitable results address the shortage of sector-specific, practical cybersecurity training. The value proposition rests on four strategic pillars:

1. Sector Specialization

CyberSecPro KERs are specifically designed for healthcare, maritime, and energy sectors. This specialization addresses the unique operational contexts and challenges of these industries. Organizations in these sectors need training that reflects their specific environments and requirements.

2. EU Academic Credibility and Quality

All training content is developed and validated by consortium universities and research institutions across Europe. This academic foundation provides pedagogical quality and institutional credibility. For educational institutions and learners, this EU consortium backing is a key differentiator.

3. Practical, Job-Ready Focus

Training emphasizes hands-on skills, real-world scenarios, and practical applications. This approach bridges the gap between theoretical cybersecurity education and actual workplace needs, helping learners become job-ready more quickly.

4. Integrated Ecosystem Approach

The four KERs function both independently and as an integrated solution. Organizations can adopt individual modules for targeted training, implement comprehensive MOOC programs, deploy the DCM platform as infrastructure, or utilize the certification scheme for competency validation. This flexibility accommodates diverse customer needs.

2.1.3 Market Positioning and Target Segments

Table 1: Customer segments and needs

Customer Segment	Needs Addressed by CyberSecPro
University Students & Graduates	Affordable, job-ready training bridging academic theory and practice.
Mid-Career Professionals	Flexible, self-paced MOOC paths for upskilling and certification.
Corporate HR / L&D Departments	Scalable and trackable enterprise training solutions with progress dashboards.
Universities & Training Providers	Ready-to-deploy Moodle-based platform with built-in content and certification flows.
Sector-Specific Organizations	Tailored training modules for health, energy, and maritime industries.

The project partners have identified distinct customer segments with specific needs that CyberSecPro KERs address:

Individual Learners

University students, recent graduates, and career changers seeking entry into cybersecurity professions need practical, affordable training that bridges academic theory and workplace requirements. Training Modules and MOOCs provide accessible pathways to job-ready skills.

Mid-Career Professionals

Established IT and security professionals require flexible, self-paced opportunities for specialization and staying current with evolving threats and technologies. MOOCs deliver structured learning paths that accommodate work schedules while providing career advancement opportunities.

Corporate HR and Learning & Development

Organizations implementing workforce upskilling programs need scalable, trackable training solutions. MOOCs and the DCM Platform enable efficient deployment of standardized training across distributed workforces with comprehensive progress monitoring.

Educational Institutions

Universities, training providers, and public sector education programs require ready-to-deploy curriculum and infrastructure for delivering cybersecurity education. The DCM Platform combined with Training Modules provides solutions that accelerate program launch while maintaining quality standards.

Sector-Specific Organizations

Healthcare facilities, maritime operators, and energy utilities need cybersecurity training that addresses their specific operational contexts. CyberSecPro offers training solutions tailored to their sector needs.

2.1.4 Exploitation Approach and Commercial Viability

CyberSecPro KERs support multiple exploitation scenarios with distinct revenue models:

Direct-to-Learner Model

Individual access to Training Modules and MOOCs through subscription or pay-per-course models. This approach targets students, career changers, and professionals seeking self-directed learning. Revenue generation is scalable with relatively low customer acquisition costs through digital channels.

Enterprise Licensing Model

Corporate subscriptions providing organization-wide access to MOOCs and training content. This B2B model delivers higher revenue per customer with longer contract terms. Enterprise customers also represent opportunities for platform licensing and customization services.

Institutional Partnership Model

Platform deployment and content licensing to universities and training institutions. This model creates stable revenue streams while expanding market reach through partner networks. Institutions serve as both customers and distribution channels.

Certification Revenue Model

Professional certification fees and credential verification services. This model creates recurring revenue while building a recognized credential ecosystem that enhances the value of training offerings.

Public Sector Partnerships

Collaborations with government agencies and EU-funded workforce development programs. These partnerships provide scale, visibility, and alignment with public policy objectives.

Intellectual property rights

Exploitation activities proposed in the current deliverable will be implemented in full compliance with the Grant and Consortium Agreements concerning ownership and access rights and do not imply the allocation of additional eligible costs under the current Grant Agreement.

2.1.5 Competitive Differentiation

CyberSecPro's competitive position is strengthened by several factors:

- **European Consortium Validation:** Multi-national academic collaboration provides credibility and trust.
- **Sector-Specific Depth:** Concentrated expertise in healthcare, maritime, and energy cybersecurity rather than generic coverage.
- **Open-Source Foundation:** Moodle-based platform architecture appeals to educational and public sector customers while avoiding vendor lock-in.
- **Practical, Job-Market Focused:** Emphasis on hands-on skills and real-world scenarios addresses the gap between academic education and employer needs.
- **Affordable Access:** Pricing designed to enable broad participation, reflecting public benefit mission while maintaining sustainability.

2.1.6 Market Opportunity

The market opportunity for CyberSecPro is driven by structural and persistent shortages in cybersecurity skills across Europe, combined with increasing regulatory and sector-specific compliance requirements. According to EU-level workforce assessments and ENISA reporting, the demand for cybersecurity professionals continues to exceed supply, particularly in critical infrastructure sectors such as healthcare, energy, and maritime. These sectors face accelerated digitalisation and increased exposure to operational technology (OT) and interconnected systems, which require specialised cybersecurity capabilities beyond generic IT security knowledge. The global cybersecurity training market has demonstrated sustained growth, with multi-billion-euro annual volume and double-digit compound annual growth rates projected through 2030. However, a substantial portion of this market is concentrated in horizontal, certification-preparation or awareness-oriented offerings. Sector-specific, ECSF-aligned, modular, and institution-ready solutions remain comparatively underdeveloped.

Within the European context, the addressable market for CyberSecPro can be segmented into three primary layers:

First, higher education institutions and vocational training providers seeking ready-to-deploy curricula aligned with European frameworks. These institutions represent a structurally stable segment with recurring curriculum renewal cycles and increasing pressure to integrate ECSF-aligned pathways.

Second, sector-specific organisations in health, energy, and maritime domains that require practical upskilling of technical and operational staff in response to NIS2 and related regulatory developments. These organisations represent medium- to high-value institutional adoption potential, particularly under structured licensing models.

Third, individual learners and professionals pursuing reskilling or career advancement in cybersecurity. This segment provides scalable but price-sensitive demand and is best approached through modular and bundled learning pathways.

CyberSecPro does not aim to capture the entirety of the European cybersecurity training market. Instead, it strategically positions itself within a defined niche: sector-specific, modular, ECSF-aligned cybersecurity education supported by a replicable Moodle-based infrastructure. This focused positioning reduces direct competition with global MOOC platforms and allows targeted institutional penetration rather than mass-market dependency. The opportunity therefore lies not in volume dominance, but in structured institutional integration within critical sectors and EU-aligned education ecosystems.Detailed Business Model Canvases for each exploitation scenario are presented in Section 4, with financial projections and go-to-market strategies elaborated in Sections 5 and 6.

2.2 Description of each KER

Below are the descriptions of the defined CyberSecPro Key Exploitable Results.

2.2.1 KER 1: Cybersecurity Training Modules

Individual, sector-specific training courses developed by project partners. These modules cover a wide range of cybersecurity topics and are designed to be delivered in online, hybrid, or in-person formats. They are aligned with job market needs and offer practical, hands-on knowledge.

CyberSecPro currently offers a total of 72 hands-on cybersecurity training modules in the field of cybersecurity (cf. D3.3-D3.5 with 25, 24 and 23 modules respectively) with basic and advanced approaches under diverse attendance formats (online/in-person/hybrid), and heterogeneous modular learning processes delivered through courses, seminars, hackathons, Summer Schools, etc. All these modules - currently located in the DCM platform - have been designed, developed and implemented by EU experts, either from the Academy and Industry, considering both general and specific security issues in three relevant strategic sectors: energy, maritime and healthcare.

Through these modules, CyberSecPro aims to: (i) reduce the effects of traditional courses with reduced pragmatic perspective, in which the training core focuses mainly on purely theoretical content, (ii) comply with social diversity without discrimination and facilitate access without economical limitations, in addition to (iii) consolidating the labour market according to its current needs. Moreover, the zero-cost modular approach and the drive to create diverse practical approaches (iv) promote the useful acquisition of knowledge and skills in the real world, (v) improve employability, professionalism and experience, as well as (vi) facilitate the start of a professional career through flexible modules specific to each sector. More specifically, we identify four relevant groups who could gain benefits from these training modules:

- **Students**, including doctoral, postgraduate, undergraduate or any other previous professional training cycle;

- **Recent graduates** interested in improving their professional Curriculum Vitae / portfolio as well as their knowledge and skills to enter the job market, compete with greater experience and practice in the field of application;
- **IT/OT professionals** who need recycle experiences, knowledge and technical skills by following reskilling training courses;
- **Individuals interested** in learning or changing their professional career to get started in the field of cybersecurity.

For each of these groups, we identify the following Key Exploitable Results:

Students and recent graduates could be introduced with (i) practical and realistic training tailored to the job market based on affordable and flexible modules; (ii) recognition from top EU entities under certificates of attendance that report on their learning activities; and, of course, (ii) acquire the necessary fundamentals to enhance the value of the Curriculum Vitae / portfolio and thereby become more competitive. All of this can even help new generations to: (i) develop skills for the real world, (ii) improve their employability in the field of cybersecurity with specialisation in the specific strategic sectors and, subsequently, (iii) embark them on specific professional careers, as well as (iv) encouraging them to undertake advanced training, obtain certifications and gain more practical experience. What is more, the latter may even (v) break down current barriers and fears to anticipate technical solutions that benefit the stability of an organization or organizations with an impact social and economic. Therefore, there is a clear cascading effect, the foundation of which lies in the training to generate social responsibility, well-being and economy.
IT/OT professionals could (i) intensify their skills and knowledge in specific topics of cybersecurity, and (ii) expand the learnt lessons to their profession fields. This not only enhances the security required today in operational environments but also makes it easier for today's professionals to be prepared for potential risks. It can also help them distinguish threating situations, know when to be proactive and reactive according to the situation, identify possible solutions, and know how and when to comply with security policies. Moreover, understanding specific cybersecurity terms, comprehending the problems and knowing how to address them correctly can also (iii) facilitate interdisciplinary communication in heterogeneous applications where multiple disciplines coexist to achieve a common goal; and even (iv) overcome the same fears mentioned in the previous point through practical experience. Balanced preparation, in theoretical and practical terms, undoubtedly enables IT/TO professionals to make decisions with a more solid and practical vision.
Individuals interested could (i) gain their first experiences in the field of cybersecurity to decide whether they wish to continue pursuing their interest and, therefore, grow in this field, either voluntarily or professionally, but also could (ii) consolidate a strong labour market. Indeed, CyberSecPro training modules could help attract and/or keep European talent, establishing a more competitive economy not only in the European territory but also in its respective Member States.

2.2.2 KER 2: Cybersecurity MooCs

The second Key Exploitable Result (KER 2) of CyberSecPro is a portfolio of Cybersecurity Massive Open Online Courses (MOOCs) that provide structured, online learning paths by bundling multiple learning components into thematic and/or sector-focused tracks. Delivered through the CyberSecPro Platform (Moodle/DCM) or other platforms, these MOOCs enable scalable, flexible, and repeatable training provision, addressing the needs of both individual learners and organisational customers seeking accessible upskilling opportunities aligned with European skills frameworks.

KER 2 directly targets mid-career professionals seeking upskilling and/or certification-oriented progression, and corporate HR / Learning & Development (L&D) departments requiring scalable training for employees. In this scenario, value creation is driven by the platform’s ability to structure learning pathways, manage access, and track learner progress, while sustainability is enabled through subscription-based access and enterprise licensing models, complemented by certification alignment where applicable.

In practical terms, CyberSecPro MOOCs are designed as complete online courses with defined learning outcomes, workload, delivery mode and assessment logic, and are offered in formats suitable for professional learners (e.g., self-paced provision). For example, CyberSecPro: Cybersecurity Fundamentals is a self-paced MOOC (estimated 130 hours, 5 ECTS) that builds foundational competence through quizzes, practical challenges and a capstone-style project. A complete CyberSecurity Toolkit MOOC provides a strongly hands-on pathway (also self-paced, estimated 130 hours, 5 ECTS) focused on practical tooling, security tasks, and continuous verification through quizzes and embedded challenges, delivered virtually via the DCM environment. Complementing technical tracks, the Human Factors of Cybersecurity MOOC (Advanced; 16 weeks, 6 ECTS) addresses behavioural, organisational, and socio-technical dimensions of cybersecurity, using an academic-style written assessment (essay) to evaluate competence acquisition.

Overall, KER 2 operationalises CyberSecPro's integrated training ecosystem by transforming modular content into coherent learning pathways that are easier to adopt, deploy and scale through a common platform infrastructure. It provides a concrete exploitation-ready offering for both B2C and B2B uptake, enabling repeatable delivery, measurable learner progression, and alignment with EU-oriented competence approaches through the CyberSecPro platform

2.2.3 .KER 3: CyberSecPro DCM Platform

The CyberSecPro Dynamic Curriculum Management (DCM) Platform represents one of the most strategically significant Key Exploitable Results of the project, serving as the core digital infrastructure that enables the delivery, monitoring, evolution, and long-term sustainability of the CyberSecPro training ecosystem.

Developed and operated by UNINOVA and populated with training material that has been developed by the project partners, the DCM is a Moodle-based platform customised to support the specific requirements of sector-oriented cybersecurity training in the domains of healthcare, maritime, and energy. While the training modules (KER 1) and structured learning paths (KER 2) constitute the educational content layer of CyberSecPro, the DCM platform provides the operational backbone that makes this content reusable, scalable, measurable, and exploitable beyond the project lifetime.

Platform Role and Strategic Value

The CyberSecPro DCM platform functions as a training delivery and governance engine, enabling Higher Education Institutions (HEIs), training providers, and security-sector organisations to deploy modular cybersecurity curricula efficiently. Its strategic value lies in the fact that it supports not only content hosting, but also the broader lifecycle of professional training programmes, including:

- learner enrolment and role-based access control,
- structured course bundling and learning pathway management,
- progress tracking and engagement monitoring,
- certification-ready reporting workflows,
- feedback loops and quality assurance analytics.

In this sense, the DCM is not merely a repository of courses, but an exploitable infrastructure that operationalises CyberSecPro's vision of a dynamic, extensible, and ECSF-aligned cybersecurity competence ecosystem.

Value Proposition Canvas (VPC) Perspective

From an exploitation standpoint, the DCM platform provides a strong Value Proposition for multiple target groups:

- Universities and HEIs benefit from a ready-to-deploy curriculum platform that accelerates the launch of cybersecurity programmes aligned with EU frameworks and labour market needs.

- Professional training providers gain access to an operational environment that supports modular delivery, learner monitoring, and structured certification pathways.
- Sector-specific organisations and SMEs can use the platform as an upskilling and reskilling tool for staff in critical infrastructures, without needing to develop training infrastructure from scratch.
- Learners and professionals benefit from flexible access to high-quality modules, combined with traceable learning outcomes and potential credential pathways.

The platform therefore supports both direct educational uptake and institutional replication, making it a cornerstone of CyberSecPro's sustainability strategy.

Differentiation and Competitive Advantage

The CyberSecPro DCM platform is differentiated from generic e-learning environments through several unique characteristics:

- Sector-specific depth, supporting cybersecurity training tailored to operational contexts in health, maritime, and energy.
- Dynamic curriculum governance, enabling modular extensibility and continuous evolution rather than static course catalogues.
- Integration with evaluation and analytics, supporting structured monitoring of implementation, learner participation, satisfaction, and learning workload.
- Alignment with ECSF professional profiles, strengthening European-wide recognition and harmonisation of skills development.
- Open and adaptable architecture, avoiding vendor lock-in and supporting deployment across diverse institutional contexts.

These differentiators strengthen the platform's exploitation potential, especially in niches where commercial providers typically offer generic, non-sectorial training.

Exploitation and Sustainability Potential

As highlighted in the broader exploitation scenarios of this deliverable, the DCM platform is the key enabler for multiple sustainability pathways:

- Institutional licensing and deployment, where universities adopt the platform as infrastructure for modular cybersecurity training.
- Enterprise upskilling solutions, where companies access learning paths and reporting dashboards for workforce development.
- Certification-as-a-service models, where the platform supports credential issuance, assessment workflows, and verification services.

Because the DCM integrates delivery, tracking, and reporting, it represents a high-value exploitable asset that can generate recurring institutional partnerships and service-based revenue, while maintaining the project's public-good orientation.

Long-Term Impact

Beyond commercial viability, the DCM platform contributes directly to CyberSecPro's long-term impact objectives by enabling:

- continuous updating of training content in response to evolving threats,
- replication of CyberSecPro modules across European HEIs,
- scalable dissemination through summer/winter schools and professional events,
- creation of a sustainable pipeline of cybersecurity talent for critical sectors.

To further clarify the exploitation potential of KER 3, summarises the main functional service layers of the CyberSecPro DCM platform and their associated sustainability and value-generation opportunities for HEIs, industry partners, and professional learners.

Table 2: Key Exploitable Functionalities of the CyberSecPro DCM Platform

Exploitable Feature / Service Layer	**Description within CyberSecPro DCM**	**Exploitation Value and Sustainability Potential**
Learning Path and Module Delivery	Hosting and structured deployment of sector-specific CSP modules and competence pathways through Moodle-based course organisation.	Enables replication across HEIs and training providers, supporting scalable programme deployment beyond the project lifetime.
User Enrolment and Role Management	Role-based access control for trainees, trainers, coordinators, and administrators, including controlled enrolment workflows.	Supports multi-stakeholder training ecosystems and sustainable governance models for future CSP offerings.
Progress Tracking and Engagement Analytics	Monitoring of participation, activity completion, login frequency, and learner progression across modules.	Provides measurable evidence of training uptake and impact, supporting institutional reporting, KPI monitoring, and continuous improvement.
Assessment and Feedback Workflows	Integration of quizzes, assignments, surveys, and structured module evaluation templates within the DCM.	Enables quality assurance processes and supports evidence-based optimisation of training content and delivery.
Certification and Attendance Validation	Support for Certificates of Attendance and foundations for future micro-credential issuance linked to learning outcomes.	Strengthens employability impact and creates pathways for certification-based sustainability and potential service models.
Admin Portal and Reporting Dashboards	Centralised administrative interface providing aggregated metrics on modules, users, events, satisfaction, and implementation status.	Enables strategic oversight for programme coordinators and supports long-term operational sustainability through data-driven governance.
Integration of Practical Training Infrastructure	Support for labs, cyber ranges, hackathons, and external tools (e.g., SIEM platforms, vulnerability scanners, OT simulators).	Enhances realism and industry relevance, positioning the DCM as an applied training hub for critical infrastructure sectors.
Dynamic Curriculum Evolution and Extensibility	Modular structure allowing continuous updates, addition of new modules, and adaptation to emerging threats and sector needs.	Ensures long-term relevance and scalability, making the platform sustainable as a living European cybersecurity training ecosystem.

2.2.4 KER 4: Certification schemes

The fourth KER is a European certification framework for professional cybersecurity training that addresses a long-standing structural gap in the EU: the absence of a harmonised, quality-assured, and mutually recognisable certification scheme for cybersecurity professional training programmes. This gap has resulted in a fragmented landscape where training offers vary widely in methodology, learning outcomes, and assessment approaches, producing certifications with limited interoperability and uneven assurance of competence. This fragmentation is even more distinct in sector-specific cybersecurity training, where programmes are often developed in isolation within individual industries and national contexts. Although many cybersecurity competencies are transversal, professionals face restricted cross-sector mobility, due to the lack of a common certification reference that validates sector-specific capability in a consistent and comparable manner.

To resolve this, CyberSecPro delivers a certification schema for professional, sector-specific cybersecurity training, defined as a structured programme, or a coherent set of modular learning units, mapped to clearly specified sector-oriented knowledge, skills, and competencies and paired with standardised assessment requirements. In line with D5.3, the schema is built on three interdependent pillars namely, (i) assessment criteria, (ii) evaluation methodology, and (iii) role profiles—ensuring that what is assessed, how it is assessed, and for which role/level it is assessed remain consistently aligned and credible across contexts.

A central feature of the present KER is that the schema is designed for formal recognition and approval by a competent higher-level European authorities. The schema is explicitly aligned to the European Cybersecurity Skills Framework (ECSF), using the ECSF as the "skills language" and alignment backbone (profiles, tasks, skills/knowledge and EQF-aligned proficiency levels). This prevents arbitrary role naming and "knowledge-only" certification claims, and ensures that certification signals what role and level a professional can actually perform.

Under this certification approach, learners who successfully complete a full programme or certified modules aligned with the schema receive a certificate issued or endorsed by the competent authority (or its delegated bodies). This certificate will serve as formal and portable proof of competence, providing employers and clients with reliable assurance that the holder meets EU-aligned proficiency standards for cybersecurity practice in a specific sectoral context. In D5.3, the certificate design is also standardised through common elements (e.g., module code/title, learner identity, providers, micro-credentials and/or ECTS credits, hours, dates, level, participation mode, and verifiable references such as QR/website), supporting transparency and trust.

The certification schema is intended to be flexible, scalable, and stackable. It supports diverse providers (academia, professional associations, industry bodies, and private training organisations), while maintaining common requirements for learning outcomes, practical competence development, and validation. Importantly, D5.3 operationalises comparability by introducing formulas to quantify micro-credentials based on workload and training characteristics, and by proposing a mapping from micro-credentials to ECTS credits, including a dedicated approach for course-type modules that incorporates an explicit mentoring factor. This enables transparency in training volume, supports portability, and facilitates alignment with European qualification practices.

The methodology underpinning the extraction and consolidation of this certification schema—building on D3.2 and finalised in D5.3 includes (i) an updated analysis of EU and international certification landscapes, (ii) the consolidation of common elements and measurement scales, and (iii) the definition of standards and factors feeding the final CyberSecPro certification schema.

2.3 Integrated Exploitation Scenarios

The Key Exploitable Results of CyberSecPro may be deployed individually or combined into structured exploitation configurations depending on the adoption context and target audience. While each KER

represents a distinct asset, training modules, structured MOOCs, the DCM platform, and certification-oriented recognition mechanisms, their long-term sustainability is strengthened when integrated into coherent operational scenarios. This section defines three progressive exploitation scenarios that translate the project outputs into structured post-project deployment pathways. The scenarios do not represent mutually exclusive commercial products. Instead, they describe different levels of integration and operational maturity.

Scenario 1 represents the baseline exploitation pathway. In this configuration, the CyberSecPro DCM platform operates as the technical infrastructure for delivering individual sector-specific training modules or the modules are delivered through other means. The primary target groups include higher education institutions, training providers, and individual learners seeking structured cybersecurity upskilling. In this model, the platform provides enrolment management, structured access to modules, progress tracking, and reporting capabilities. The focus is on enabling sustainable access to existing training content with manageable operational overhead. Scenario 1 establishes the minimum operational conditions required to maintain CyberSecPro outputs beyond the project lifetime.

Scenario 2 builds upon the foundational infrastructure by introducing bundled learning pathways through structured MOOCs. In this configuration, individual modules are integrated into thematic or sector-specific tracks that support scalable delivery for institutions and organisations. The scenario is particularly relevant for enterprise upskilling programmes, multi-department university deployments, and structured professional training initiatives. Scenario 2 therefore represents a scaling pathway in which the CyberSecPro ecosystem transitions from standalone module delivery to structured programme-level deployment.

Scenario 3 represents the most advanced integration level and introduces structured certification-oriented validation mechanisms aligned with European competence frameworks. In this configuration, the DCM platform supports assessment workflows, credential issuance processes, and documentation of learning outcomes mapped to ECSF profiles. It introduces higher value potential but also increased operational responsibility.

3 Market Analysis

3.1 Cybersecurity training market overview

This section presents an overview of the cybersecurity professional market analysis (D2.1) conducted as part of work package 2 of the CyberSecPro project.

Purpose and Scope

The primary aim of the cybersecurity professional market demand and supply analysis is to examine cybersecurity skills gaps across the EU critically. It focused on aligning industry demand with the academic supply of cybersecurity workforce talent. Given the complexity and variability of cybersecurity skill nomenclature across EU member states, the analysis leveraged the European Cybersecurity Skills Framework (ECSF) and harmonised outcomes from previous EU-funded cybersecurity workforce skills development initiatives. It also prioritised the critical sectors of health, energy and maritime. However, the analysis findings were not limited to the prioritised areas; they also spanned other sectors. Further details on sector-based market analysis are provided in later sections.

Method

In conducting the market analysis, the project deployed a mixed-methods approach, including a desktop research to analyse current cybersecurity curricula and skills frameworks in Europe. Popular international frameworks, such as NIST's NICE, were also considered in the analysis. A market-demand survey polling of industry professionals was also conducted. Data collection was also conducted through expert workshops and seminars that brought together industry and academic stakeholders.

Summary of Key Findings

- One of the key findings of the professional market analysis is a significant skills gap in Europe. The demand for skilled cybersecurity professionals outpaced the supply of training from HEI academic programmes and other training institutes. This outcome aligns with previously published findings.
- During the analysis, over 25 essential cybersecurity knowledge areas and more than 25 cybersecurity skills were determined to be in demand across the three targeted sectors of health, energy, maritime and other sectors.
- In comparing the demand and supply skills gap, 18 concrete cybersecurity knowledge and skills areas were identified as the most dominant areas, where gaps exist. Thus, they indicate the "pressing and urgent" practical cybersecurity workforce skills required across Europe.
- In addition to the three-sectoral analyses, cybersecurity workforce skills were identified to be mostly cross-sectoral. This implies that the identified skills are insufficient across all economic sectors.

Table 3: Summary of cybersecurity market demand and supply analysis

Focus	**Market Demand: Knowledge Areas & Hands-on Skills**	**Market Supply: HEIs & training providers**	**Gaps**
Core knowledge areas (cross-sector)	Risk management & compliance; network & cloud security; incident response & digital forensics; secure software engineering/DevSecOps; identity & access management; data protection & privacy; security architecture & governance; threat intelligence.	European programmes broadly cover fundamentals and frameworks, but sector depth and ECSF-aligned pathways are uneven. Coverage varies by country and initiative.	Limited sector contextualisation; inconsistent alignment to ECSF roles; emerging tech (e.g., OT/IIoT, cloud-native, container security) underrepresented.
Hands-on practical skills (cross-sector)	Threat detection & analysis (SOC practices), vulnerability assessment, penetration testing, security hardening, incident handling/containment/eradication, log analysis & SIEM, malware analysis basics, digital evidence handling, secure configuration & baselining.	Labs, simulations, and real-world exercises are present but inconsistent; many offerings remain theory-oriented with sporadic practical components.	Shortage of experiential learning (live labs, red/blue-team drills, sector-specific scenarios); limited exposure to modern toolchains and workflows.
Role alignment (ECSF)	High demand for analysts, incident responders, security architects, and governance/compliance professionals; employers in the sector seek job-ready capabilities.	Partial mapping to ECSF is visible across initiatives; pathways to specific roles are fragmented across courses and projects.	Gap between academic outcomes and operational role readiness; need for clearer, stackable, ECSF-mapped competence development.

Key Recommendations

Following the market gap analysis, the implications and recommendations are summarised as follows:

- Enhancement of HEIs and cybersecurity training programmes to better reflect and meet workforce demands for cybersecurity skills.

- Widening of investment in cybersecurity education and continuous training via upskilling and reskilling of the existing workforce.
- Support for the effective adoption and dissemination of the ECSF across educational institutions and training providers. This will, in turn, help standardise and align the cybersecurity workforce skill set across the EU.
- Strengthening of collaboration between industry, academia, governments and other stakeholders towards building a harmonised and responsive cybersecurity workforce landscape.

The findings in D2.1 align with broader EU concerns about the state of HEI cybersecurity curricula and their misalignment with industry needs and the evolving cybersecurity threat landscape. The outcomes also emphasise the need for multi-stakeholder involvement, including HEIs, the private sector, and EU initiatives, to design and develop curricula, implement training programmes, and develop certification schemes. This, in turn, will enable the EU to build and sustain a competent cybersecurity workforce capable of addressing current and emerging threats. Informed by the outcomes and recommendations in D2.1, CyberSecPro developed (Work Package 3) and implemented (Work Package 4) a professional training programme that HEIs and other training providers can adopt.

3.1.1 Energy, Maritime, and Health

72 modules have been defined in WP3 with their corresponding syllabus, 24 for energy, 23 for maritime, and 25 for health. From all these specifications, more than 150 modules (100+ Basic-level, 60+ Advanced-level) have been successfully implemented, such that: 32.32% have been executed in different formats within the energy sector, 27.44% in health, 18.90% in maritime, and 21.34% for general cybersecurity scenarios, reaching 4000+ learners with 27.90% focused on energy, 31.96% on health, 18.09% on maritime, and 22.05% for general cybersecurity.

All these modules have been defined in accordance with the 10 Knowledge Areas (KAs) identified D2.3 as a result of the D2.1 market analysis, and taking into account the 12 ECSF profiles. This feature this reflected both in **Error! Reference source not found.**4 and **Error! Reference source not found.**5. The first highlights the influence that each KA has on the modules implemented, as well as the impact on the end user. The most developed KAs within the project and throughout the modules are those related to Cybersecurity Management, Cybersecurity Tools and Technologies, Cybersecurity Threat Management, and Cybersecurity Risk Management. Similarly, **Error! Reference source not found.**5 details the most developed ESCF profiles within CSP, and specifically in Cybersecurity Risk manager, Cybersecurity Researcher, Chief Information Security Officer (CISO), Cyber Incident Responder, and Penetration Tester.

Table 4: Relevance of the KAs established as part of CSP

Module Name	# Impl. Modules	% Impl. Modules	# Learners	% Learners
Penetration Testing	52	31.90 %	1408	34.59 %
Cybersecurity Tools and Technologies	88	53.99 %	2339	57.46 %
Cybersecurity Management	99	60.74 %	2220	54.53 %
Cybersecurity Threat Management	81	49.69 %	2036	50.01 %

Cybersecurity Risk Management	70	42.94 %	1723	42.32 %
Cybersecurity Policy, Process, and Compliance	30	18.40 %	936	22.99 %
Cyber Incident Response	51	31.29 %	1413	34.71 %
Network and Communication Security	65	39.88 %	1907	46.84 %
Privacy and Data Protection	36	22.09 %	1051	25.82 %
Human Aspects of Cybersecurity	30	18.40 %	811	19.92 %

Table 5: Relevance of the ECSF Profiles in CSP

Module Name	# Impl. Modules	% Impl. Modules	# Learners	% Learners
Chief Information Security Officer (CISO)	56	34.36 %	1364	33.51 %
Cyber Incident Responder	55	33.74 %	1295	31.81 %
Cyber Legal, Policy & Compliance Officer	31	19.02 %	608	14.93 %
Cyber Threat Intelligence Specialist	47	28.83 %	1069	26.26 %
Cybersecurity Architect	34	20.86 %	880	21.62 %
Cybersecurity Auditor	38	23.31 %	726	17.83 %
Cybersecurity Educator	42	25.77 %	1059	26.01 %
Cybersecurity Implementer	41	25.15 %	859	21.10 %
Cybersecurity Researcher	62	38.04 %	1517	37.26 %
Cybersecurity Risk manager	76	46.63 %	1430	35.13 %
Digital Forensics Investigator	36	22.09 %	877	21.54 %
Penetration Tester	53	32.52 %	1342	32.96 %

Therefore, the analyses addressed in D2.1 and the designs and developments of materials in WP3 have been fundamental and critical for the implementation of a significant number of modules designed in line with current market needs and with a relevant impact to the end audience. 57.46% has addressed KA on Cybersecurity Tools and Technologies and 50.01% on Cybersecurity Threat Management, whereas 37.26% of the CSP audience has developed Cybersecurity Researcher and 33.51 % the CISO profile, among others.

3.2 Key trends and emerging technologies in cybersecurity

The cybersecurity landscape is currently undergoing a radical shift due to accelerated digitalization and the transition to a world where “everything is connected with everything”. This complexity has introduced new vulnerabilities and expanded the attack surface, particularly within critical infrastructures such as the health, energy, and maritime sectors.

Across the various research and training deliverables produced by the CyberSecPro project, the following key trends and emerging technologies were identified. These build the basis for the exploitation planning.

3.2.1 Artificial Intelligence (AI) and Machine Learning (ML)

AI and Machine Learning represent a dual-track trend in modern cybersecurity:

AI as a Defensive Tool: AI-driven approaches are increasingly used to create advanced security controls, enhancing network and endpoint security through anomaly detection and behavior analytics. This is particularly vital in the health sector for detecting behavior that could compromise patient confidentiality.

Malicious Use of AI: Conversely, attackers are leveraging AI to automate attacks and create more sophisticated threat vectors, leading to the necessity of "Cybersecurity for AI" to protect AI models from being compromised themselves.

Explainable AI (XAI): In sensitive sectors like healthcare, there is a growing trend toward making AI models transparent and robust so that security analysts can understand the logic behind threat detection.

3.2.2 The Internet of Things (IoT) and Industrial Systems

The integration of the Internet of Things (IoT), Internet of Medical Things (IoMT), and Internet of Energy (IoE) has created significant interdependencies.

Legacy Systems vs. Modern Paradigms: A major trend is the challenge of securing "legacy" devices and protocols while adopting Industry 4.0/5.0 paradigms.

SCADA and Smart Grids: In the energy sector, the move toward Smart Grids, microgrids, and electric vehicle charging infrastructures has introduced new risks to traditional SCADA systems.

3.2.3 Blockchain and Secure Data Sharing

Blockchain technology is emerging as a critical trend for ensuring data integrity and privacy. Its application within the maritime and energy sectors focuses on securing supply chain data and protecting digital transactions from tampering.

3.2.4 Next-Generation Communication and Infrastructure

5G and Quantum Computing: The project identifies 5G security and the future threat of quantum computing to traditional cryptography as essential emerging topics.

Cloud and Edge Computing: As organizations move data to the edge and the cloud, specialized security for virtualized environments and cloud-based security information management has become a high-demand capability.

Digital Twins: The use of Digital Twins for simulation and testing allows for proactive defense by simulating attacks on virtual replicas of critical infrastructure to refine defensive strategies.

3.2.5 Regulatory and Human-Centric Trends

The landscape is heavily influenced by a shift toward "Privacy by Design" and alignment with new EU legislation such as GDPR, NIS2, and the EU Cybersecurity Act. Furthermore, there is an increasing recognition that Human Factors (psychological and social influences) are as critical as technical solutions, leading to a trend of integrating behavioral analysis into cybersecurity defense models.

In summary, the project characterizes the future of cybersecurity as an agile and multidisciplinary field where technical innovation in AI and IoT must be balanced with robust regulatory compliance and an understanding of human behavior.

3.3 Competition Analysis

The European cybersecurity training landscape is characterised by three primary competitor groups: (i) global commercial e-learning platforms, (ii) certification-focused training providers, and (iii) EU-funded or public-sector digital skills initiatives. Each group addresses specific segments of the cybersecurity education market and presents different substitution risks for CyberSecPro.

1. Global Commercial E-Learning Platforms

Platforms such as Cybrary, EC-Council CodeRed, and InfoSec Skills provide large-scale, subscription-based cybersecurity training libraries. Their offerings typically include video-based courses, virtual labs, certification preparation tracks, and role-based learning paths (e.g., SOC analyst, penetration tester, security engineer). These platforms operate primarily under B2C subscription or enterprise licensing models and benefit from established brand recognition and broad content coverage. However, their training content is predominantly horizontal and role-oriented rather than sector-specific. While they provide strong technical skill coverage, adaptation to operational contexts such as healthcare IoMT systems, maritime navigation infrastructure (AIS/GNSS/ECDIS), or energy-sector SCADA environments is limited. Furthermore, alignment with the European Cybersecurity Skills Framework (ECSF) is not systematically embedded in most global commercial offerings. Their business models also focus on centralized SaaS delivery rather than institutional curriculum integration within European higher education systems. For CyberSecPro, these platforms represent indirect competition at the individual learner level, particularly in technical upskilling. They represent lower substitution risk for sector-specific institutional deployment within EU-aligned education frameworks.

2. Certification-Focused Academies and Vendor-Aligned Training

Providers such as EITCA Information Security Academy and vendor-aligned certification programmes (e.g., CompTIA Security+, CEH training providers, ISO 27001 auditor training) focus on structured certification pathways and examination-based credentialing. Their value proposition centres on globally recognised credentials, exam preparation, and formal validation of knowledge. These providers compete directly in the certification and employability domain. However, they typically emphasise exam readiness rather than modular sector-specific competence development. Their training logic is certification-driven rather than curriculum-driven. Additionally, integration into institutional higher education curricula or sector-tailored contextualisation is often secondary to exam alignment. For CyberSecPro, these providers represent moderate substitution risk under Scenario 3 (certification-enabled model), particularly if CyberSecPro's certification logic lacks clear differentiation or governance maturity. However, CyberSecPro's ECSF alignment and sector contextualisation provide differentiation in European workforce alignment rather than global vendor certification equivalence.

3. EU-Funded and Public Digital Skills Initiatives

Several initiatives funded under the Digital Europe Programme and related EU instruments focus on cybersecurity upskilling, workforce development, and digital competence strengthening. These projects often develop training frameworks, pilot programmes, or specialised academies targeting SMEs, public administrations, or specific professional groups. While these initiatives contribute to a growing ecosystem of EU-supported cybersecurity education, many are project-based, time-limited, or focused on framework development rather than replicable modular infrastructure. Overlap risk exists, particularly in awareness-level or general cybersecurity upskilling domains.

CyberSecPro differentiates itself through the combination of:

- Sector-specific modular content (health, energy, maritime)
- ECSF-mapped competence alignment
- Moodle-based infrastructure enabling institutional replication
- Integrated pathway logic (modules, MOOCs and validation)

Rather than competing on scale or generic breadth, CyberSecPro positions itself within a defined niche of sector-integrated, EU-aligned, curriculum-ready cybersecurity education.

Comparative Positioning Summary

Compared to large global training platforms, CyberSecPro places structured emphasis on sector-integrated curricula in healthcare, energy, and maritime contexts, while operating at smaller scale and with more limited content breadth.

Compared to certification-oriented academies, CyberSecPro prioritises modular competence pathways aligned with ECSF professional profiles, with certification serving as validation of learning outcomes rather than preparation for proprietary vendor examinations.

Compared to many EU-funded digital skills initiatives that focus on framework development or pilot-level training, CyberSecPro integrates modular content with a deployable Moodle-based infrastructure designed for institutional replication and post-project sustainability.

The competitive strategy therefore focuses on institutional embedding within critical infrastructure sectors, leveraging ECSF alignment and public-good orientation, rather than direct confrontation with high-scale commercial SaaS platforms.

3.4 Target Audience and user profiles

CyberSecPro aims to serve a multifaceted target audience, ranging from individual learners to large-scale industrial organisations, united by the shared objective of addressing the European cybersecurity skills gap. This audience is understood as a dynamic ecosystem in which Individual Learners constitute the future talent pipeline, Educational Institutions act as key enablers for competence development, validation, and scalable uptake within education and training systems, and Sector-Specific Organisations and SMEs function as the primary engines for commercial, technological, and market-oriented exploitation of project results.

The project's exploitation strategy specifically categorizes these target audiences into distinct segments based on their operational needs and the Value Proposition of the project's Key Exploitable Results (KERs).

3.4.1 Primary Target Segments

The consortium will target five overarching customer segments that serve as the foundation for the project's exploitation plans:

- Individual Learners: This group includes university students (undergraduate to doctoral levels), recent graduates, and career changers who require practical, affordable training to transition into cybersecurity professions.
- Mid-Career Professionals: Established IT and security professionals who seek flexible, self-paced opportunities to specialize in emerging technologies or stay current with evolving threat landscapes.
- Corporate HR and Learning & Development (L&D) Departments: Organizations requiring scalable and trackable training solutions to upskill distributed workforces effectively.
- Educational Institutions: Universities and vocational training providers that need ready-to-deploy curricula and technical infrastructure, such as the Moodle-based DCM System, to accelerate their program offerings.
- Sector-Specific Organizations: Critical infrastructure operators within the healthcare, maritime, and energy sectors that require training tailored to their unique operational contexts and regulatory requirements.

3.4.2 Detailed User Profiles and ECSF Alignment

In alignment with the European Cybersecurity Skills Framework (ECSF), CyberSecPro training modules are designed to support twelve specific professional profiles. The target audience includes, but is not limited to, the following roles:

- Technical Specialists: This includes Security Analysts, System Administrators, Network Engineers, and Developers focused on secure coding practices.
- Operational Experts: Cyber Incident Responders, Digital Forensics Investigators, and Ethical Hackers/Penetration Testers who require immersive "Learning Factory" environments.
- Strategic Leaders: Chief Information Security Officers (CISOs), IT Managers, and Executives responsible for organizational risk management and governance.
- Compliance and Legal Officers: Professionals, such as Auditors and Privacy Officers, who must navigate complex regulatory frameworks like GDPR and NIS2.
- Public Sector and Policy Bodies: Stakeholders from Law Enforcement, Government Agencies, and policy-making entities like ENISA and NCCCs.

3.4.3 Inclusivity and Demographic Targets

In line with the CyberSecPro project inclusivity and demograph targets (e.g. minimum of 150 trainees who are women or non-binary individuals; at least 70 trainees over the age of 45; at least 80 non-ICT graduates), the exploitation plans also aim to support gender and diversity by providing exploitation plans that target a wide variety of stakeholders.

3.4.4 Sector-Specific User Contexts

Beyond general cybersecurity skills, user profiles are further refined by the operational challenges of the three target sectors of CyberSecPro:

- Healthcare Users: e.g. focus on protecting sensitive patient data and securing connected medical devices (IoMT).
- Energy Users: e.g. focus on safeguarding SCADA systems, Smart Grids, and ensuring the resilience of critical energy distribution assets.

- Maritime Users: e.g. focus on unique systems such as AIS, GNSS, and ECDIS, which are critical for the security of transport logistics and coastguard operations.

4 Business and Exploitation Strategy

The development of CyberSecPro's business and exploitation framework followed a **Lean and iterative methodology** designed to progressively evolve conceptual ideas into structured, market-validated business models. The process, led by ZELUS, adopted the **Lean Startup and Business Model Canvas (BMC)** approaches, complemented by the **Value Proposition Canvas (VPC)** and **Unique Value Proposition (UVP)** formulations. This methodology ensured that each **Key Exploitable Result (KER)** was analysed not only in terms of its technical and educational merit, but also in relation to **market needs, customer segments, and sustainability potential**.

4.1 Business Model Canvas Methodology for each Exploitation Strategy Scenario

The methodological flow consisted of four consecutive stages:

4.1.1 Lean Model Canvas Development

At the early stage, ZELUS applied the **Lean Model Canvas (LMC)** to identify each KER's *problem-solution fit*. The LMC allowed the team to focus on key assumptions — the customer problem, proposed solution, value metrics, and early adopter profiles. This lightweight, hypothesis-driven tool provided a starting point to test initial value propositions and to ensure alignment with real-world needs.

4.1.2 Transition to Business Model Canvas (BMC)

Insights from the Lean Canvas were then expanded into full **Business Model Canvases** for each exploitation scenario.
The BMCs were developed following Osterwalder and Pigneur's nine-block framework, covering:

- Customer Segments
- Value Propositions
- Channels
- Customer Relationships
- Revenue Streams
- Key Resources
- Key Activities
- Key Partners
- Cost Structure

This step enabled a comprehensive understanding of how each KER could generate, deliver, and capture value, both individually and as part of the integrated CyberSecPro ecosystem.

4.1.3 Value Proposition Canvas (VPC) Refinement

Once the overall business model logic was defined, ZELUS and partners created **Value Proposition Canvases** for each key customer segment.

The VPCs identified the *customer jobs*, *pains*, and *gains* and matched them with the *product's pain relievers* and *gain creators*. This process ensured that the offer design was clearly connected to actual user needs and sectoral expectations (e.g., students, professionals, enterprises, universities).

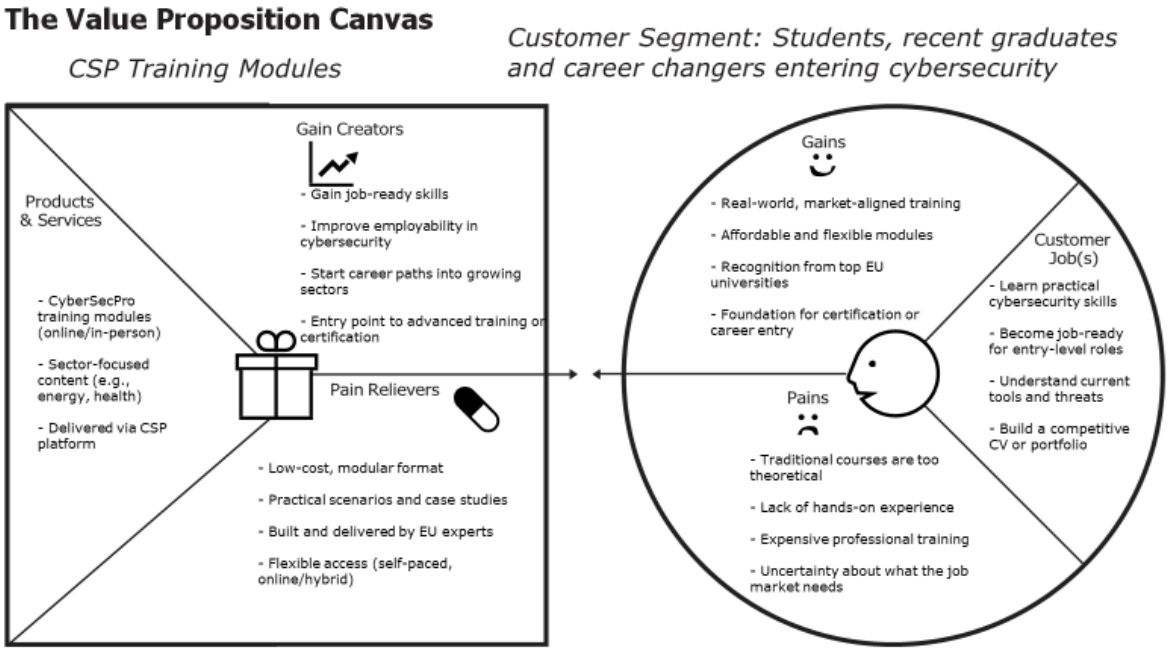
4.1.4 Unique Value Proposition (UVP) Formulation

Finally, insights from both VPC analyses were consolidated into concise **Unique Value Propositions** per KER and scenario. Each UVP articulated a compelling, evidence-based statement that summarized why customers would choose CyberSecPro offerings over alternatives. These UVPs now serve as the foundation for building the BMCs for each KERs combination while also serving for marketing, communication, and positioning strategies in WP6.

4.2 Business Model Canvases

4.2.1 Scenario 1: Platform and Modules BMC

This scenario focuses on the exploitation of the **CyberSecPro Platform (DCM)** as the delivery infrastructure for **sector-specific training modules**. It targets **students, recent graduates, and career changers** seeking practical cybersecurity skills and **universities** aiming to deploy modular courses quickly. The business model combines direct-to-learner sales with institutional partnerships. Its core advantage lies in **hands-on, affordable, and flexible training**, bridging the gap between academic programs and job market needs. Below figure 1 represents the VPC for the first scenario and the students, recent graduates and career changers entering cybersecurity customer group. Figure 2 presents the extracted BMC



Figure

Figure 1: VPC for the first scenario and the students, recent graduates and career changers entering cybersecurity customer group

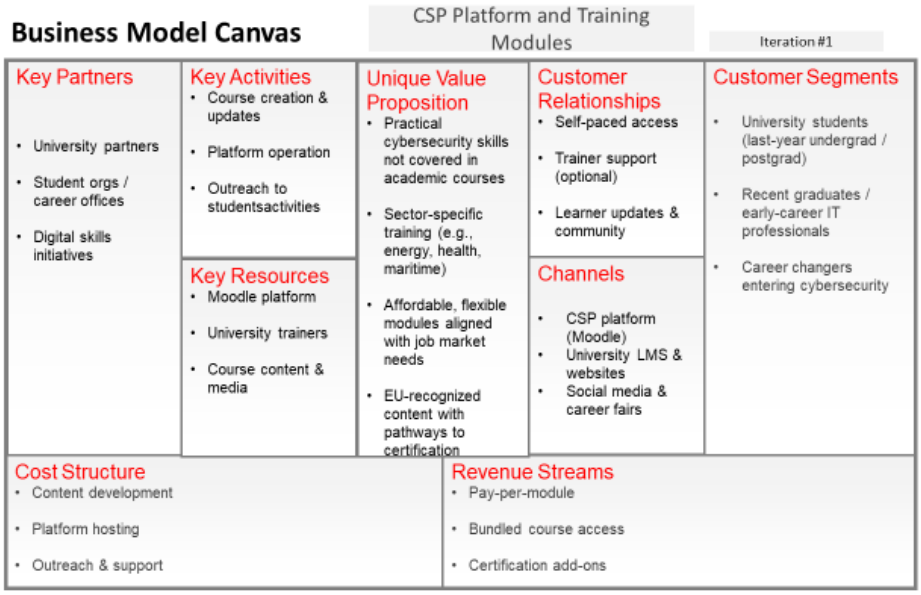


Figure 2: BMC for the 1st scenario

4.2.2 Scenario 2: Platform and MooCs BMC

This scenario builds on the **CyberSecPro Platform** as the central delivery environment for **MOOC-based cybersecurity learning paths**. It targets two key markets: **mid-career professionals** who want to upskill or certify, and **corporate HR / Learning & Development (L&D)** departments that need scalable training for employees. The business model focuses on **subscriptions, enterprise licensing, and certification revenue**, leveraging the platform's ability to track learning progress and align content with **ECSF and EU digital skills frameworks**. Below Figure 3 and 4 represents the VPC for the 2nd scenario and the related customer groups. Figure X5 presents the extracted BMC.

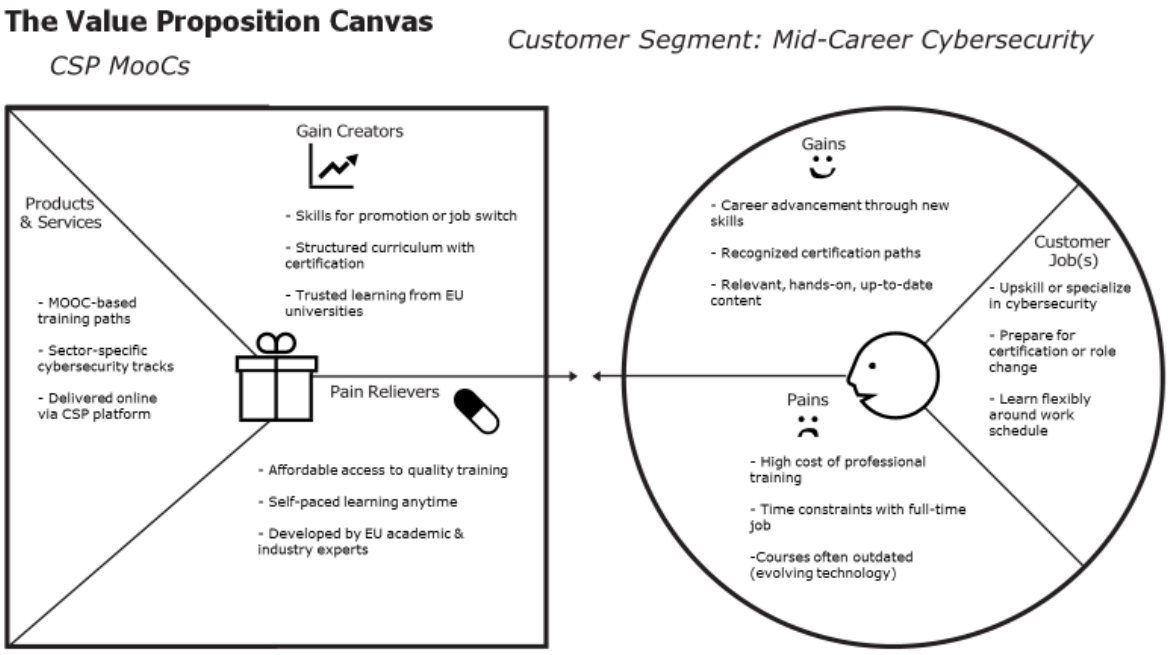


Figure 3: VPC for the second scenario and the *Mid-Career Cybersecurity customer group*

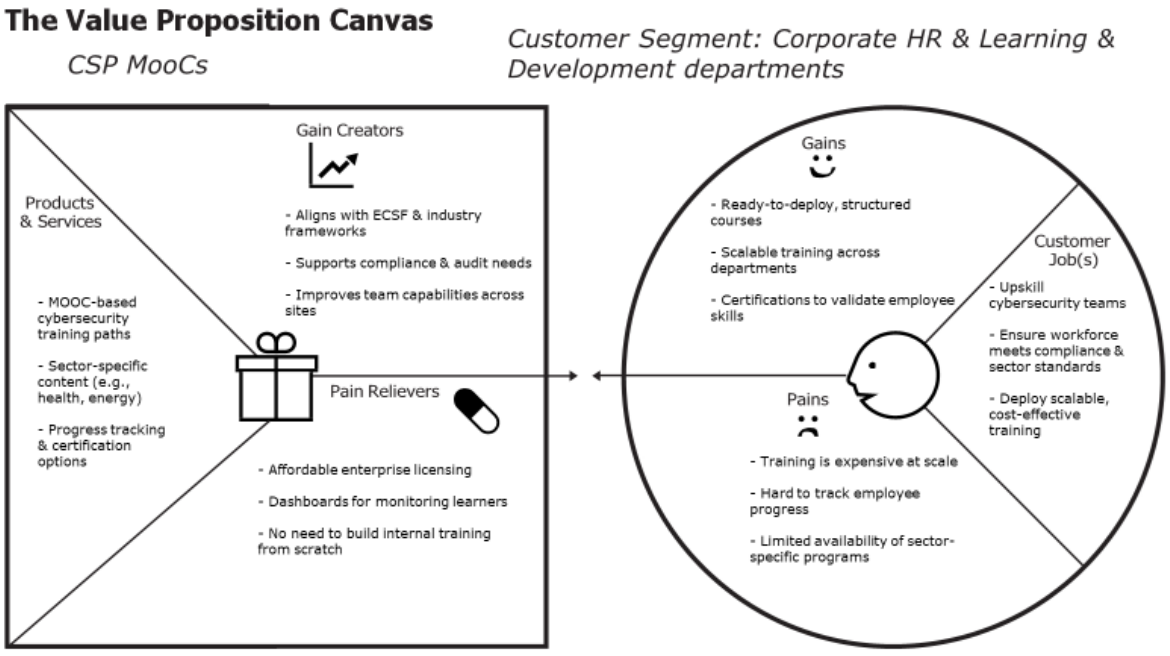


Figure 4: VPC for Corporate HR & Learning & Development departments customer group

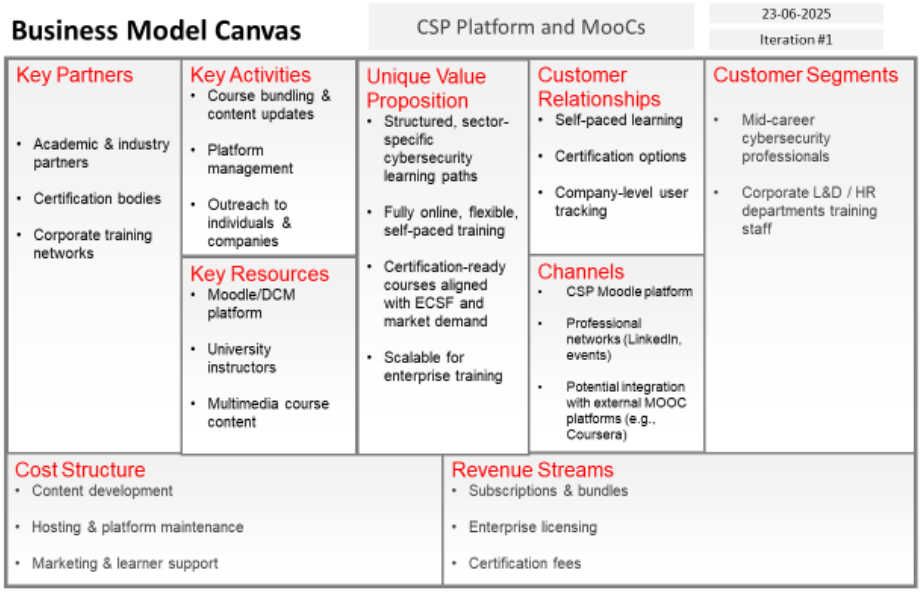


Figure 4.5: BMC for the 2nd scenario

4.2.3 Scenario 3: Platform, MOOCs and Certification BMC

Scenario 3 combines the **CyberSecPro DCM Platform (Moodle-based Dynamic Curriculum Management)** with a **Certification Scheme** to create a scalable exploitation pathway focused on **skills validation, credential issuance, and credential lifecycle management**. While Scenarios 1 and 2 primarily monetize training delivery, Scenario 3 introduces a higher-value offering by enabling **verifiable proof of competence** through structured assessments, ECSF-aligned learning outcomes, and credential verification services. This scenario targets three main customer segments, namely, **individual learners** seeking recognized credentials to strengthen employability and career progression, **enterprises** aiming to validate workforce readiness and demonstrate compliance-driven competence, and **universities / training providers** seeking certification-ready learning infrastructure and standardized credentialing workflows. The core differentiator of this scenario lies in offering **certification-as-a-service** powered by the DCM platform's tracking, assessment, reporting, and credential management capabilities. The model supports recurring revenue through **certification fees, credential renewal, verification services, and institutional licensing**. The following figures present the VPC for the two aforementioned customer groups and the respective BMC.

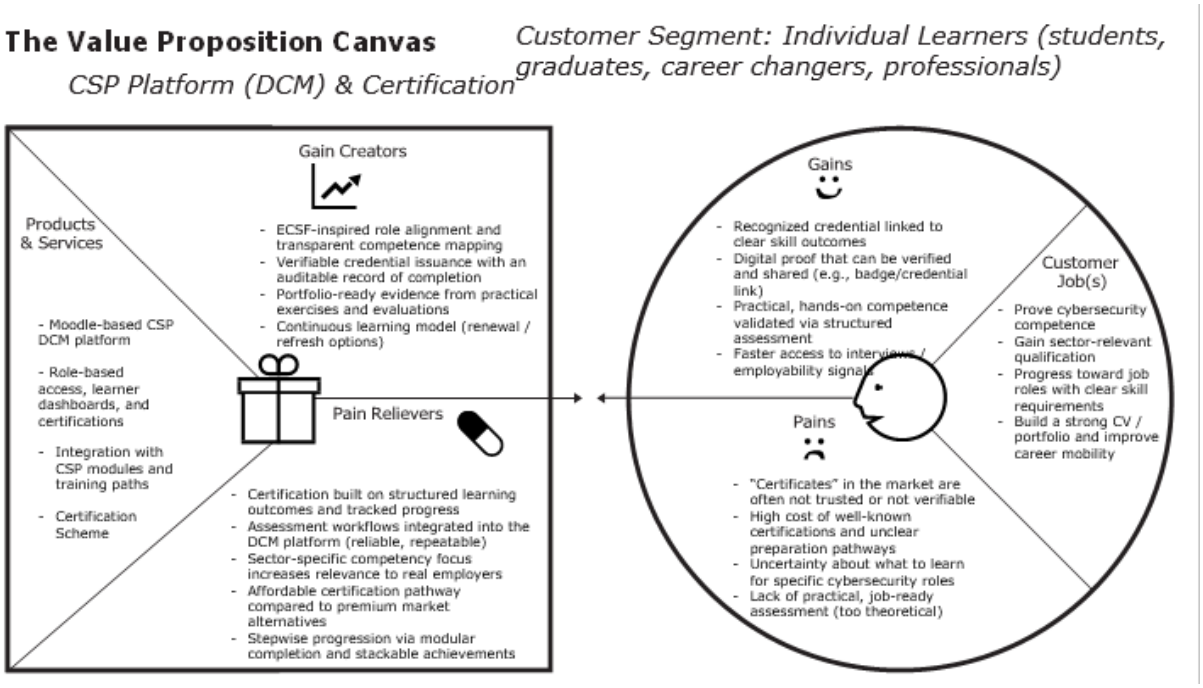


Figure 5: VPC for Individual Learners (students, graduates, career changers, professionals) customer group

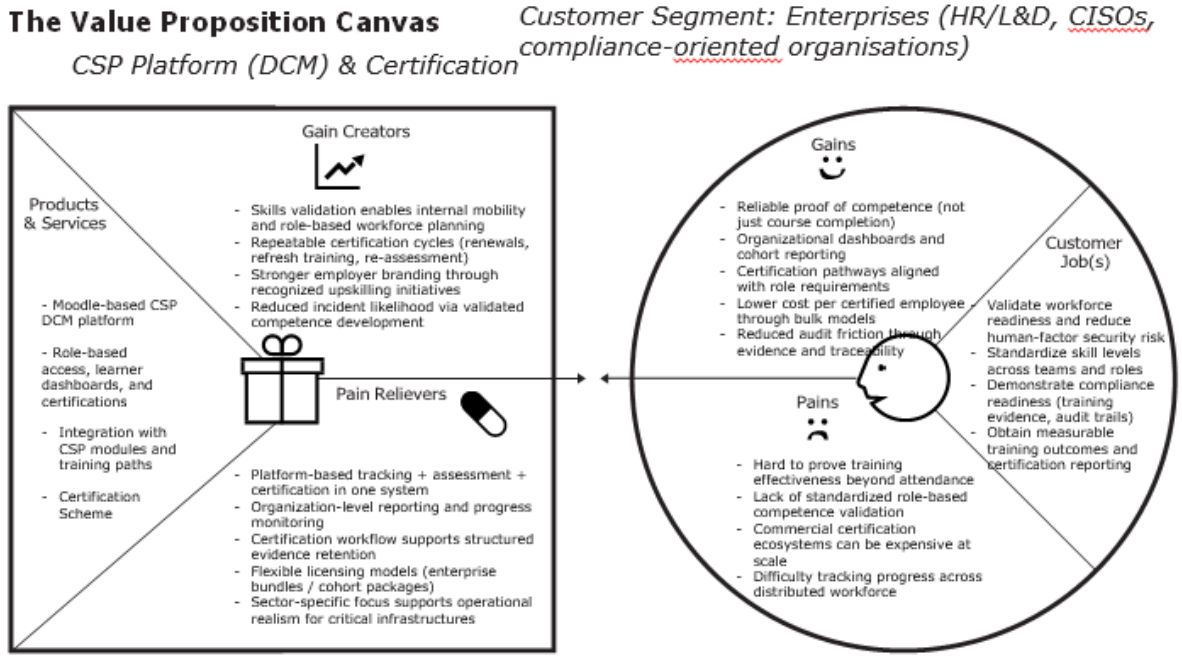


Figure 6: VPC for Enterprises (HR/L&D, CISOs, compliance-oriented organisations) customer group

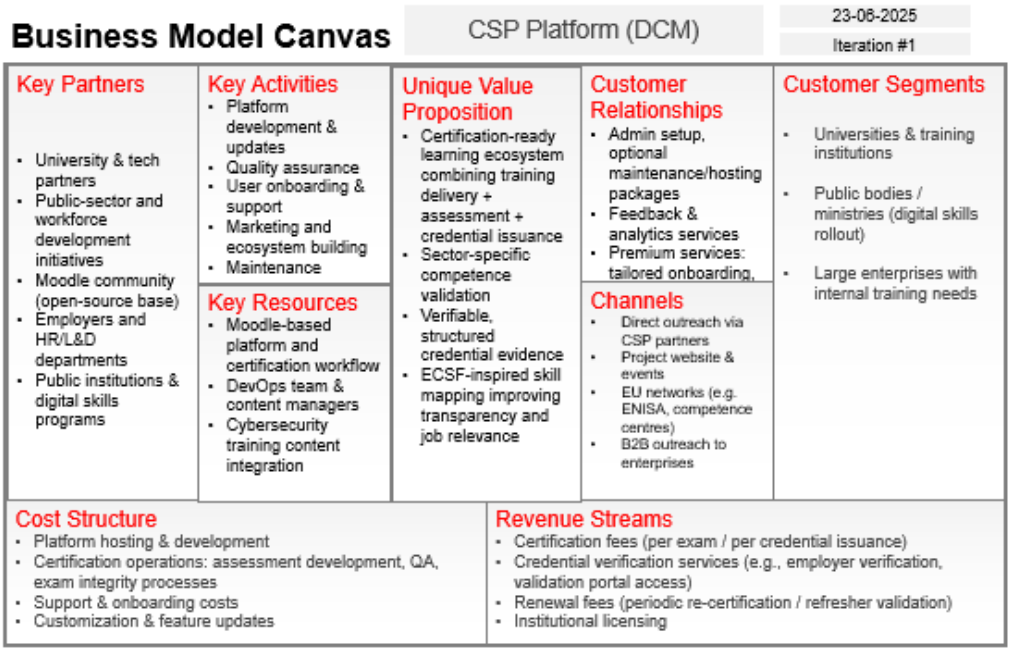


Figure 7: BMC for the 3rd scenario

4.3 Intellectual property (IP) management and strategy

CyberSecPro employs an IP management strategy designed to balance the protection of individual partner assets with the project's overarching mission to serve as a "public good" for the European cybersecurity workforce. Governance of Intellectual Property Rights (IPR) is centralized through the Innovation Manager (ACEEU) and the Dissemination, Exploitation, Sustainability Manager (MAG), who coordinate the identification, protection, and dissemination of project results. A dedicated IPR Committee, chaired by the Innovation Manager and consisting of specialized representatives from each project partner, is responsible for protecting both background (pre-existing) and foreground (newly generated) data, managing access rights for third parties, and overseeing joint ownership and licensing agreements[1].

4.3.1 Licensing Model: Creative Commons

To maximize the impact and accessibility of the project's outputs, the consortium has adopted a Creative Commons Attribution-Non-commercial-Share Alike 4.0 International License (CC BY-NC-SA 4.0) for all education and training materials. This strategic choice enables the following:

Permissions: Third parties are permitted to share, adapt, and remix materials for non-commercial purposes.

Requirements: Any use of the materials requires clear attribution to the EU CyberSecPro project and its official website, along with a mention of the specific license used.

[1] Ownership of results, background access rights, and rights of use by the granting authority are governed by Article 16 of the Grant Agreement and the CyberSecPro Consortium Agreement. Any licensing models described herein shall be implemented subject to beneficiary ownership rights and EU rights of use for policy, communication, and dissemination purposes

Share Alike Provision: To ensure the continuous growth of open educational resources, any derivative works created from CyberSecPro materials must be distributed under the same CC BY-NC-SA 4.0 license.

The rationale for this open approach is to minimize legal complexities that often restrict the fair use of materials in collaborative EU initiatives. By providing a simple transparency declaration and a standardized license, the project ensures its results function as a sustainable public resource.

4.3.2 Transparency and Ethical Conduct

In addition to the CC license, the project has established strict transparency guidelines for material creators. All materials must include appropriate academic references formatted according to the grant agreement policy. Furthermore, due to the innovative nature of the project, any content generated or enhanced using AI-based tools must be clearly declared to maintain fairness and professional integrity.

4.3.3 Proprietary Tools and Ownership

While the project promotes openness for educational content, it maintains a clear distinction regarding technical infrastructure and proprietary assets:

Commercial Tools: The IPR for specific cybersecurity tools used within the training modules remains the property of the individual partner providing that tool. While the syllabi for these modules are open to all partners and interested participants, the underlying proprietary technologies are protected.

Consortium Property: Official project documents and their contents remain the property of the CyberSecPro Consortium. These documents may not be used in any manner inconsistent with the interests of the consortium or disclosed externally without prior written consent from the partners.

Publication Approval: To prevent unintended IPR violations, all partners must submit the final version of any planned publication to the consortium for approval. If no objections are raised within one week, the silence is treated as an agreement to proceed with the publication.

In line with Erasmus+ and Horizon Europe principles on open access and intellectual property, the project's IP strategy functions like a specialised library: educational outputs such as syllabi, curricula, and training materials are made openly accessible for use, reuse, and learning, while proprietary tools, methodologies, and software brought into or developed within the project remain the background or foreground intellectual property of the respective partners.

4.4 Marketing and Communication Strategy

The marketing and communication activities of CyberSecPro were successfully implemented throughout the project, ensuring strong visibility, stakeholder engagement, and effective dissemination of project results. The strategy was aligned with the objectives and impact expectations defined in the Grant Agreement and supported exploitation and sustainability goals.

The project effectively communicated the value of its professional cybersecurity training programmes, learning pathways, pilot activities, and validated outcomes to key target audiences, including cybersecurity professionals, SMEs, training and education providers, Higher Education Institutions, and public-sector stakeholders.

A multi-channel dissemination approach was applied, combining digital communication and targeted dissemination actions, including:

- Use of online communication channels as central information and dissemination points
- Digital outreach activities supporting awareness and engagement
- Organisation and participation in workshops, training activities, and conferences
- Cross-promotion and collaboration with relevant EU projects and initiatives

- Promotion of project achievements, pilot results, and exploitable outputs

All communication actions complied with EU visibility and data protection requirements. The effectiveness of the strategy was monitored through qualitative and quantitative indicators, such as reach, engagement, and stakeholder participation.

Overall, the implemented marketing and communication strategy contributed significantly to the visibility, impact, and sustainability potential of CyberSecPro results.

5 Go-to-Market Strategy

The go-to-market scenarios described in this section are planning models. They do not constitute binding commercial agreements between beneficiaries nor create obligations beyond the duration of the Grant Agreement.

5.1 Market Commercialization Potential

The growing complexity of cyber threats, combined with regulatory requirements and fast digitalisation across many sectors, has created strong demand for targeted and practical cybersecurity upskilling in Europe. While several online training platforms already exist, most focus on generic role-based skills or certification preparation and do not specifically address the operational needs of different industries. CyberSecPro responds to this gap by providing a professional cybersecurity training platform which is built around industry-specific courses and hands-on learning, aligned with European skills frameworks and market needs.

CyberSecPro is designed for flexible deployment across different learning and training contexts. Its content can be delivered as standalone online professional course, courses for individual learners, as structured training programmes for companies and public organisations, and as modules integrated into university professional education and lifelong learning programmes. This multi-layer approach allows CyberSecPro to address both individual upskilling and organisational workforce development without being restricted to a single delivery method.

A key differentiating aspect of CyberSecPro is its focus on sector-specific cybersecurity training for the health, energy and maritime industries. These sectors operate under distinct regulatory frameworks, threat models and technological environments that are not sufficiently covered by horizontal cybersecurity platforms. By aligning training content with real operational scenarios and sector-specific challenges, CyberSecPro increases its practical relevance and value for companies and public bodies seeking immediately applicable cybersecurity skills on demand.

From a commercialization perspective, CyberSecPro enables multiple exploitation paths, including fee-based professional training, company-level training programmes, institutional agreements with public organisations, and integration into university professional and executive education offerings. The platform's European orientation, scalability and cross-border applicability support sustainable market convergence beyond the project duration.

5.2 SWOT Analysis of the market positioning

Table 6: Relevance of the KAs established as part of CSP

Strengths	Weaknesses
Strong EU consortium validation and academic credibility	Limited initial brand recognition outside EU projects
Sector-specific training (health, maritime, energy)	Dependence on continued partner engagement for updates
Moodle-based open architecture (low entry barrier for institutions)	Initial marketing and sales resources limited
Practical hands-on learning bridging education and market needs	Certification scheme still under development

Strengths	Weaknesses
Opportunities	**Threats**
Rising demand for cyber skills and ECSF alignment in EU training	Competition from commercial training platforms and MOOCs
Public-sector funding for digital skills programs	Rapid evolution of cyber threat landscape requiring continuous updates
Growing acceptance of online and hybrid learning	Economic constraints limiting training budgets
Institutional partnerships for content reuse and white-label platforms	Market fragmentation and overlap of initiatives

5.3 Marketing and Sales strategy

The marketing and sales strategy of CyberSecPro is designed to support the transition from project dissemination activities to the effective uptake, adoption, and long-term exploitation of the project's Key Exploitable Results (KERs). Building on the market analysis and SWOT assessment presented in the previous sections, the strategy focuses on positioning CyberSecPro's results as credible, practical, and sector-relevant solutions addressing the European cybersecurity skills gap.

The strategy adopts a high-level, flexible approach that is applicable across the different exploitation scenarios identified within the project. Rather than focusing on short-term commercial objectives, it emphasises sustainable market uptake, stakeholder engagement, and alignment with European policy, skills frameworks, and sectoral needs.

The strategy builds on the project's strong value proposition, sector focus, and EU academic credibility, and follows a phased, multi-channel approach targeting both individual and institutional customers.

Target Audiences and Market Focus

CyberSecPro addresses a diverse set of target audiences, reflecting the multi-stakeholder nature of the cybersecurity education and training ecosystem. These audiences include individual learners (such as students, early-career professionals, and experienced practitioners seeking reskilling or upskilling), educational and training institutions, enterprises and organisations aiming to strengthen their cybersecurity workforce, and sector-specific stakeholders in healthcare, maritime, and energy.

The marketing and sales strategy recognises that these audiences have different motivations, adoption pathways, and engagement mechanisms. As a result, the approach supports both individual-level uptake through accessible digital offerings and institutional-level adoption through structured engagement with organisations and training providers.

Market Positioning and Value Communication

CyberSecPro is positioned as a high-quality, practical, and sector-oriented cybersecurity training ecosystem, combining academic credibility with hands-on learning and real-world relevance. Key value elements communicated through marketing and sales activities include the alignment of training content with labor market needs, compatibility with recognised European skills frameworks such as the European Cybersecurity Skills Framework (ECSF), and the modular and scalable nature of the CyberSecPro platform, training modules, and MOOCs.

The integrated delivery of training content, platform-based access, and certification pathways supports flexibility for different user profiles and facilitates adoption by both individuals and institutions. This positioning aims to differentiate CyberSecPro from generic training offerings by emphasising sector specificity, practical applicability, and European relevance.

Marketing Channels and Promotion Activities

The marketing and sales strategy leverages a combination of digital, partnership-based, and event-driven channels to support awareness, adoption, and uptake of CyberSecPro's results. Core channels include the project's online presence, webinars, targeted communication activities, and participation in relevant European and sectoral events. These channels are used not only to increase visibility, but also to facilitate onboarding, pilot use, and replication of the project's outcomes. Collaboration with universities, vocational education and training providers, professional associations, and sectoral organisations acts as a multiplier, extending reach and reinforcing credibility. Marketing and promotion activities are closely aligned with dissemination efforts implemented under WP6, ensuring consistent messaging and efficient use of project resources while maintaining a clear focus on exploitation and sustainability objectives.

Sales and Uptake Approach

In the context of an EU-funded collaborative project, "sales" is understood as the facilitation of access, adoption, and structured use of CyberSecPro results rather than direct commercial transactions. Sales and uptake approaches vary depending on the target audience and exploitation scenario.

Individual learners are primarily supported through direct digital channels and self-service access to training offerings. Institutional and organisational users are engaged through partnership-driven approaches, pilot deployments, and tailored training packages. High-level access models such as licensing, subscription-based access, or institutional agreements may be considered within specific exploitation pathways, without pre-defining contractual, or financial arrangements within the scope of the project.

Feedback, Refinement, and Sustainability

An important component of the marketing and sales strategy is the integration of feedback from early adopters, learners, and institutional users. Feedback collected through platform usage, pilot activities, and stakeholder engagement is used to refine training content, improve user experience, and strengthen market positioning.

This iterative approach supports continuous improvement and enhances the long-term sustainability of CyberSecPro's results beyond the project lifetime. By aligning marketing and sales activities with exploitation objectives and stakeholder needs, the strategy contributes to building trust, recognition, and sustained adoption within the European cybersecurity ecosystem.

Pricing and Access Logic

Pricing and access models are defined at a high level and adapted per exploitation scenario, taking into account the diversity of target audiences and usage contexts. Different access options may be considered, such as freemium entry points for awareness-building, pay-per-course or subscription-based access for individual learners, and institutional licensing models for organisations and training providers seeking structured deployment.

The pricing and access logic is designed to balance affordability and inclusiveness with the need to support long-term sustainability of the CyberSecPro results. Flexibility in access models allows the project outcomes to be adopted by a wide range of stakeholders, while enabling gradual progression from initial engagement to more structured use within institutional or organisational settings. Specific pricing structures, financial conditions, or contractual arrangements are not defined within the scope of the project and will be addressed within the relevant exploitation pathways.

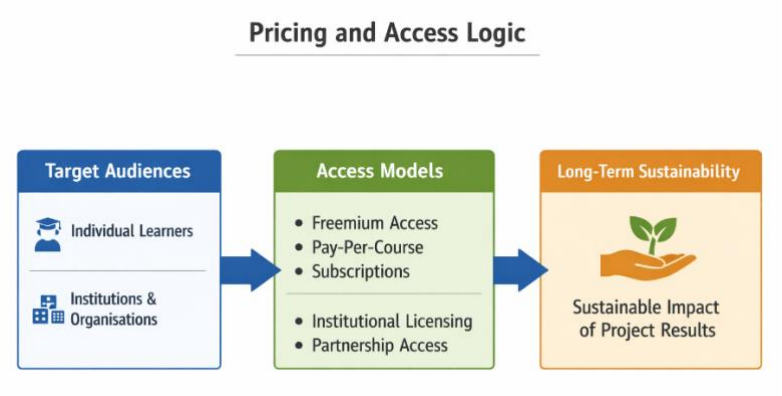


Figure 8: Pricing and Access Logic

Alignment and Consistency Across Scenarios

The Marketing and Sales Strategy is designed to be consistently applied across all exploitation scenarios, ensuring coherent positioning, messaging, and customer engagement. This harmonised approach supports clarity for end users and stakeholders while allowing flexibility for scenario-specific adaptations.

Overall, the strategy aims to maximise market penetration, foster trust and recognition, and support the sustainable exploitation of CyberSecPro results beyond the project lifetime.

6 Financial Analysis

6.1 Scenario 1

Scenario 1 monetizes either the **CyberSecPro DCM platform as delivery infrastructure** and, or the **sector-specific modules (72 hands-on modules)**, targeting **individual learners** (students, graduates, career changers) and **institutions** (universities/training providers). This scenario assumes that the DCM platform functions as the primary digital delivery environment, while modules may be offered either as standalone learning units or as structured offerings within the platform. Because delivery is predominantly digital, the model benefits from high scalability; however, long-term sustainability depends on maintaining (i) platform availability and cybersecurity resilience, (ii) periodic content updates to ensure continued relevance, and (iii) structured user acquisition and support mechanisms.

6.1.1 Cost Structure analysis

The fixed and semi-fixed costs in Scenario 1 represent the baseline operational expenses required to keep the CyberSecPro DCM platform and modules running, regardless of the number of learners. These costs include core platform hosting and infrastructure services such as server resources, storage, backups, monitoring, and domain management. They also include platform administration and maintenance activities such as Moodle/DCM configuration, software updates, security patching, access management, and general troubleshooting. A key fixed cost element is content governance and quality assurance, which covers periodic review and updates of the training modules to ensure technical accuracy, sector relevance (health, maritime, energy), and alignment with evolving cybersecurity practices. In addition, fixed costs include the development and maintenance of basic user support materials (FAQs, onboarding guides, documentation), as well as minimum-level marketing and dissemination activities required to maintain visibility and ensure a stable pipeline of new users and partners. Finally, compliance-related costs such as GDPR-related processes, documentation, and basic legal/accounting overhead can be considered semi-fixed recurring costs that are necessary for sustainable operation.

The variable costs in Scenario 1 scale directly with adoption and increase as the number of active learners, institutional clients, and platform activity grows. The most significant variable cost is user and partner support, since support demand increases proportionally with user volume, onboarding needs, and technical inquiries. Additional variable costs arise when onboarding institutional customers, including configuration effort, training for administrators or instructors, and set-up of dashboards and reporting workflows. If Scenario 1 includes live or hybrid training delivery components, facilitation time and teaching support become variable expenses linked to cohort size and delivery frequency. Other variable costs include transaction and payment processing fees in case of individual learner payments, as well as increased infrastructure cost if scaling requires higher compute capacity, higher concurrency, additional storage, or more robust logging and analytics. Finally, variable costs may also include targeted marketing spend (paid campaigns, outreach, event participation) that rises as the consortium seeks to accelerate adoption in new regions or sectors.

Below is a realistic operational cost envelope to run Scenario 1 as a small sustainable service (not a full venture-scale SaaS).

Table 7:Indicative Annual Cost Structure for Scenario 1 based on partners experience — Scenario 1

Cost category	Year 1	Year 2 and 3	Notes
Hosting + technical tooling	€6k–€18k	€10k–€30k	depends on traffic + monitoring/security stack

Platform admin & maintenance	€25k–€45k	€40k–€70k	0.5–>1.0 FTE equivalent
Content QA + updates	€20k–€45k	€30k–€60k	review + refreshing modules
Support & user success	€8k–€20k	€15k–€35k	scales with users
Marketing + dissemination	€10k–€25k	€20k–€45k	includes partner campaigns + events
Legal/GDPR + accounting	€3k–€10k	€5k–€12k	privacy policies, DPA templates
Total	**€72k–163k**	**€120k–€252k**	realistic sustainability range

To improve cost efficiency and accelerate break-even in Scenario 1, the exploitation approach should prioritize **self-service onboarding supported by automated reporting**, reducing the need for continuous manual support as the user base grows. In parallel, the offering should be structured around **sector bundles** (e.g., health, maritime, energy), which reduces the number of separate module variations and therefore lowers operational overhead in content management, updates, and customer guidance. Content maintenance should follow a **fast-track update approach** focused on targeted improvements and periodic technical refreshes, rather than resource-intensive full rewrites, ensuring the modules remain current while keeping update costs predictable. Finally, the strategy should prioritize **institutional licensing** early, as B2B contracts provide higher revenue per account and more stable cash flow compared to relying primarily on individual learner purchases.

6.1.2 Market adoption and revenue projections

The market analysis identifies a major cybersecurity skills gap across EU sectors with a) a high demand for hands-on skills and role readiness, and b) an EU workforce shortage[2] measured in the hundreds of thousands, meaning continued demand for upskilling pipelines. ENISA[3] also highlights that cybersecurity skills shortages persist and are increasing in Europe, especially as the demand for ICT/cyber skills rises. On top of that, the *global cybersecurity training market itself is growing strongly* with USD 4,532.2 million in 2023 and is expected to reach USD 13,698.1 million by 2030 (multi-billion market with 17,1% CAGR by 2030).

Pricing assumptions

To keep projections realistic and competitive, pricing assumptions are aligned with typical training spend levels observed in the market, with security training programs commonly sit around **$20–$50**[4] **per employee per year** (awareness scale) while per-user annual ranges like **£20–£100/user/year** are also common[5] in basic training offerings.

CyberSecPro modules are **hands-on and sector-oriented**, so a *moderate premium over awareness-only* is reasonable while still staying affordable. Thus for a **B2C (individual learners) pricing strategy we adopt the a**verage purchase amount on the above figures, namely **€50 per learner/year** (e.g., one paid module or a small bundle, with some modules free/open).

The tier-based institutional pricing model for Scenario 1 was derived using a market-aligned, seat-based approach consistent with typical cybersecurity training platform pricing structures. Industry benchmarks indicate that security awareness and training solutions are commonly priced on a per-user-per-month

[2] https://www.isc2.org/Insights/2024/05/Closing-the-EUs-Cybersecurity-Workforce-and-Skills-Gaps

[3]https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf?

[4] https://www.jerichosecurity.com/blog/how-much-cyber-security-training-cost?

[5] https://www.metacompliance.com/blog/cyber-security-awareness/cyber-security-training-cost

basis, with published market ranges for modern, self-service platforms typically falling between approximately **USD $0.45 and $1.25[6] per user per month**, depending on organisational scale, included services, and contract duration. To reflect this market logic and maintain affordability for universities and training providers, the CyberSecPro B2B pricing was structured into three annual tiers (Starter, Growth, Enterprise), each defined by a maximum number of active learners per year and an annual fee that decreases in effective per-learner cost as volume increases. This approach supports predictable budgeting for institutions, enables volume discounting as adoption scales, and aligns with Scenario 1's operational design assumptions (self-service onboarding and automated reporting), while also ensuring that platform operations and support remain financially sustainable. Table 8 below describes the different tiers.

Table 8: Tier-Based Institutional Licensing — Scenario 1

Tier	Target customer size / use case	Annual coverage (active learners/year)	Annual fee (€ / year)	Approx. cost per learner/year*
Tier 1 — Starter Institution	Small HEI / pilot cohort / single department	Up to **250**	**€4,500**	~€18
Tier 2 — Growth Institution	Multi-department rollout / recurring cohorts	Up to **1,000**	**€9,500**	~€9.5
Tier 3 — Enterprise Institution	Large university / multi-campus / national academy	Up to **3,000**	**€18,000**	~€6

*Cost per learner/year assumes full utilization of the tier limit.

Adoption projections

The adoption projections for Scenario 1 are based on a conservative and realistic post-project scaling pathway, aligned with both the CyberSecPro market analysis findings and external EU workforce evidence. The project's market gap analysis confirms that cybersecurity workforce shortages remain structural in Europe, with strong demand for practical, hands-on skill development across sectors and an identified set of **18 dominant knowledge and skills gaps** that require urgent upskilling interventions.
In addition, CyberSecPro targets higher education and training providers that need "ready-to-deploy" modular content and platform infrastructure, and this institutional route enables efficient distribution through partner networks rather than relying solely on individual learner marketing.

The broader market context reinforces this adoption potential with the EU cybersecurity workforce gap to be estimated at **274,000 unfilled roles**[7], indicating sustained demand for

[6] https://caniphish.com/blog/how-much-does-security-awareness-training-cost?

[7] https://www.isc2.org/Insights/2024/05/Closing-the-EUs-Cybersecurity-Workforce-and-Skills-Gaps

training pipelines, role readiness, and skill conversion pathways. ENISA[8] further highlights that demand for ICT and cybersecurity skills is rapidly increasing while the skills shortage is growing, supporting continued uptake of structured training solutions beyond the project lifetime. Therefore, the adoption trajectory assumes moderate Year 1 uptake driven by consortium dissemination and early institutional pilots, followed by growth in Years 2–3 through replication across departments and additional partner organisations, reflecting the gradual but scalable adoption patterns typical of higher education and workforce training ecosystems.

For the B2C adoption projections we follow:

Paid learners per year = reachable audience × adoption conversion

Where "reachable audience" grows each year through dissemination and partner replication, and "conversion" stays conservative, For year 1, reachable audience is estimated ~10,000–20,000 relevant visitors / exposures, and ~2%–4% purchase conversion. Year 2 assumes a 3× increase because a) more partner institutions actively directing learners to the modules, b) improved credibility (case studies + better onboarding) and c) broader conversion from free/open participation into paid engagement.On the same line year 3 assumes a **2× increase** because a) partner adoption continues, but the base is larger, b) marketing gains are incremental, not exponential and c) demand stays strong, but growth becomes more operationally driven. Even 2,400 paid learners/year is still a very small capture of the European market need and workforce gap signals, which keeps it realistic rather than inflated.

Table 9: Projected B2C Adoption (Paid Individual Learners) — Scenario 1

Year	Projected active paid learners (B2C)	Key adoption drivers
2026	400	Initial uptake from consortium dissemination + early visibility of sector modules
2027	1,200	Increased awareness + repeat cohorts + improved conversion from free/open content
2028	2,400	Expanded reach via partner channels + stronger demand for hands-on skills pathways

For the B2B adoption projections, we follow a similar conservative ramp logic to B2C, but applied to institutional conversion: Paying institutions per year = reachable institutional pipeline × institutional conversion rate. In Year 1, the reachable pipeline is assumed to consist of approximately 20–40 institutions actively approached through consortium dissemination, partner networks, and direct outreach (universities and training providers that need "ready-to-deploy" modular content and platform infrastructure).

A conservative 15%–30% conversion rate from pipeline to paid pilots results in ~6 institutional customers, reflecting early adopters that are easiest to onboard (partner-aligned and pilot-ready). In Year 2, the projection increases to 14 institutions based on structured replication effects: (a) more partner

[8]https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf

institutions recommending or reusing the modules, (b) improved credibility through initial reference deployments and success stories, and (c) reduced friction due to standardized onboarding and automated reporting, which your sustainability and risk sections highlight as key operational scaling levers. In Year 3, the projection reaches 30 institutions, assuming a further scale-up driven by broader institutional partnerships and multi-programme adoption, but still keeping growth realistic because procurement and adoption cycles in higher education are gradual and depend on internal replication rather than exponential marketing. Even 30 institutions by Year 3 remains a small, credible share of the potential EU university and training-provider landscape, meaning the projection stays realistic rather than inflated while aligning with the project's institutional partnership model and long-term sustainability plan.

Table 10: Projected B2C Adoption (Paid Individual Learners) — Scenario 1

Year	Projected paying institutions (B2B)	Key adoption drivers
2026	6	Early adopters (pilot deployments, partner institutions, fast onboarding)
2027	14	Replication into additional departments + stronger evidence/case studies
2028	30	Scaling via institutional partnerships and modular deployment across programmes

Projected B2B Adoption (Institutional Customers) — Scenario 1

Revenue and Profit Projections

The revenue and profit projections for Scenario 1 are based on the commercial assumptions defined in the deliverable for both B2C and B2B adoption and pricing. For the B2C stream, it is assumed that the platform converts **400 paid learners in 2026**, **1,200 paid learners in 2027**, and **2,400 paid learners in 2028**, with an average annual revenue of **€50 per paid learner**, reflecting low-friction access to modules and entry-level affordability. For the B2B stream, the institutional adoption forecast is doubled compared to the initial baseline to reflect a stronger institutional replication effect through partner networks, resulting in **6 paying institutions in 2026**, **14 in 2027**, and **30 in 2028**, using the tier-based annual licensing model of **€4,500 (Starter)**, **€9,500 (Growth)**, and **€18,000 (Enterprise)**. Since the distribution of tiers per institution is not fixed in the deliverable, a realistic scaling mix is applied in the projection to reflect typical market evolution from pilot uptake to maturity: **2026 assumes 100% Starter-tier pilots**, **2027 assumes a mix of Starter and Growth tiers**, and **2028 assumes a balanced mix of Starter, Growth, and Enterprise tiers as institutional utilisation increases**. Finally, the profit estimation uses the operational cost envelope provided in the deliverable, applying midpoint values for Year 1 and Year 2 and a slightly increased growth cost estimate for Year 3 to reflect increased support and platform operations at higher adoption levels.

Table 11: Revenue Projections — Scenario 1

Year	Paid learners (B2C)	B2C revenue (€50 each)	Institutions (B2B)	Assumed tier mix	B2B revenue	Total revenue
2026	400	€20,000	6	6× Starter	€27,000	€47,000
2027	1,200	€60,000	14	8× Starter + 6× Growth	€93,000	€153,000
2028	2,400	€120,000	30	12× Starter + 12× Growth + 6× Enterprise	€276,000	€396,000

Table 12: Profit Projections — Scenario 1

Year	Total revenue	Operating cost (assumption)	Profit / (Loss)
2026	€47,000	€117,500	–€70,500
2027	€153,000	€186,000	–€33,000
2028	€396,000	€210,000	+€186,000

6.1.3 Break-even analysis

Break-even is defined as the point where total annual revenues (B2C module/bundle sales and B2B institutional licensing) equal annual operating costs. This analysis applies the Scenario 1 pricing and adoption assumptions described in the deliverable: a B2C blended average revenue of €50 per paid learner/year and B2B tiered annual licensing of €4,500 (Starter), €9,500 (Growth) and €18,000 (Enterprise) per institution.

In addition, it uses the operating cost assumptions already applied in the Scenario 1 in Table 11 (€117,500 for 2026, €186,000 for 2027, and €210,000 for 2028), which are consistent with the operational cost envelope reported for Year 1 and Year 2-3.

The break-even requirement is estimated by subtracting the projected annual B2C revenue from total costs and calculating the minimum number of B2B institutional licenses required to close the remaining revenue gap.

Table 13: Break-even Institutional Licenses Required (B2B) — Scenario 1 ((Assumes B2C adoption remains as projected: 400/1,200/2,400 learners per year at €50 each)

Year	Operating cost (assumption)	B2C revenue	Remaining gap to break-even	Institutions needed (Starter €4,500)	Institutions needed (Growth €9,500)	Institutions needed (Enterprise €18,000)	Institutions needed (blended fee*)
2026	€117,500	€20,000	€97,500	**22**	**11**	**6**	**11**
2027	€186,000	€60,000	€126,000	**28**	**14**	**7**	**14**
2028	€210,000	€120,000	€90,000	**20**	**10**	**5**	**10**

*“Blended fee” uses the average institutional fee implied by the tier mix used in the revenue table for that year

Under our assumptions, Scenario 1 does **not** break even in 2026–2027 unless institutional adoption is significantly higher than the forecast or a higher tier mix is achieved earlier. However, for 2028 the break-even threshold becomes realistic: only **~10 institutions (blended)** are needed to break even, while the projected adoption is **30 institutions**, which supports a positive margin and sustainability.

Table 14: Break-even Paid Learners Required (B2C-only case) — Scenario 1

Year	Operating cost (assumption)	B2C price (ARPU)	Paid learners needed to break even (B2C-only)
2026	€117,500	€50	2,350
2027	€186,000	€50	3,720
2028	€210,000	€50	4,200

Table 14 shows the number of paid learners required if Scenario 1 relied only on B2C revenue at €50 per learner/year and no B2B licensing. The B2C-only break-even volumes are much higher than the projected B2C adoption (400/1,200/2,400), which confirms that Scenario 1 sustainability is primarily enabled by **institutional licensing** rather than individual purchases alone.

The break-even results confirm that Scenario 1 becomes financially sustainable only when institutional licensing reaches a critical mass. Under the assumed operating-cost baseline and €50 B2C ARPU, the model requires approximately **22 Starter-tier institutions in 2026** and **19 institutions in 2027 (blended pricing)** to cover remaining costs after B2C revenues, which is above the projected institutional uptake for those years. In contrast, in **2028**, break-even is achievable with approximately **10 institutions (blended)**, while the adoption forecast anticipates **30 institutional customers**, enabling a positive operating surplus and confirming that the B2B pathway is the main sustainability lever for Scenario 1.

6.2 Scenario 2

Scenario 2 focuses on the exploitation of the CyberSecPro platform through structured MOOC-based learning paths, targeting mid-career professionals and organisational customers such as enterprises and HR/L&D departments. In contrast to Scenario 1, which emphasises individual module uptake, Scenario 2 prioritises bundled content, platform-based delivery, and longer-term organisational engagement. This scenario leverages the platform's ability to provide scalable, subscription-based learning with certification alignment, offering a financially stable pathway for enterprise-oriented adoption.

6.2.1 Cost Structure analysis

The cost structure of Scenario 2 is primarily driven by platform operation and the maintenance of MOOC-based learning paths rather than by per-course delivery costs. Compared to Scenario 1, direct instructional and learner-support costs are reduced, while fixed and semi-fixed platform-related costs become more significant and variable costs are mainly associated with enterprise onboarding and ongoing customer support.

The main cost components include the hosting, operation, and scaling of the CyberSecPro platform, ensuring reliable access, performance, and data management for organisational users. Indicative annual costs for platform operation and technical maintenance are estimated in the range of **€40,000–€70,000**, depending on usage levels and scalability requirements.

Content-related costs are associated with the continuous maintenance, updating, and quality assurance of MOOC learning paths, including alignment with evolving cybersecurity practices and sector-specific requirements. These costs are estimated at **€25,000–€50,000 per year**, reflecting the need for periodic updates rather than continuous content development.

Additional costs relate to enterprise onboarding, user management, reporting, and support services, which are more relevant in a B2B-oriented model. These activities are estimated to require **€20,000–€40,000 annually**, depending on the number of organisational customers and the level of support required.

Finally, coordination, administrative overheads, compliance-related activities, and alignment with certification-oriented frameworks represent an additional **€10,000–€20,000 per year**.
Overall, the indicative annual cost envelope for Scenario 2 is estimated to range between **€95,000 and €180,000**. This reflects a platform-centric structure with a limited volume of individual participation while is well aligned with organisational subscription and licensing models.

Table 15: Indicative Annual Cost Structure for Scenario 2 based on partners experience — Scenario 2

Year	Operating Costs (€)	Notes
2026	95,000–130,000	Platform operation + content maintenance + onboarding for early adopters
2027	110,000–160,000	Slight increase with scaling organisational customers
2028	120,000–180,000	Full target adoption, including ongoing content updates and reporting

6.2.2 Market adoption and revenue projections

Scenario 2 addresses organisational customers seeking structured and scalable cybersecurity training solutions. Target customers include mid-career Cybersecurity professionals, public organisations, and enterprises, Corporate Human Resources (HR), learning and development departments aiming to upskill or reskill cybersecurity-related roles.
Market adoption under this scenario is expected to follow a gradual trajectory, as organisational decision-making processes typically involve longer evaluation and procurement cycles. However, once adopted, organisational customers tend to demonstrate higher retention rates and longer-term engagement compared to individual learners.
Revenue generation is based on 44ustomizatio-level subscriptions or access agreements to bundled MOOC learning paths delivered through the CyberSecPro platform. Indicative pricing assumptions consider annual contract values in the range of **€15,000–€30,000 per organisational customer**, depending on factors such as the number of users, access duration, and reporting or 44ustomization requirements.
Based on indicative adoption projections, several organisational uptake assumptions are considered to reflect alternative revenue outcomes during the early exploitation phase. These assumptions differ in terms of the number of participating organisations and the average annual contract value per organisation. The following table summarises three indicative revenue prognosis cases, illustrating how variations in organisational adoption levels translate into different annual revenue ranges.

Table 16: Indicative Revenue Projections under Alternative Organisational Adoption Levels – Scenario 2

Revenue prognosis	Number of organisations	Average annual contract (€)	Indicative annual revenue (€)
Low scenario	5–6	18,000	90,000–108,000
Medium scenario	8–10	20,000	160,000–200,000
High scenario	12–15	22,000	264,000–330,000

Compared to Scenario 1, this model relies on fewer customers but higher average revenue per customer, offering increased predictability and reduced dependency on large-scale individual enrolments.

6.2.3 Break-even analysis

The break-even point in Scenario 2 is primarily influenced by the number of organisational customers and the average contract value rather than by overall user volume. Due to the recurring nature of

subscriptions and the higher value per customer, financial sustainability can be achieved with a relatively limited number of contracts.

Based on the indicative cost envelope and conservative revenue assumptions, break-even is expected to be achievable with approximately **6–8 organisational customers** at mid-range contract values. This threshold is considered realistic within the targeted enterprise and professional training market.

Table 17: Break-even Institutional Licenses Required (B2B) — Scenario 2

Year	Number of organisations	Cumulative revenue (€)	Break-even
2026	5–6	90,000–108,000	No
2027	8–10	160,000–200,000	Yes
2028	12–15	264,000–330,000	Yes

In comparison to Scenario 1, Scenario 2 presents a more stable and resilient financial pathway, characterised by lower volatility and stronger alignment with long-term platform sustainability. The reliance on organisational engagement rather than individual enrolment volumes reduces exposure to market fluctuations.

Overall Assessment

Scenario 2 represents a complementary exploitation pathway for the CyberSecPro platform, offering a financially viable alternative to individual-oriented training models. While adoption is expected to progress at a slower pace, the enterprise-focused approach supports greater revenue stability and clearer cost control mechanisms.

The use of indicative ranges and conservative assumptions ensures internal consistency with the overall financial analysis while avoiding overestimation of market penetration or revenue growth.

6.3 Scenario 3

6.3.1 Cost Structure analysis

Scenario 3 builds on the platform-centric model of Scenario 2 and adds **certification operations** (assessment delivery, credential issuance, verification services, governance/QA). Therefore, the baseline cost structure remains largely aligned with Scenario 2 (platform operation, MOOC maintenance, enterprise onboarding/support and coordination/overheads), while incremental costs reflect the requirements to issue and maintain a credible certification scheme.

Baseline costs (from Scenario 2). Scenario 2 estimates a platform-centric annual cost envelope of **€95,000–€180,000** across the early exploitation years, with typical ranges by year of **€95,000–€130,000 (2026)**, **€110,000–€160,000 (2027)** and **€120,000–€180,000 (2028)**. These costs cover platform operation and technical maintenance, periodic MOOC pathway updates/QA, organisational onboarding and support services, and coordination/administrative overheads.

Incremental certification costs (Scenario 3 add-on). Compared to Scenario 2, Scenario 3 introduces incremental costs in four areas:

- **Assessment lifecycle management** (question bank updates, assessment review, moderation, and handling of exceptions/appeals where relevant).
- **Credential issuance and verification** (certificate generation, verification mechanism/endpoint, audit trail and evidence retention).
- **Certification governance and QA** (policy upkeep, periodic review of certification alignment to target profiles/frameworks and maintaining credibility).
- **Support overhead related to certification** (candidate support for exam/certification flows, verification requests).

These certification-related costs are expected to be **mainly fixed/semi-fixed** (governance, QA, tooling) with a smaller variable component that increases with certification volumes. As a result, Scenario 3 remains scalable and does not introduce linear cost growth with overall learner numbers, provided certification workflows are standardised.

6.3.2 Market adoption and revenue projections

Scenario 3 uses the same organisational adoption logic and pricing assumptions as Scenario 2 for the base platform and MOOC revenues, and then adds certification revenue based on the share of learners within those organisational deployments who opt for certification ("certification uptake"). This ensures Scenario 3 stays internally consistent and avoids inventing a separate user base.

Baseline revenue (reused from Scenario 2). Scenario 2 revenue is driven by organisational customers purchasing subscriptions/access agreements for bundled MOOC learning paths, with indicative annual contract values in the range of €15,000–€30,000 depending on the number of users and service requirements. Under the Scenario 2 adoption cases, indicative annual revenue ranges are:

- Low scenario: 5–6 organisations at ~€18k average → €90,000–€108,000
- Medium scenario: 8–10 organisations at ~€20k average → €160,000–€200,000
- High scenario: 12–15 organisations at ~€22k average → €264,000–€330,000

Certification revenue (Scenario 3 add-on). Certification revenue is modelled as an "attach rate" to Scenario 2 deployments:

- each organisational customer trains a number of learners per year (cohort size),
- a share of those learners select certification (uptake),
- and each issued credential generates a certification fee.

To keep the model conservative and operationally realistic, certification uptake can be represented using low/medium/high planning values for organisational cohorts (e.g., 30% / 50% / 70%), reflecting whether certification is optional, encouraged, or employer-sponsored/mandated. Certification revenue then scales with the same organisational adoption trajectory already assumed in Scenario 2, increasing the revenue per organisation without fundamentally changing the platform subscription model.

Compared to Scenario 2, Scenario 3 increases average revenue per customer by adding an additional monetisation layer that is directly tied to learner outcomes and credential value. The key point is that certification is not assumed to drive adoption by itself in the early phase; instead, it monetises part of the trained population already captured through Scenario 2 organisational contracts.

6.3.3 Break-even analysis

The break-even logic in Scenario 3 follows Scenario 2's structure: sustainability is primarily driven by the **number of organisational customers and average contract value**, with certification revenue

acting as an additional uplift that improves the margin and reduces sensitivity to the exact contract mix.

Baseline break-even anchor (from Scenario 2). Scenario 2 break-even is expected to be achievable with approximately **6–8 organisational customers at mid-range contract values**, based on the indicative cost envelope and conservative revenue assumptions.

Scenario 3 impact on break-even. In Scenario 3, the addition of certification introduces:

- a **new revenue stream per organisation** (proportional to certification uptake in organisational cohorts), and
- a **moderate incremental cost layer** for certification operations and governance.

Because certification revenues scale with the number of learners certifying (and therefore with usage inside contracted organisations), while certification operating costs are largely fixed/semi-fixed when workflows are standardised, Scenario 3 typically:

- **improves the break-even outlook** relative to Scenario 2 for the same number of organisational customers, and
- **reduces downside risk**, because revenue per customer is less dependent on contract value alone.

Using the same adoption pathway as Scenario 2 (low → medium → high organisational uptake), Scenario 3 is expected to reach break-even at least as early as Scenario 2, with certification acting as a supporting lever that increases revenue per cohort and strengthens long-term sustainability once a stable base of organisational customers is in place.

7 Sustainability Plan

7.1 Vision for the long-term sustainability of the project

The vision for the long-term sustainability of CyberSecPro is to establish a self-sustaining, pan-European ecosystem that continues to bridge the gap between academic supply and market demand for practical cybersecurity skills long after the initial funding period. This vision is centered on maintaining an operational balance between continuous platform availability and security, content relevance, and predictable benefits (not limited to but including revenue streams) derived from a diversified portfolio of exploitable results.

7.1.1 A Multi-Pillar Sustainability Strategy

To ensure the project functions as a lasting "public good," the sustainability plan rests on the following pillars:

Diversified and Scalable Revenue Streams: Long-term viability depends on transitioning from grant funding to a mix of commercial and institutional revenue models. This includes enterprise licensing for corporate upskilling, institutional partnerships with universities for platform deployment, and certification fees for credential validation. By targeting multiple segments—ranging from individual learners to critical infrastructure operators—the project minimizes the risk of revenue concentration.

Lifecycle Governance and Ownership: To prevent "project-end abandonment," the consortium envisions a clear governance mechanism that persists beyond the 36-month duration. This involves identifying post-project lifecycle owners for the Key Exploitable Results (KERs), specifically the DCM System and the Certification Scheme, to ensure dedicated oversight for release governance and technical support.

Content Dynamism and Quality Assurance: A core component of this vision is the systematic update cadence of the training catalogue. Given the high likelihood of content becoming outdated due to the rapid evolution of cyber threats, the sustainability plan requires formalized partner engagement through Memorandums of Understanding (MoUs) and an editorial board responsible for biannual reviews and "fast-track" updates.

Technical Resilience and Security: The long-term vision requires the DCM platform to remain a secure, public-facing service. Sustainability includes a dedicated budget for hosting, patching, and security baseline hardening to maintain the "market asset" of trust and ensure compliance with GDPR and other legal data protection requirements.

7.1.2 Strategic Integration and Impact

By leveraging the strength of a European consortium validation, the project aims to become a recognized brand in the sector-specific niches of healthcare, maritime, and energy. This specialization serves as a competitive differentiator against generic commercial training platforms. Ultimately, the vision is to foster sustainable Public-Private Partnerships (PPPs) where Higher Education Institutions (HEIs) adopt a more entrepreneurial teaching approach, utilizing state-of-the-art tools provided by industrial partners to create a continuous pipeline of cybersecurity talent for the European Digital Single Market

7.2 Key issues and Risks

The long-term sustainability of CyberSecPro depends on maintaining an operational balance between (i) continuous platform availability and security, (ii) continuous content relevance and quality, and (iii) predictable revenue streams that cover operational costs and future evolution. This deliverable frames

sustainability as the ability to finance continuous content development, platform maintenance, and operational costs through diversified exploitation models (direct-to-learner, enterprise licensing, institutional deployment, certification-related revenue, and public-sector partnerships).

A first key issue is lifecycle ownership of the CyberSecPro Key Exploitable Results (KERs) as an integrated ecosystem (modules, MOOCs/learning paths, DCM platform, and certification scheme). The DCM (Moodle-based) is positioned as the enabling infrastructure for delivery, tracking, role management, course bundling and (future) certification flows; therefore, operational responsibilities, release governance, and support capacity must be clearly allocated to avoid single-point failures or "project-end abandonment".

A second key issue concerns content relevance and update cadence. CyberSecPro offers a large catalogue of sector-focused modules, delivered in multiple formats (courses, seminars, hackathons, seasonal schools). Keeping this catalogue credible requires systematic updates aligned with the fast-evolving threat landscape; otherwise, market differentiation erodes and customer willingness to pay declines.

A third issue is market positioning and adoption under competitive pressure. The current deliverable aims at identifying threats such as competition from commercial training platforms/MOOCs, economic constraints limiting training budgets, rapid evolution of threats requiring continuous updates, and market fragmentation/overlap of initiatives; it also highlights weaknesses such as limited initial brand recognition, dependence on continued partner engagement for updates, limited initial marketing resources, and the certification scheme still being under development.

A fourth issue is compliance and trust. Because the DCM platform relies on user tracking and training analytics to support multiple business models and future credentialing, data protection, confidentiality controls, and secure platform operations become central to sustainability (trust is itself a market asset).

Finally, a fifth issue is dependency management across partners. CyberSecPro's value proposition explicitly leverages consortium validation, sector depth, practical hands-on focus, and an integrated ecosystem approach; these strengths require a governance mechanism that persists beyond the funded project and can sustain partner contributions, decide roadmap priorities, and manage quality.

To support a structured and transparent sustainability assessment, the following table consolidates the main issues and risks identified for the long-term exploitation of CyberSecPro results. It provides an integrated view of technical, organisational, financial, legal, and market-related risks, together with their potential impact, likelihood, and corresponding mitigation measures. The table is intended to serve both as a risk awareness instrument and as a practical reference for partners responsible for post-project operation, governance, and continuous improvement of the CyberSecPro ecosystem.

Risk register (indicative)

Table 18: Key Sustainability Issues and Risks for the Long-Term Exploitation of CyberSecPro

Risk area	Risk description	Impact	Likelihood	Proposed mitigation / controls
Platform operations	Insufficient resources for DCM hosting, maintenance, upgrades, and support after project end (service degradation, downtime).	High	Medium	Define platform operator role(s), establish an operational budget line funded by exploitation revenues, implement minimum SLAs (availability, patching), maintain backup/DR procedures.
Cybersecurity of the platform	DCM is a public-facing Moodle-based service; delayed patching or	High	Medium	Security baseline hardening, regular vulnerability scanning, access control reviews, incident

Risk area	Risk description	Impact	Likelihood	Proposed mitigation / controls
	misconfiguration can lead to compromise, reputational damage, and loss of trust.			response plan, log monitoring, least-privilege role model.
Content relevance	Course/module content becomes outdated due to rapid threat evolution; reduces differentiation and willingness to pay.	High	High	Content owner assignment per module, annual/biannual review cycle, lightweight "fast update" mechanism, advisory input from industry partners, versioning and changelogs.
Partner engagement	Sustainability depends on continued partner engagement for updates; partner withdrawal reduces update capacity and sector depth.	High	Medium	Formalize post-project cooperation (MoUs), create an editorial board, define incentives (revenue share, visibility, co-branding), reduce dependency via maintainers pool.
Certification scheme maturity	Certification scheme not fully established; delays reduce monetization and market credibility of credential pathway.	High	Medium	Phase rollout: start with standardized completion credentials and verification; align progressively with ECSF-linked profiles; pilot with selected institutions/companies.
Market competition	Commercial platforms and MOOCs compete on brand, marketing, and scale; risks lower adoption/pricing power.	Medium–High	High	Focus messaging on differentiators (EU consortium validation, sector specialization, practical labs), target niches (energy/maritime/health), build partnerships with institutions/public sector.
Budget constraints in buyers	Economic constraints reduce training budgets; impacts enterprise/public procurement.	Medium	Medium	Flexible pricing tiers, modular purchasing (per track/module), public-sector co-funding opportunities, "train-the-trainer" institutional approach to lower delivery cost.
Fragmentation/overlap	Overlap with other initiatives creates confusion and reduces visibility and adoption.	Medium	Medium	Clear positioning, structured stakeholder mapping, alignment with EU frameworks, partner network as distribution channel; emphasize integrated ecosystem approach.
Revenue concentration	Over-reliance on a single revenue stream (e.g., only B2C or only institutional licensing) threatens	High	Medium	Maintain diversified exploitation portfolio (B2C, B2B licensing, institutional deployment, certification, public sector).

Risk area	Risk description	Impact	Likelihood	Proposed mitigation / controls
	stability if demand shifts.			
Brand recognition	Limited initial brand recognition outside EU projects slows adoption and increases acquisition cost.	Medium	High	Partner-led dissemination, showcasing success stories, reference deployments, coherent visual identity, leveraging sector events and public-sector partnerships.
Quality variability at scale	As modules are reused/white-labeled, delivery quality becomes inconsistent (hurts reputation and outcomes).	Medium–High	Medium	Minimal quality standards for reuse, standardized templates, trainer onboarding pack, periodic audits of reused offerings, feedback loops.
Legal/data protection	Learner tracking and analytics underpin the business models; weak GDPR/retention controls create compliance and reputational risk.	High	Medium	Data minimization, clear retention policy, role-based access to reports, DPIA where needed, documented lawful bases, secure processing agreements for institutional deployments.
IP and licensing	Unclear ownership/reuse rights for materials/tools reduces ability to commercialize or share across institutions.	Medium–High	Medium	Standard licensing model (e.g., partner-agreed content license), explicit third-party tool terms, content provenance tracking, reuse clauses in partner agreements.
Operational scaling	Growth in users/institutions increases support load; without scaling plan, user experience and retention worsen.	Medium	Medium	Tiered support model (self-service + paid support), documentation, automation for enrolment/reporting, capacity planning, prioritization of roadmap features.

7.3 Implementation plan and timeline

The implementation plan defines the structured transition of CyberSecPro results from project-funded operation to sustainable post-project continuation. While the exploitation scenarios and financial envelopes described in previous sections provide the strategic and economic rationale, this subsection translates them into phased operational steps.

The implementation timeline is structured into three sequential phases: (i) transition preparation, (ii) initial post-project stabilisation, and (iii) structured scaling and consolidation. These phases reflect progressive maturity rather than rigid deadlines and are designed to reduce operational risk during the transition period.

Phase 1: Transition Preparation (Final 6 Months of the Project)

During the final phase of the funded project, preparatory actions must focus on defining governance and operational ownership. This includes identifying the entity or partner responsible for hosting and maintaining the DCM platform, clarifying content governance responsibilities, and documenting procedures for system administration, updates, and compliance management. In parallel, a review of training modules and MOOCs should be conducted to ensure technical consistency, removal of outdated references, and alignment with the latest cybersecurity developments. Documentation of operational workflows, including onboarding processes and reporting mechanisms, should be finalised to support continuity. Financial planning during this phase should include confirmation of indicative cost envelopes, identification of minimum sustainability thresholds, and assessment of potential early institutional adopters willing to continue collaboration beyond the project lifetime. The primary objective of Phase 1 is to eliminate ambiguity regarding operational responsibility before project closure.

Phase 2: Post-Project Stabilisation (Months 1–12 After Project End)

The first year following project completion represents a stabilisation period focused on ensuring operational continuity under the selected governance structure. The DCM platform must remain technically stable, secure, and accessible. Regular system monitoring, security patching, and user management processes must be maintained according to defined procedures. During this period, emphasis should be placed on consolidating institutional partnerships and structured adoption under Scenario 1 and, where feasible, Scenario 2. Early post-project activities should prioritise low-complexity deployments that do not require significant structural expansion but demonstrate operational viability. Content review cycles should be implemented at least once during this period to validate relevance and maintain credibility. Feedback collected from participating learners and institutions should be analysed and integrated into improvement plans. The objective of Phase 2 is operational stability and proof of sustainability under real post-project conditions.

Phase 3: Structured Scaling and Consolidation (Year 2 and Beyond)

Following stabilisation, the focus may gradually shift toward structured scaling under Scenarios 2 and 3, depending on governance maturity and available resources. This phase may include expansion of institutional licensing agreements, broader deployment of MOOC-based learning pathways, and—where governance structures permit—the introduction or formalisation of certification-oriented services. Scaling during this phase should remain gradual and controlled to avoid disproportionate operational burdens. Expansion must be accompanied by proportional investment in platform capacity, user support, and quality assurance mechanisms. Periodic strategic reviews should be conducted to evaluate adoption trends, financial sustainability indicators, and operational risks. These reviews allow the consortium or designated operating entity to adjust pricing logic, partnership strategies, or technical investments based on observed performance. The objective of Phase 3 is to transition from sustainability maintenance to structured ecosystem growth while preserving quality, credibility, and financial balance.

Across all phases, sustainability performance should be monitored through measurable indicators that reflect operational continuity, adoption, financial coverage, and content relevance.

Operational adoption should be measured through:

i. the number of institutions with an active deployment agreement during the reporting year;
ii. the number of active learner accounts defined as users who log into the platform at least once within a rolling 12-month period; and
iii. the total number of module and MOOC enrolments per year, disaggregated by sector (health, energy, maritime, general).

Technical sustainability should be assessed through:

iv. annual average platform uptime percentage;
v. number of completed security patch cycles per year;

Educational relevance should be evaluated through:

vi. number and percentage of modules formally reviewed within the annual update cycle;
vii. learner completion rate per module and per MOOC pathway;
viii. average learner satisfaction score derived from structured end-of-module surveys; and

Financial sustainability should be measured through:

ix. annual operational cost coverage ratio (recurring revenues divided by total operational expenditure);
x. number of active institutional agreements renewed year-over-year.

Where certification services are operationalised, additional indicators may include:

xi. number of credentials issued annually;
xii. percentage of learners completing certification pathways relative to enrolments; and

These indicators are not designed to impose growth targets but to ensure that the CyberSecPro ecosystem remains operationally viable, financially balanced, technically secure, and educationally relevant throughout its post-project lifecycle.

7.4 Post-Project Operational Structure

The long-term sustainability of CyberSecPro depends on the establishment of a clearly defined post-project operational model prior to project completion which will be established outside the framework of the current Grant Agreement and shall not create financial or operational obligations for beneficiaries beyond those defined in the Grant Agreement unless formalised through separate legal arrangements. While the project does not mandate the creation of a new legal entity, continued exploitation requires the designation of responsible operational roles, technical oversight, and decision-making authority.

Operational sustainability requires clarity in four domains:

1. Technical Maintenance

Responsibility for DCM hosting, security patching, version upgrades, and system monitoring must be assigned to a designated technical partner or subcontracted service provider under defined service-level expectations.

2. Content Governance

A structured annual content review cycle shall be implemented to ensure alignment with evolving cybersecurity threats, regulatory frameworks (e.g., NIS2), and ECSF updates. Module updates may be distributed across contributing partners based on expertise.

3. Financial Oversight

Annual review of operational cost envelopes and cost coverage ratios shall determine whether current adoption levels sufficiently sustain platform continuity. If sustainability thresholds are not met, scope adjustments (e.g., scaling of services) may be applied.

4. Certification Governance

Activation of certification-enabled deployment requires a separate governance agreement specifying assessment standards, Credential issuance authority, Liability and verification processes, Data protection compliance.

Below a post-project timeline of important milestones is showcased.

Within 6 months after project closure:

- Decision on selected exploitation scenario(s).
- Nomination of Operational Coordinator.
- Definition of hosting and maintenance arrangements.

Within 12 months after project completion:

- First annual sustainability KPI review.
- Financial envelope reassessment.
- Content update cycle execution.

Beyond Year 1 post-project:

- Progressive institutional onboarding.
- Evaluation of certification readiness (if applicable).
- Expansion or consolidation based on adoption levels.

8 Conclusion

This deliverable has presented the structured exploitation, business, and sustainability framework for the CyberSecPro project. Building upon the market analysis conducted in D2.1 and the training development activities implemented under Work Packages 3 and 4, it has defined how the project's Key Exploitable Results can transition from EU-funded implementation to sustainable post-project operation. CyberSecPro delivers a coherent ecosystem consisting of sector-specific training modules, structured MOOCs, the DCM platform infrastructure, and a certification-oriented recognition approach aligned with European competence frameworks. While each component has standalone value, their integration within structured exploitation scenarios significantly enhances long-term sustainability potential.

The analysis demonstrates that sustainability does not depend solely on market demand, which remains strong due to persistent cybersecurity skills shortages across Europe, but rather on structured operational governance, realistic financial planning, and progressive institutional adoption. The three exploitation scenarios defined in this deliverable represent increasing levels of integration and maturity, allowing flexibility in post-project implementation depending on resource availability and stakeholder engagement. The financial framework provides indicative sustainability envelopes and break-even logic rather than deterministic forecasts. It illustrates the operational thresholds required to maintain platform stability, content relevance, and administrative continuity. Long-term viability will require disciplined cost management, prioritisation of institutional partnerships, and structured reinvestment of generated revenues.

From a strategic perspective, the following recommendations are critical for ensuring successful continuation:

First, partners should formalise the post-project operational structure before project closure, clearly defining roles, responsibilities, and decision-making processes.

Second, institutional licensing and structured partnerships should be prioritised in early post-project phases to secure stable and predictable revenue streams.

Third, periodic content and platform review cycles should be institutionalised to preserve relevance and maintain alignment with emerging cybersecurity threats and European regulatory developments.

Fourth, stakeholder engagement mechanisms should remain active beyond the funded period in order to support iterative improvement and maintain ecosystem credibility.

In conclusion, CyberSecPro has established a solid foundation for contributing to the European cybersecurity skills ecosystem. Its long-term success will depend not only on the technical and educational quality of its outputs, but also on disciplined governance, operational realism, and strategic coordination among partners. With structured continuation planning and gradual adoption, CyberSecPro has the potential to remain a relevant and sustainable sector-oriented cybersecurity training ecosystem beyond the lifetime of the funded project.