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

D6.1
Dissemination, Communication Plan and Exploitation

Document Identification	
Due date	2023-05-31
Submission date	2023-06-13
Version	1.0

Related WP	WP6	Dissemination Level	PU - Public
Lead Participant	CNR	Lead Author	Fabio Martinelli (CNR)
Contributing Participants	GUF, CNR, ACEEU, MAG, ZELUS	Related Deliverables	D6.2, D6.3, D6.4, D6.5

Abstract:

This document reports the dissemination, communication and exploitation plan for the CyberSecPro project. The approach is incremental and dynamic and considers the growth of material and experience that the project partners will elaborate.

This document also presents the dissemination and communication objectives and approach and lists planned publications and events. It describes the target audience and communication channels we plan to adopt as project.

Similarly, the exploitation and innovation approach presented in this document cover business scenarios and models, exploitation approach, knowledge and intellectual property management and protection, and sustainability.

Individual dissemination, communication, and exploitation activities from each partner focus on specificities of each partner and how they can contribute to increase the impact of the overall results.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594.

Executive Summary

This is the dissemination, communication plan and exploitation for the CyberSecPro project.

The dissemination and communication plan defines the communication objectives and approach, including target audience and communication channels.

The consortium identified plans at the individual and consortium level for increasing the dissemination and communication impact, including proper branding approaches, usage of social media and web portal.

The dissemination will involve several phases ranging from awareness on the project goals till advocacy of the results versus target audiences. A specific focus on training events is given in the project, including for PhD summer schools.

There is a significant commitment of the partners in achieving the planned results.

Similarly, the second part of the document describes the initial exploitation approach and strategies both at individual and consortium level. This also includes approaches for intellectual property management.

Document information

Contributors

Name	Beneficiary
Fabio Martinelli, Ilaria Matteucci, Alessandro Arena	CNR
Kai Rannenberg	GUF
Paresh Rathod	LAU
Cristina Alcaraz, Javier Lopez	UMA
Thorsten Kliewe	ACEEU
Natalia Christofi, Vaia Gousdova	FP
Spiros Borotis, Alexandros Rizopoulos	MAG
Kitty Kioskli	TRUSTILIO
Stella Markopoulou	ZELUS

Reviewers

Name	Beneficiary
Cristina Alcaraz	UMA
Thorsten Kliewe	ACEEU

History

Version	Date	Contributors	Comments
0.1	2023-03-01	Fabio Martinelli	ToC
0.2	2023-03-27	Fabio Martinelli	Initial skeleton
0.3	2023-05-04	Spiros Borotis	Minor changes and additions
0.4	2023-05-10	Spiros Borotis, Alexandros Rizopoulos	Several sections added
0.5	2023-05-21	Stella Markopoulou	Several sections added
0.6	2023-05-27	Fabio Martinelli, Alessandro Arena, Ilaria Matteucci	Contributions added
0.7	2023-05-28	Thorsten Kliewe	Comments on all sections, ACEEU-specific sections added, new sections on brand identity and web portal
0.8	2023-05-29	Spiros Borotis	Addressing reviewers' comments
0.91	2023-05-30	Stella Markopoulou	Addressing reviewers' comments
0.92	2023-05-31	Fabio Martinelli, Alessandro Arena	Addressing reviewers' comments and finalization
0.93	2023-06-03	Fabio Martinelli	Addressing latest review comments
0.94	2023-06-05	Atiyeh Sadeghi	Final check, layout correction and refinement and submission process
0.95	2023-06-08	Fabio Martinelli	Final check.
1.0	2023-06-12	Atiyeh Sadeghi	Final check, layout refinement and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
	ACM	Association for Computing Machinery
	API	Application Programming Interface
B	**B2B**	Business-to-Business
C	**CAGR**	Compound Annual Growth Rate
	CERT	Computer Emergency Response Team
	CERT-EU	Computer Emergency Response Team for the EU institutions
	CISPE	International Conference on Cybersecurity and Privacy Education
	CSIRT	Computer Security Incident Response Team
	CS	Computer Science
	CSE	Cybersecurity Education
	CSP	CyberSecPro
	CSTE	Cybersecurity Training & Education
D	**DSM**	Dynamic Syllabus System, Digital Single Market
	DCM	Dynamic Curriculum Management
E	**ECGFF**	European Coastguards Functional Forum
	ECSF	European Cybersecurity Skills Framework
	EDA	European Defence Agency
	ENISA	European Union Agency for Cybersecurity
	ECSF	European Cybersecurity Skills Framework
	ESG	External Stakeholders Group
	ETSI	European Telecommunications Standards Institute

	EU	European Union
	EUROPOL	European Union Agency for Law Enforcement Cooperation
G	**GDPR**	General Data Protection Regulation
H	**HEI**	Higher Educational Institutions
I	**IBM**	International Business Machines Corporation
	IEEE	Institute of Electrical and Electronics Engineers
	IEE INFOCOM	Institute of Electrical and Electronics Engineers - International Conference on Computer Communications
	ICT	Information and communications technology
	ICCERP	International Conference on Cybersecurity Education Research and Practice
	IoT	Internet of Things
	IPR	Intellectual Property Rights
	ISACA	Information Systems Audit and Control Association
J	**JRC**	Joint Research Committee
K	**KA**	Knowledge Area
	KPI	Key Performance Indicator
N	**NACGF**	Northern Atlantic Coast Guards Forum
	NIS	Network and Information Security
	NIST	National Institute of Standards and Technology
	NIS2	Network and Information Security Directive
	NRLA	National, Regional and Local Authorities
S	**SEO**	Search Engine Optimization
	SMEs	Small and Medium-sized Enterprises

STEEP	Social-Technological, Economic-Environmental-Political
SWOT	Strengths, Weaknesses, Opportunities, and Threats

Glossary of Terms

A **Generic Glossary of terms based on JRC, Taxonomy and glossary for Cybersecurity by European Commission**

Link: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

C **CSP training programme**

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

CSP training modules

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

CSP syllabus

every training module will be accompanied by a syllabus that will include information like Learning Outcomes; Who should attend; Relative conventions and standards; Prerequisite competencies (skills & knowledge); Training module outline; List tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training; Training tools that will be used; Assessment methods; Exams; Study time (physical and online learning).

A standard template for a CSP syllabus will be finalised in D4.1 ('CyberSecPro Training Operational Plan'), and it will be used in all CSP training modules.

CSP training material

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

CSP sector-specific training modules

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

CSP syllabus

every training module will be accompanied by a syllabus that will include information like Learning Outcomes; Who should attend; Relative conventions and standards; Prerequisite competencies (skills & knowledge); Training module outline; List tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training; Training tools that will be used; Assessment methods; Exam; Study time (physical and online learning).

A standard template for a CSP syllabus will be finalised in D4.1 and it will be used in all CSP training modules.

CSP knowledge areas

The knowledge areas listed were based on the CyBoK Skills Framework, JRC recommendation and mainly from the European Cybersecurity Organisation report based

on industry-academia cooperation and development work. However, the project will be further aligned with the ECSF and the market Analyses outcomes.

CSP practical skill

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

CSP competence

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

CSP training tools

Training tools that will be used in the training of the CSP modules (the assessment of the various tools, selection and portfolio will occur in T.2.3).

CSP training format

CSP training format describes the way how modules will be provided OnDemand, Web-based, Live Online, In Person, Hybrid/mix,

CSP Dynamic Curriculum Management System

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

The main requirements of the CyberSecPro DCM will be flexibility and responsiveness to the continuously changing cybersecurity market needs. Overall, CSP Dynamic Curriculum Management (DCM): The online Dynamic Curriculum Management (DCM) is an online tool that will be integrated by parametrising the Moodle or e-class open-source learning platform where the cybersecurity market needs will be monitored, and curricula will be managed.

1 Dissemination and Communication

The CyberSecPro project generates both tangible and intangible outputs through its activities, including training competence, data, knowledge, and information. These outputs are valuable resources that can be utilized by project partners and other stakeholders for further exploitation in several realms of cybersecurity, especially where cybersecurity skills and competences need to be increased. Effective communication and dissemination actions surrounding the CyberSecPro results, guided by clear objectives and strategies, are crucial for maximizing their impact.

The overall communication and dissemination objectives of CyberSecPro are as follows:

- Raise awareness: Promote awareness of the CyberSecPro project and the issues related to training and education for cybersecurity
- Reach diverse stakeholders: Engage a wide range of stakeholders from the scientific and industrial communities, as well as the general audience, with the key findings and results of CyberSecPro to ensure maximum impact during and after the project
- Transfer knowledge and results: Facilitate the transfer of CyberSecPro knowledge and results to enable others to utilize and adopt them, thus maximizing the overall impact of the project's research and development.

The dissemination and communication activities within CyberSecPro have been strategically planned in this deliverable with these objectives in mind. The project aims to achieve impact and contribute to competitiveness and address societal challenges in the cybersecurity domain. There is an increasing need of cybersecurity training and education capabilities.

Dissemination and communication efforts will effectively convey the project's messages and results to relevant communities.

1.1 Approach

CyberSecPro will maintain continuous and comprehensive communication to achieve the defined communication and dissemination objectives outlined in this document. These objectives encompass both general aspects, such as the project's vision and values, as well as specific goals, such as promoting and facilitating the adoption of a particular security tool.

To illustrate our marketing phases, we adopt a high-level dynamic model. This model consists of four primary communication phases: Awareness, Consideration, Conversion, and Advocacy. However, the communication logic within each phase and the overall model should remain agile to adapt to the dynamic communication and dissemination needs.

Each phase corresponds to a specific communication objective aimed at shaping the mind-set of the target audience towards CyberSecPro. Our communication and dissemination approach will progressively transition our communication targets from mere "recipients" (individuals who passively receive CyberSecPro information) to "practitioners" (individuals who trust and adopt CyberSecPro concepts and training modules) and finally to "promoters" (individuals who actively advocate for CyberSecPro solutions and actively promote the project). The ultimate goal of communication and dissemination is to engage stakeholders in support of CyberSecPro, contributing to the development of a resilient, secure, and digital Europe through well-established CyberSecPro education and training solutions that will improve the European cybersecurity workforce.

Each consortium member has developed an individual communication and dissemination plan that complements the project-level plan and caters to their specific targets and requirements. Consequently, while the communication and dissemination plan has been designed in a top-down approach, successful implementation relies on the collective efforts of all project members and will be executed in a bottom-up manner.

1) Awareness

During the initial communication phase, our primary objective is to capture the attention of the audience and generate awareness around CyberSecPro. The target audience during this phase is relatively broad, serving as the foundation for our communication pyramid. In this section, we will outline our prioritized marketing targets, although anyone interested in CyberSecPro concepts and solutions in general can be included. Given the current circumstances where remote work is prevalent and offline events are limited, the communication channels utilized in this phase will predominantly be web-based. This includes leveraging the CyberSecPro website and social media platforms, as web marketing enables swift and direct audience engagement and attraction.

2) Consideration

The focus of this phase is to pique the audience's interest and motivate them to consider and explore CyberSecPro solutions further. The project should plan targeted marketing campaigns accompanied by detailed technical information within dissemination materials. During this phase, communication channels such as conferences, workshops, seminars, and white papers can be utilized to provide in-depth information about CyberSecPro and encourage the audience to seriously consider adopting CyberSecPro.

3) Conversion

During this phase, our objective is to actively engage the audience and encourage them to adopt CyberSecPro solutions. A personalized communication approach is crucial as our target audience consists of diverse groups with varying expectations from CyberSecPro. Additionally, CyberSecPro solutions encompass techniques and tools contributed by various consortium members. To effectively communicate during this phase, scientific and communication events, including technology demonstrations, and technical training, should be powerful tools to convince the audience to become active users of CyberSecPro.

4) Advocacy

During this stage, our aim is to transform CyberSecPro practitioners or adopters into "CyberSecPro advocates" who actively promote and increase awareness, consideration, and conversion through word-of-mouth recommendations. This creates a positive marketing cycle within the model, amplifying its impact. Target audiences will have access to more research outcomes from the project and may even participate in validations, refinements, and demonstrations of CyberSecPro solutions.

To achieve the CyberSecPro dissemination and communication objectives and to guide the target groups through the 4 primary communication phases, we have planned the following activities across different stages:

1. Creation of information brochures: Develop comprehensive information brochures including branding guidelines, website materials, leaflets, presentations, and posters. These will be distributed at industry/academia fairs, conferences, and workshops to enhance visibility and provide valuable information about CyberSecPro;
2. Maintenance of interactive social media channels: Establish interactive social media channels to facilitate better communication among project participants and the external world. We will actively engage in email lists and forums to draw attention to the project;
3. Organization of specific events: Organize workshops, training events, PhD schools, and other events as essential tools for disseminating project results. We will invite stakeholders to participate in these events, which not only provide valuable feedback and validation of project outcomes but also help spread awareness among the stakeholders;
4. Utilization of various dissemination media: Utilize diverse media channels for dissemination, including news articles, scientific journals, the internet, conferences, and workshops. A press campaign will be conducted to raise awareness about our objectives and progress within various end-user communities.

By implementing these activities, we aim to foster engagement, communication, and dissemination of CyberSecPro, ensuring its wide recognition and adoption within the cybersecurity community and relevant stakeholders.

1.2 Target audiences

The project involves several stakeholders, and we can consider the following target audiences:

- **Security services and/or training providers:** These organizations can benefit from using or licensing CyberSecPro solutions to enhance the security or privacy-preserving capabilities of their products and services;
- **Enterprises and Small and Medium-sized Enterprises (SMEs)**: CyberSecPro solutions offer significant value to enterprises and SMEs, enabling them to increase their workforce competence that is critical to develop secure products, and services;
- **Academia:** contribute to their training and education activities in the area of cybersecurity and increase the capability to build a new generation of skilled researchers and practitioners;
- **Policy-making bodies** (certification stakeholders, ministries of education, National Cybersecurity Competence Centres, ENISA, ECC): impact standardisation and policy-making activities around cybersecurity training and education capabilities;
- **Individual trainees and practitioners**: Individuals will benefit the CyberSecPro solutions to increase their skills and competences;
- **General public:** The general public is also a target audience for CyberSecPro. The objective here is to raise awareness about the importance of security in their daily activities and encourage them to adopt CyberSecPro techniques and tools. This engagement helps in delivering a secure, resilient, and digital Europe.

By addressing the specific needs and concerns of these target audience groups, CyberSecPro aims to provide tailored solutions and effectively contribute to improving cybersecurity in various sectors and among the general public.

1.3 Communications channels

Social media channels offer a powerful platform for the dissemination and communication of the project's progress, milestones, and outcomes. These digital platforms not only increase the visibility of the project but also foster open dialogue, collaboration, and knowledge exchange amongst diverse stakeholders. Through LinkedIn, Twitter, and YouTube, we can reach a wide variety of audiences, from industry experts and policymakers to students and the general public, highlighting the impact and significance of the CyberSecPro project in real-time. These platforms also allow us to create a sense of community around the project, promoting stakeholder engagement, collaboration, and feedback.

Furthermore, social media platforms serve as an invaluable tool for promoting events, workshops, and webinars associated with the project. By providing real-time updates and facilitating online discussions, these platforms can maximize audience participation and engagement, making them an integral part of the project's communication and dissemination strategy. Equally important, these platforms offer a diverse and pluralistic space for the project's messages, reflecting the multifaceted nature of the CyberSecPro project and its impact on various sectors.

ZELUS plays a pivotal role in ensuring the smooth operation and strategic utilization of these social media platforms for the CyberSecPro project. Tasked with creating and running the project's social media channels, ZELUS acts as the central node, curating and posting content provided not only by its team but also by all the project partners. This process not only ensures that the content shared is accurate and up to date, but it also contributes to the diversity and pluralism of the messages communicated, echoing the collaborative and inclusive spirit of the project.

In addition, ZELUS is committed to encouraging and facilitating active participation from all project partners on these platforms. By inviting partners to contribute with project updates, achievements, and relevant content, ZELUS ensures a broad range of perspectives and voices are represented, reinforcing

the collective effort and diverse expertise that underpin the CyberSecPro project. Ultimately, ZELUS's work in managing the project's social media channels is crucial in enhancing the project's visibility, stakeholder engagement, and impact, all while emphasizing the importance of diversity and collaboration in this ground-breaking project.

1.3.1 Brand identity

Given the central role that a strong project brand identity plays in the success of dissemination and communication efforts, the CyberSecPro team has undertaken significant efforts to design a visual identity. The process has been collaborative and integrated all project partners to ensure that the resulting brand identity is accepted by the consortium partners.

Following a workshop in early 2023 in which project partners outlined their ideas and opinions, a designer developed a variety of logo alternatives. Through a 2-step process in which each project team member was able to vote, a final logo was selected (see image below). Minimal adaptions to the logo are currently undertaken and different versions for different purposes are created. In addition, the core visual elements are currently being defined (see Figure 1). These elements build the basis for the creation of all marketing material (as defined in this document).

Figure 1: CyberSecPro logo and brand identity

1.3.2 Web portal

The web portal is currently on line at the URL: https://www.cybersecpro-project.eu/. In order to manage the large size of the project team (>100 individuals) and the commitment that dissemination and communication activities are shared among the partners, an admin platform is currently being developed as the central point for all information on dissemination and communication. In the platform, each partner can update its own information (e.g., organisational logo, social media accounts) and add dissemination and communication efforts it is planning or has undertaken (i.e., events, publications, media appearances). In the near future, the data will be fed into the project website so that the information is constantly updated. In addition, the system will be core in monitoring the dissemination and communication efforts as it provides a dashboard comparing targets and achievements. Two screenshots of the beta version of the admin platform can be found in Figure .

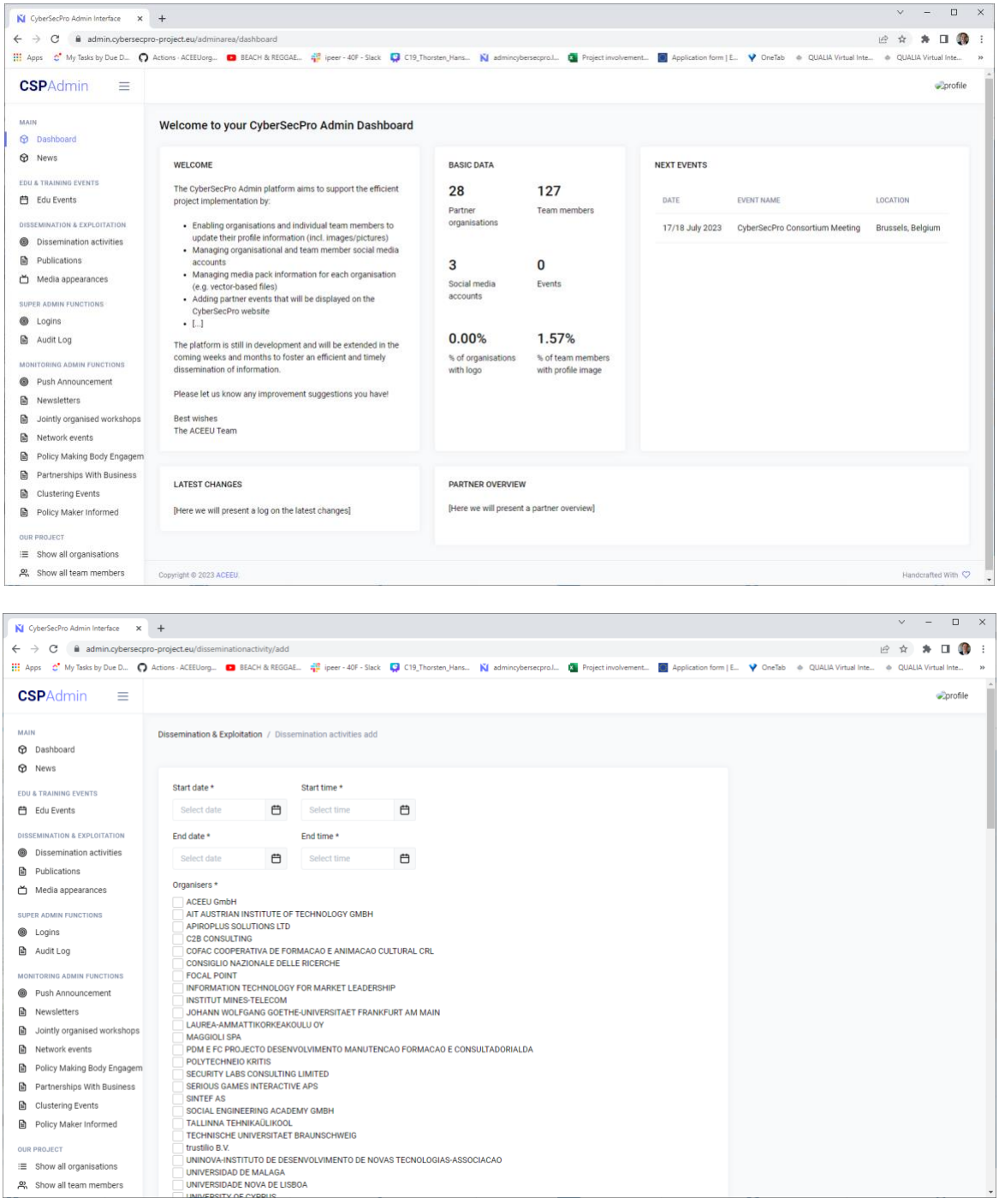

Figure 2: Screenshots for new admin

1.3.3 Social media

In establishing a robust online presence for the CyberSecPro project, ZELUS has successfully launched dedicated LinkedIn and Twitter accounts. These platforms, meticulously curated by ZELUS, serve as key pillars for the project's digital communication and dissemination strategy:

- LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject
- Twitter: https://twitter.com/CyberSecPro_eu
- YouTube: https://www.youtube.com/channel/UCQaoldKcHbjMFJpBwOgU9Xw

The LinkedIn page acts as a professional hub where beneficiaries, industry experts, and other stakeholders converge for meaningful exchanges, fostering a collaborative atmosphere. The page was set up during the second month (M2) of the project. Initially, the activity was slow, as the focus was primarily on internal consortium alignment rather than external communications. However, starting from the fifth month (M5), the CyberSecPro LinkedIn page became more active and populated with project updates, achievements, and relevant content, making it a go-to source for comprehensive information about the project. Moreover, LinkedIn will play an instrumental role in promoting various events, workshops, and webinars, thereby maximizing stakeholder engagement.

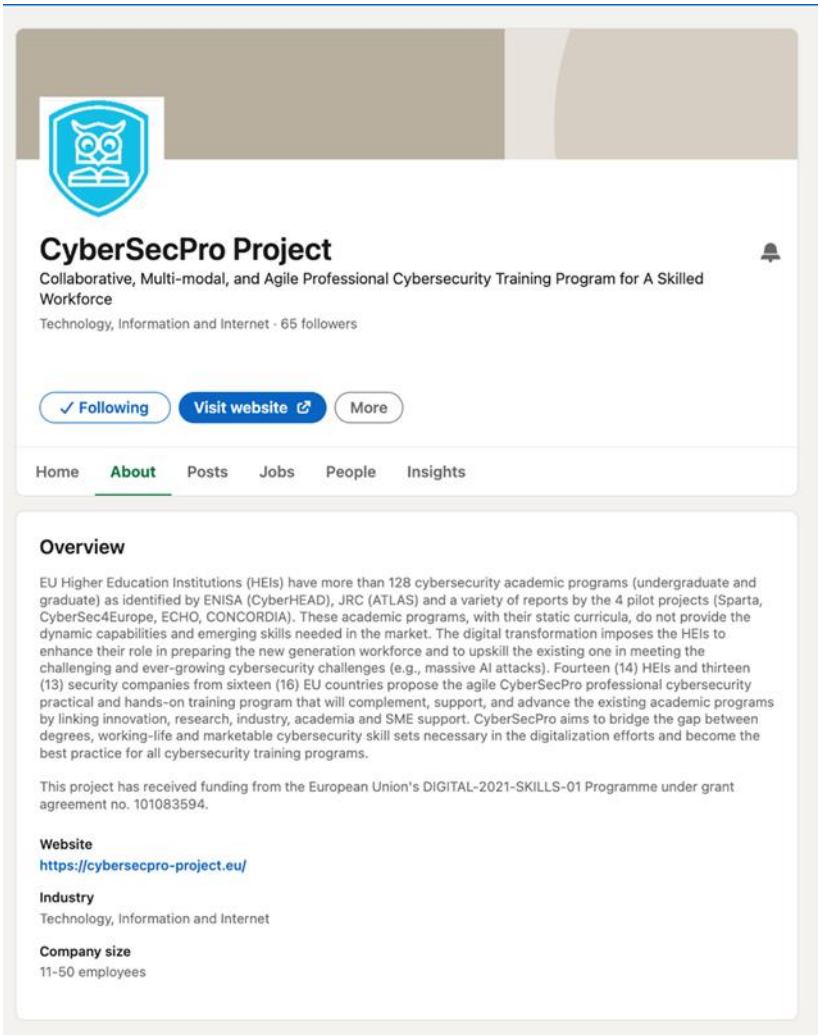

Figure 3: CyberSecPro LinkedIn Page.

Similarly, the Twitter account was launched back in February 2023 (M2 of the project) and has remained active ever since. Twitter provides a real-time snapshot of the project's progress. By leveraging the platform's dynamic nature, ZELUS has managed to facilitate a consistent flow of updates and announcements related to the project. Beneficiaries have been invited to be actively engaged in this platform, tweeting about milestones, sharing relevant content, and using project-specific hashtags to drive the conversation. The active contributions from all partners on this platform will the reach of CyberSecPro's messages, connecting with a broad audience that includes cybersecurity experts, industry leaders, and policymakers.

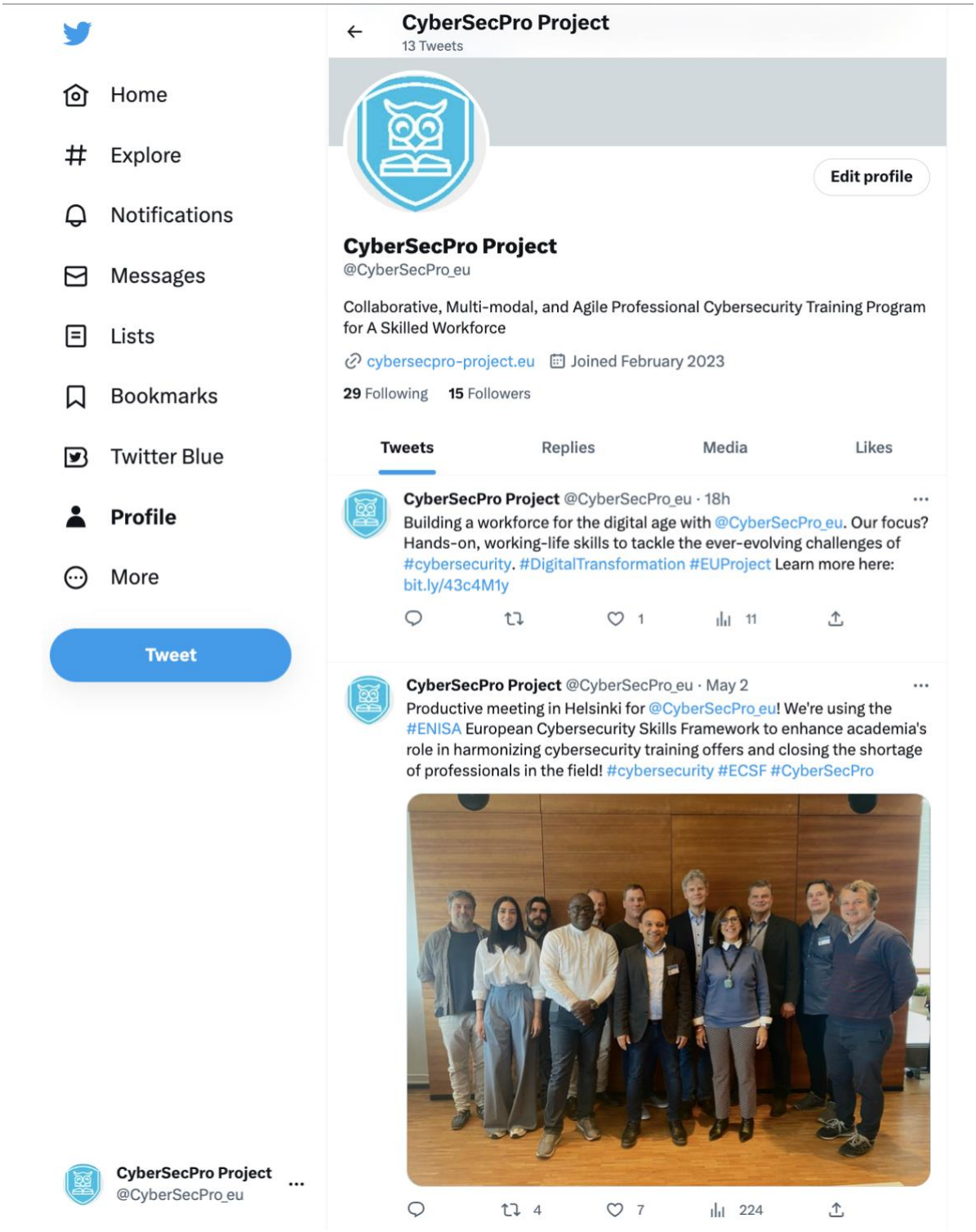

Figure 4: CyberSecPro Twitter Account

Additionally, a dedicated YouTube channel for the CyberSecPro project is already in place, providing even more exciting opportunities. This exciting platform will soon be populated with high-quality video content that brings the project to life in a whole new way. The YouTube channel can be an engaging visual journey through the project's developments and accomplishments, further enhancing the reach and impact of CyberSecPro. This social media platform can prove of great significance for the dissemination and communication efforts of the project especially in reference to the hosting of virtual events, educational videos etc.

Finally, the active involvement of all partners in the CyberSecPro project's social media channels is vital for multiple reasons. Not only does it ensure that a diverse range of perspectives, ideas, and voices are represented, but it also reinforces the collective, collaborative ethos that underpins our project. Each partner brings unique expertise and insight to the table, and their contributions to the social media posts enrich the overall narrative of the project, providing a comprehensive picture of the work being done. Moreover, regular monthly contributions from each partner ensure that our platforms remain vibrant, dynamic, and relevant, reflecting the ongoing progress and achievements of the project. This commitment to shared participation amplifies the project's reach, fosters deeper engagement with our audiences, and, crucially, illustrates the collective endeavour that makes the CyberSecPro project a ground breaking initiative in cybersecurity education and training.

1.3.4 Campaigns

Social media plays a significant role in promoting project-related events, workshops, and webinars. Through targeted campaigns, these platforms help build anticipation, increase attendance, and extend the event's reach and impact. Post-event, they facilitate the continued dissemination of key insights and discussions, ensuring the sustainability of the event's outcomes. That said, ZELUS will mobilize the CyberSecPro social media channels throughout the lifespan of events organized by the CyberSecPro consortium and/or partners of the project individually. To maximise the impact of such campaigns ZELUS will closely collaborate with all partners via the implementation of the following steps:

- Step 1: The partner should inform ZELUS via email with the details of the event they plan to organize at least one month before the event;
- Step 2: ZELUS will prepare promotional posts for the event aiming to raise awareness and attract a targeted audience;
- Step 3: During the event, the event organizer should share with ZELUS real-time photos and text to generate live tweets for sharing on social media.

ZELUS can also provide support with creation of templates for email invitations and other material upon request.

1.3.5 Key messages

Communications from the project should be in the context of a uniform set of messages, which evolve as the project and its findings become refined.

During the initial phase of the project, the key messages echo the project overarching goal i.e.,

CyberSecPro's ambition is to enhance the role of the Higher Education Institutes (HEIs) in offering hands-on and working-life skills for driving a trustworthy digital transformation in critical sectors of the economy. The enhanced HEIs will equip the workforce with the necessary capabilities to address the digital challenges and be capable to develop secure privacy aware innovative ICT and industrial products that serve people, businesses and working-life communities practising their democratic values and rights. By establishing a unique Learning Factory, CyberSecPro will be an authentic environment to link innovation, research, industry, academia, and SME support. The outcome of the CyberSecPro is to empower the NextGen Europe.

Communications towards the wider community should consider the External Stakeholders Group (ESG) of the project that in addition to technical development support is also devoted to assess and improve the exploitation efforts.

Communications associated with research publications will summarise the abstract of the associated paper, poster, or presentation.

1.4 Publications

1.4.1 Press release

Partners may handle their individual press releases independently, using agreed text that will be agreed on WP6 activities.

1.4.2 Promotion

Information about the project will be distributed at relevant events, conference, and workshops as well as target audience events.

Interactive project only forums (as svn) will be created to support communication among the project participants. Similarly social media, web portal and other tools will be used to promote the project. We will make use of different media for the dissemination, including news articles, scientific journals, Internet, conferences, and workshops.

Special emphasis will be placed on fostering open access of CyberSecPro results. The consortium will be in contact with the EU and make available results and documents (reports, deliverables, and data) at an open access portal. The Consortium will fully address the European Commission requirements through the support of open access for published articles. All scientific publications of project's results will be granted open access according to publisher and law regulations as set out in the Grant Agreement. Depending on the nature of the publication, the articles will be made available immediately through open access publishing ("gold" open access) (e.g., by an open access journal) or within a period of 6 months through self-archiving ("green" open access).

1.4.3 Brochure

A brochure will be created to support all partners in the promotion of CyberSecPro. This brochure will contain information on the CyberSecPro project objectives, information about the Consortium and the CyberSecPro approach to cybersecurity training.

1.4.4 PhD schools

CyberSecPro researchers will utilise significant experience of running summer school as FOSAD and (one of the PhD summer schools in computer security with the longest tradition) and NeCS, that was held in Trento in 2023 and already supported by CyberSecPro. Also, CyberHOT Summer School series will be supported.

1.4.5 Conferences, seminars and events

The project partners are committed to producing presentations at conferences and seminars and related industrial and policy making events. Attention will be devoted to scientific publications to disseminate the project results as well as white papers and webinars. When possible, recording of the material will be promoted in order to maximise impact and adoption of the solutions.

We list here some venues and conference series we plan to contribute and attend:

- Information Security Education (WISE);
- International Conference on Cybersecurity Education (CSE);
- International Conference on Cybersecurity and Privacy Education (CISPE);
- International Conference on Cybersecurity Education Research and Practice (ICCERP);
- IT Training & Events by ISACA;
- Cybersecurity Training & Education (CSTE) Conference.

1.5 Individual dissemination and communication plans

GUF

GUF is the public research university in Frankfurt/Main, the 5th largest city in Germany and one of the top business and logistics hubs of Germany including critical infrastructures like the management of the .de domain, the country-code top-level domain for Germany, and Frankfurt airport (FRA). Dissemination and communication are among the main objectives of GUF and this is usually done though publications, participation in events, collaboration with the scientific and professional community including media releases to different target groups. For CyberSecPro the goal is to further strengthen the scientific and professional presence. GUF researchers are active in the scientific community by publishing in international journals and conferences. GUF members have also a significant experience in running summer schools as the IFIP Summer School on Privacy and Identity Management (since 2007 Kai Rannenberg has been active in e.g., the Programme and the Steering Committee).

IMT

Institut Mines-Télécom is France's leading public group of engineering and management graduate schools. It is made up of eight public graduate schools: IMT Atlantique, IMT Mines Albi, IMT Mines Alès, IMT Nord Europe, Institut Mines-Télécom Business School, Mines Saint-Étienne, Télécom Paris and Télécom SudParis and two subsidiary schools: EURECOM and InSic. It leads and develops a rich ecosystem of partner schools, economic, academic and institutional partners, and players in training, research and economic development. Created in the 19th century to meet France's economic and industrial development needs, Institut Mines-Télécom graduate schools have accompanied every revolution in industry and communications. Through research and training of engineers, managers, and PhDs, Institut Mines-Télécom takes up the major industrial, digital, energy and ecological challenges in France, Europe and around the world. Nowadays, with its schools Institut Mines-Télécom is working to imagine and create a world that combines science, technology and economic development with respect for the planet and for the women and men who live on it. Cybersecurity is one of the twelve strategic themes of IMT for 2023-2027, within our contributions to digital economy and sovereignty. In the context of CyberSecPro, we will circulate the activities of the project to our community, inside Institut Mines-Télécom (Cybersecurity and Risk) and within the French cybersecurity research and education community (GDR sécurité, RESSI Conference, etc.)

LAUREA

LAUREA plans individual dissemination activities in multiple ways including conducting and participating workshops, clustering activities, exhibitions, scientific events, hackathon, personal contacts with existing partners and collaborators. Further, LAUREA will disseminate the results of CyberSecPro at workshop, conferences, seminars, journals, and general publication. Also, LAUREA plans to participate in events and workshops to raise awareness on the project's progress and real-world implications including and not limited IEEE, ENISA (EU), ECCC, ECCO, ECSO (Brussels) events, awareness and capacity building efforts.

LAUREA also disseminate the CyberSecPro progress, results, assets, knowledge and services within their educations, training and RDI activities. LAUREA will leverage its existing partners and industry networks to disseminate the project's progress, results, knowledge and services to relevant diverse target groups.

TUC

TUC aims to target the broad research community in the field of cybersecurity, IoT security, cybersecurity training, cloud application development and virtualized networking domains. Furthermore, through its educational activities it will target CS and Computer engineering students (at

all levels), as well as working professionals in startups, SME and larger established companies operating at the national and European economic area. TUC plans to disseminate the research outcomes of CyberSecPro primarily in highly respected conferences, journals, and related publications. Taking advantage of physical or virtual events organised in relation to such activities, TUC also plans to participate in workshops, presentations, and booths in order to engage the participating research community. TUC plans to publish at least two papers in journals or magazines and five or more papers in conferences/workshops. Besides participating in the activities of said events, TUC will also consider the organization of specific workshops, presentations, and summer schools. These activities can be organized with the collaboration of Telecommunication Systems Institute or other Academic and research institutes in Greece, and/or as part of events or exhibitions organized by other research or industrial bodies. Examples of such activities include networking events of EU research projects, workshops organized by projects such as REWIRE that aim to follow up on the efforts of the four pilot cybersecurity research projects and bring together the research communities and industries. TUC members have also linked with ENISA (EU agency for Cybersecurity) and have organized educational events in the form of summer schools in the past. TUC will try to organize similar events to promote the results of CyberSecPro.

TUBS

TUBS, as a leading institution in education, research, and technology, recognizes the vital role of effective dissemination and communication in ensuring the successful execution and impact of the CyberSecPro project. A strategic dissemination and communication plan has been developed to align with the project's objectives and maximize its reach to relevant audiences.

TUBS will use its existing academic and industry networks to disseminate the project's progress, results, and knowledge to a diverse audience including academia, researchers, students, industry professionals, policymakers, and the general public. TUBS will make extensive use of its institutional website, social media platforms, seminars, workshops, and conferences to communicate the project's findings. Additionally, TUBS will leverage its position as an active member of the higher education community in Europe to facilitate communication exchanges with other HEIs.

TUBS will also contribute to the project's social media campaigns, providing regular updates on its activities within the project. The social media activities will be coordinated with project partners to ensure a consistent and engaging message is delivered. TUBS is committed to promoting any CyberSecPro-related events and will make sure that these events are well publicized through various communication channels.

UCY

UCY is the leading public higher-education institute in Cyprus and provides education to all levels, undergraduate, graduate and PhD. UCY is active in research related to systems security and privacy and many of the outcomes are published in established conferences. It is therefore expected that many activities of the CyberSecPro project will be linked with published research papers. Moreover, UCY has established courses in undergraduate and graduate level for system security, data security and software analysis. These courses will be enhanced with the ideas materialised in the context of the CyberSecPro project.

UMA

The University of Malaga (UMA) is a public institution of Higher Education that provides university education in Spain. As a university institution, UMA is particularly interested in carrying out some dissemination and communication activities; in fact, both aspects are among its main objectives. For example, UMA researchers are quite active in publishing in international journals and conferences, particularly in the field of cybersecurity. But also, UMA shows interest in participating in specific events and/or conferences related to CyberSecPro. It is intended, therefore, to promote the participation of researchers in conferences and events of great interest to the scientific and academic community. Through these activities, UMA could interact with different types of actors and know/understand the

different perspectives in the field of application, especially those applied in critical sectors such as energy. Likewise, UMA will contribute in training sessions (for other trainers and students), as well as in the organization of webinars if necessary. On the other hand, although UMA is not directly involved in the organization of Summer Schools, it is interested in promoting the participation of UMA members, mainly PhD students and professors, as a way to recycle knowledge and improve technical skills.

CNR

CNR is a main public research body in Italy. Dissemination and communication are among the main objectives of CNR and this is usually done though publications, events participation and organization, and with videos and press releases. For CyberSecPro the goal is to strengthen the already visible scientific presence and increase objects like the cybersecurityosservatorio.it that already present several sources of information for the researchers and practitioners interested in cybersecurity. The members of the project are quite active in the scientific community by publishing several papers in main journal and international conferences. CNR researchers have also a significant experience on running summer schools as the FOSAD one (since 2012 edition, Fabio Martinelli is the chair of the scientific committee), one of the long-lasting PhD summer schools in computer security. CNR in addition to the SERIT platform and dissemination also runs the security@fosad.org mailing list (with 1500 addresses of scientists world-wide). CNR also considers communication activities at the wider audience as relevant. The CNR brings expertise of the CNR Web TV that disseminates the CNR results through several means including audio-video materials. Fabio Martinelli was last interviewed by Italian TV RAI about the cybersecurity observatory endorsed by the Tuscany Region (www.cybersecurityosservatorio.it).

COFAC

COFAC is an educational entity hosted in Lisbon, Portugal, which is currently the largest non-profit educational organization in Portugal not funded by the State. COFAC is the entity legally responsible for the management and development of the Universidade Lusófona (Lusófona University), among many other Higher Education Institutions in Europe, Africa, and South America. Within the scope of CyberSecPro, COFAC will promote and organize targeted workshops, webinars, and training sessions, develop the component of Multifaceted Evaluation, Benchmarking and Best Practices and will publish comprehensive materials and scientific research, participate in conferences, and foster collaborations with national and international universities, public and private organizations, and industries. COFAC has several observatories, cybersecurity laboratories e.g., LAPI2S - Laboratory of Privacy and Information Systems Security and governmental accredited research units e.g., COPELABS headed by Dr. Marko Beko; COFAC also maintains a regular presence and communication stream about cybersecurity in the media.

SINTEF

SINTEF is located in Norway and one of Europe's largest independent research organisations. Part of our mission is to spread research results and create benefit to the research community, organisations, and the society as a whole. Within CyberSecPro, SINTEF's dissemination and communication approach covers the following:

- Identification of target audience: Including researchers, scholars and students, policy makers and government agencies, professionals within industry and the technology sector, and general public;
- Publishing: Targeting open access peer-reviewed journals and conference proceedings;
- Online presence: Create a project information page on our Web-site, which has more than 3 million views annually. Social media: Per 11.04.2023 SINTEF SoMe accounts have 180.964 followers and these channels can be used to share research highlights, news, and engage with the audience. SINTEF's podcast and blog have about 5K weekly downloads/views;
- Collaboration and networking: Organize and participate in cyber skills workshops and seminars to foster collaboration and knowledge exchange with other research institutions, industry

partners, and policymakers. SINTEF has already proposed a workshop as part of the 10th ACM Celebration of Women in Computing – womENcourage (https://womencourage.acm.org/2023/). SINTEF actively seeks collaborations with other research institutions, industry partners, and organizations to enhance the impact and visibility of research outcomes and engages with professional networks and associations to disseminate research findings among relevant communities. This includes the Norwegian Computing Society, the Norwegian Information Security Society, OWASP Norway and ACM;

- Media engagement: Facilitate interviews with researchers for print, broadcast, and online media outlets. Contribute opinion pieces and feature articles to popular media outlets related to the project topics;
- Public engagement: Organize public lectures and talks by institute researchers to engage the general public and promote scientific literacy. Participate in science festivals and exhibitions to showcase research outcomes and interact with a diverse audience;
- Evaluation and feedback: Continuously evaluate the effectiveness of dissemination activities through metrics such as website analytics, social media engagement, publication citations, and feedback from stakeholders. Use this information to refine and improve future dissemination efforts.

UNI-UNINOVA

UNINOVA is a non-profit research institute located in Portugal, inside the campus of the Science and Technology Faculty of the NOVA University of Lisbon. NOVA is an academic institution, based in Lisbon. Both partners will disseminate the project by publicising it through publications in reputed conferences and journals, organisation of and participation in workshops, webinars, training sessions and other academic events and online presence for publicising the project's results. Both partners will also foster synergies and collaborations with both national and international institutions, from universities to public and private organisations.

UPRC

UPRC is an academic institution that offers undergraduate, graduate and postgraduate programs and courses in cybersecurity. UPCR manages and participates in national, EC and international R&D projects in cybersecurity, and participates in cybersecurity exercises.

APIRO

APIROPLUS Solutions Ltd. (APIRO) is an SME located in Cyprus. The company provides cybersecurity related Consulting, Auditing and Training services. APIRO fully understands the importance of dissemination and communication in the context of such a project and is committed to actively contributing to the project's dissemination and communication initiatives. The approach of APIRO regarding dissemination and communication can be condensed to the following two steps: Step 1. APIRO personnel shall participate in the project work as prescribed and required, shall monitor the work being carried out and shall keep informed on the developments of the projects. Step 2. When information that could interest parties APIRO is related to, is identified, suitable dissemination and communication activities will be planned and carried out. To facilitate the dissemination and communication of the relevant information, APIRO will use the company's social media accounts, will participate in relevant workshops and conferences, will present to various stakeholders in Cyprus and in Europe in general and will present and liaise with other European and National funded projects.

C2B

C2B is a French SME located in the Southern Part of France. The company has been deeply involved in providing expertise for the Maritime community. From 2018 to 2021 it conducted a study on Maritime cybersecurity and contributed to the inception of a Maritime CERT dedicated to federate wills and needs. In 2017 a study has been conducted by the company to update the EU Coastguards sectorial

qualification framework (SQF). These to missions have conducted the company to identify the specific needs of coastguards in Cybersecurity.

A set of measures on targeted audiences will help C2B to reach its objective to:

- identify main target audiences;
- insert cybersecurity within the coastguards SQF;
- promote on the hands training dedicated on specific maritime systems (AIS, GNSS, ECDIS) used by coastguards.

FP

FOCAL POINT (FP) is a Belgian based SME providing comprehensive solutions mainly on Cybersecurity issues related to Cyber Incident Response. Focal Point will participate in dissemination, communication and exploitation activities to increase the impact of the overall results of the CyberSecPro project in different ways:

- FP will actively post on its social media channels (LinkedIn, Twitter, Website) regarding CyberSecPro Project. The posts can vary from information regarding CyberSecPro to small videos, promotion of CyberSecPro events, etc;
- FP will also push to disseminate the project across multiple events. An event coming up where FP is one of the co-organisers is CyberHOT Summer School on 29th September 2023 (https://www.cyberhot.eu/). FP has communicated this to partners through an email. More events that FP would push the dissemination of the project could be linked to the policy area as CSP closely follows the rapid developments in the policy area (e.g. ECSF ongoing work, ESDC work, ECC and Cybersecurity skills certification efforts). FP has good connections with standardization bodies such as ENISA and ETSI;
- FP, as a commercial partner, will also organise trainings to the project's academic partners. So far, there is an upcoming joint training where FP will be partnering with UPRC to provide training to the trainers.

ITML

ITML is an SME company located in Athens, Greece which as research performer and technology developer is continuously designing, developing, and offering platforms, tools and products towards the cybersecurity protection; the data fusion (from multiple modality data streams) and analytics (ML-based big data analytics and insights through AI models). ITML aims to disseminate in regular basis the progress and the outcomes of CyberSecPro project, not only to enhance its (ITML) market position with respect to the relevant technologies but also to promote the researches and innovation's findings. Finally, ITML through its individual dissemination plan aims to support and enhance synergies between CyberSecPro project and other Horizon Europe funded projects that we are engaged. ITML considers as target groups, to which it will communicate and disseminate the results and findings: other research and technology providers; other cybersecurity companies; Higher Education Institutions (HEIs); Research Institutes; Universities. The planned dissemination and communication activities will be delivered through online channels (website and social media). Therefore, in order to enhance the visibility of the project and communicate the progress and outcomes of CyberSecPro project, ITML is aiming for regular: (1) website activity (dedicated section @ https://itml.gr/, News) and (2) social media activity: LinkedIn, Twitter, Facebook official channels. In addition, ITML will participate in public events, workshops related cybersecurity training.

MAG

Large ICT company with customers in Europe and beyond. These will be our dissemination and exploitation target. MAG has established the MAGGIOLI Academy and the existing trainees will be our initial exploitation group.

SGI

Dissemination and communication are usually done though SGI's SOME channels, participation in events and preparing workshops. We have around +6000 followers on LinkedIn and Facebook but these are not necessarily only aimed at cybersecurity.

SLC

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

Trustilio

An SME that offers consultation and professional trainings in Cyber Threat Intelligence; Human-Centric Security Management; Sectoral Security (maritime, health); Self-Audit; Hands-on Personalised Cyber Training; Sector Specific Behaviour Change Interventions; Behavioural Science; Behavioural Economics; Cyber psychology; Human-Computer Interaction; Business and Business Process Reengineering. Participates in standardisation efforts (ETSI, NIST, ISACA, NATO, ENISA) and has a long publication record.

ACEEU

ACEEU is an international quality assurance body aiming at promoting, evaluating, and celebrating excellence in entrepreneurship and engagement in higher education. Aligning universities and their education and training offers to the needs and demands of business and society is one of the core challenges ACEEU is working on. Disseminating and communicating methods, models, tools, experiences, and best practices is a core priority of ACEEU. Central dissemination and communication channels include social media (Twitter and LinkedIn), the ACEEU website, ACEEU's online magazine Spotlight, the ACEEU "Project Updates" section of its EU Project Unit, the annual ACEEU Forum, the ACEEU mailing list (around 1000 subscribers) as well various smaller scale events (e.g. workshops and webinars) that ACEEU hosts yearly. The main target group for CyberSecPro dissemination will be university representatives (university leaders, academics, professionals) who are interested in learning more about (1) training development that is relevant to business and society (transversal topic), and/or cutting-edge cybersecurity trainings (specific/technical topic).

UNSPMF

UNSPMF is academic institution located in Novi Sad, Serbia. UNSPMF will exploit the networks and communication channels that already exist at partner institutions and related projects that can reach the specific stakeholder of interest. UNSPMF plans to participate on the events, publish articles and papers, collaborate with other projects, and participate in the relevant exhibitions in order to present the project results and to get feedbacks from the community. The main technical outcomes, activities and results will be disseminated in the various workshops with the main objective to inform, collect and summarize the learnings for future exploitation. Also, the UNSPMF team will use its University courses to present project results with aim to share knowledge and to support establishing of a community of future industrial engineers.

2 Exploitation Strategy and Business Planning

2.1 Objectives and phases of exploitation strategy

In Europe today 44% or 169 million people do not have basic digital skills and of these, 77 million people have no digital skills at all. Furthermore, Europe lacks a growing number of ICT specialists with there being already over 350,000 vacancies for ICT specialists in Europe. This is a serious problem for Europe, as our countries are getting more and more digitised, and everyone needs cybersecurity skills to take part in a trustworthy society and to work safely.

The education cybersecurity market is expected to grow in USA by a compound annual growth rate (CAGR) of 13.9% by 2030[1]. Cybersecurity, also known as information technology security, is the practice of protecting electronic information by mitigating information risks and vulnerabilities. It is a process that defends an organization's computer systems, networks, and data from unauthorized access or theft. Cyber attacks can come in many different forms, including viruses, ransomware, and phishing schemes. The accelerated digitalisation in all economic sectors increased the demand for cybersecurity skills and enhanced capabilities.

As reported in the EC Communication on a Cybersecurity Skills Academy ("the Cyber Skills Academy") on 18 April 2023, "*the shortage of cybersecurity professionals in the European Union ranged between 260,000 and 500,000, while the EU's cybersecurity workforce needs were estimated at 883,000 professionals*[2]*, suggesting a misalignment between the competences available and those required by the labour market*."

CyberSecPro (CSP) aims to contribute towards this need by advancing the academic cybersecurity training supply with harmonised and practical capabilities that can address the market needs.

CSP will exploit the harmonised training modules in knowledge areas demanded by the market. Based on the training module type (course, summer school, short seminar, mini course etc.) the CSP cybersecurity training market will be segmented into knowledge areas needed by the market e.g., risk assessment training modules, penetration testing, code auditing, software security etc.

2.1.1 Exploitation Models

CSP consortium recognizes three main exploitation models for the project results:

1) The *commercial exploitation model*, which implies the paid provision of the project results to the end-users (e.g., academies, institutions, HEIs, Cybersecurity Academy, National Competence Centres, ECC, SMEs, industries) complying with a licensing scheme which will be defined in the CSP business plan;

2) The *academic exploitation model*, which implies the re-utilization of the training modules know-how acquired in future cybersecurity courses, programmes and educational provisioning;

3) The *technological exploitation model*, which implies the re-utilization of the technological know-how acquired for the usage of cybersecurity products for the provision of cybersecurity educational services built on top of them.

However, not all project partners and interested stakeholders may exploit all project results using the three models defined above.

The exploitation models of the CSP project results will be dependent on three main parameters:

- the nature and interests of the project partners and stakeholders in general;

[1] https://dataintelo.com/report/global-education-cyber-security-market/
[2] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

- the distribution model (commercial or non-commercial) of the project results;
- the distribution of the IPRs amongst the project partners.

2.1.2 Exploitation Group

Following the aforementioned parameters and analysing the nature and expertise of the CSP consortium, we may state the following regarding the exploitation interests of the *CSP exploitation groups*:

Cybersecurity tools providers: the CSP technological partners and cybersecurity technological companies are mainly interested in commercially exploiting the project results and exploit new markets in the education/awareness/training economic sector.

Training suppliers: Academic, research organizations and cybersecurity training providers are mainly interested in adopting the research exploitation model for project results that will be provided, integrating them in their research and/or teaching activities and/or setting up future research projects further promoting the project results;

Industries (in particular: maritime, health, ICT, energy) are mainly interested in adopting the project training modules derived from the CSP for upskilling their employees in cybersecurity issues in order to address future cybersecurity challenges. Only then the EU industries and the DSM will be able to develop trustworthy innovative products;

Individual Trainees: Individual persons that wish to become cybersecurity professionals, to re-skill, up-skill, change professions, come-backs, including:

- Employers and employees that wish to upskill or reskill;
- Administrators (e.g., Data base/ cloud/network/ administrators);
- Testers (e.g., penetration testers, crypto analysts, conformity assessment testers, etc.);
- CERT, CSIRT operational team members, incident handlers;
- ICT developers and integrators;
- Security Managers, Auditors (e.g., ISO27001/ ISO27005/ ISOxxx/GDPR auditors);
- Cybersecurity Insurance providers;
- Public and Private decisions makers (e.g., Presidents/Cos/Security Officers);
- Regulatory Stakeholders (e.g., cybersecurity policy makers, legislators);
- Sector specific (industry, manufacturers, financial, health, transport etc.);
- Basic Cybersecurity educators (e.g., primary/high school/ college teachers).

Policy makers: CSP aim to close the gap of the cybersecurity academic supply and market need and will highly contribute towards EU efforts in closing the cybersecurity skills gap. CSP aims to reach and inform all policy stakeholders (e.g., DGCNET, ENISA, ECC, EDA, EUROPOL, CERT-EU) that work towards this need.

2.2 Intellectual Properties (IP) and assets per partner

The exploitation plan of each partner will be based on respect of the IPRs and the terms and conditions reflected in the GA and the Consortium Agreement as for example: (i) confidentiality concerning the information disclosed by the parties during the project development; (ii) ownership of results resulting from the execution of the project; (iii) legal protection of results through patent rights; (iv) commercial utilization of results, also taking into account joint ownership of the results; (v) patents, know-how and information related to the use of knowledge, owned by one of the parties, resulting from work carried out prior to the agreement; (vi) sub-licenses of the commercial offerings to third parties within clearly defined limits; (vii) availability of the information, deliverables, results, etc., to other EU funded projects; and (viii) disclaiming rules. The IPRs of the tools used in trainings will belong to the partner provider where the syllabus will be open to all partners and interested participants.

2.2.1 Market Analysis

In the deliverable D.2.1 an extended market analysis was conducted using two instruments: state of the art and surveys. The findings of this analysis clearly identified the need for skills in different

cybersecurity Knowledge Areas including risk management, penetration testing, cybersecurity engineering, software security.

The analysis of European cybersecurity higher education programmes conducted in D.2.1 confirms that the demand for skilled professionals outpaces supply. Recommendations for improvement of cybersecurity education, included increasing investment in cybersecurity education and training, transforming higher education programmes to address market demand, and promoting collaboration between academia, industry, and government in developing cybersecurity talent. The need for a coordinated effort to bridge the practical skills gap and meet market demand for skilled cybersecurity professionals in Europe was emphasised.

In D.2.1 the most demanded knowledge areas were identified and reported. Our marketing educational choices will be based on these knowledge areas:

Table 1: Knowledge units / skills

Knowledge Units/Skills	Percent Covered in HEI (Mandatory only)	Health	Energy	Maritime	ICT	Other
Cryptography	75%-79%					
Secure Communication Protocols	65%-69%					
Network Defence	50%-54%					
Data Integrity and Authentication	45%-50%					
Network Architecture	45%-50%					
System Control	45%-50%					
Access Control	40%-45%					
System Access	40%-45%					
Risk Management	40%-45%					
Data Privacy	35%-39%					
Fundamental Principles	35%-39%					
Network Implementations	35%-39%					
Digital Forensics	30%-35%					
Cryptanalysis	30%-35%					
Design	30%-35%					
Implementation	30%-35%					
Distributed Systems Architecture	30%-35%					
Network Services	30%-35%					
Common System Architectures	30%-35%					
Security Governance and Policy	30%-35%					
Cyber Law	30%-35%					
Analysis and Testing	25%-29%					

System Thinking	25%-29%					
Information Storage Security	20%-25%					
Ethics	20%-25%					
Identity Management	20%-25%					
Social Engineering	20%-25%					
Personal Data Privacy and Security	20%-25%					
Analytical Tools	20%-25%					
Systems Administration	20%-25%					
Privacy	20%-25%					
Component Design	15%-19%					
Physical Media	15%-19%					
Hardware Architecture	15%-19%					
System Management	15%-19%					
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	15%-19%					
Awareness and understanding	15%-19%					
Usable Security and Privacy	15%-19%					
Cybersecurity Planning	15%-19%					
Business Continuity	15%-19%					
Cyber Ethics	15%-19%					
Component Reverse Engineering	10%-14%					
System Testing	10%-14%					
Social and Behavioural Privacy	10%-14%					
Security Program Management	10%-14%					
Personnel Security	10%-14%					
Security Operations	10%-14%					
Cybercrime	10%-14%					
Cyber Policy	10%-14%					
Deployment and Maintenance	5%-9%					
Documentation	5%-9%					
Component Testing	5%-9%					
Physical Interfaces and Connectors	5%-9%					
Customer Service and Technical Support	5%-9%					
Component Procurement	<5%					
System retirement	<5%					

2.3 Exploitation plans

The cybersecurity skills gap is increasing; the number of unfilled cybersecurity jobs grew by 350% in the past eight years and the (ISC)2 Cybersecurity Workforce Study for 2021 estimates that an additional 2.7 million cybersecurity professionals are needed; whereas the World Economic Forum Future of jobs report indicates that 50% of all employees will need cybersecurity reskilling by 2025. This is the opportunity of the CyberSecPro project to promote the training modules that will be developed in order to upskill, reskill the EU workforce and enhance the role of the HEIs in Digital Single Market (DSM).

CSP aims to exploit the entire CSP set of training modules or individual training modules. The target market is the cybersecurity educational and awareness market.

2.3.1 Individual exploitation plans and activities

There are two types of partners in the CSP consortium: Higher Educational Institutions (HEIs) and Cybersecurity SMEs with different visons, and exploitation needs.

The CSP HEIs will individually present their exploitation plans based on the fact that CyberSecPro (CSP) extends the mission of the HEIs to what is commonly referred to in the literature as the "third mission" which is "the generation, use, application and exploitation of knowledge with external stakeholders and society in general" [1]. HEIs exploitation plans will promote the CSP sustainable hands-on training on cybersecurity and privacy issues. HEIs exploitation efforts will aim to further contribute to upskilling the workforce and become the main enablers in the secure digital transformation in all sectors of the economy. The plans will build the HEI–Security Industry Collaboration as a means towards fulfilling the third mission and becoming an important point of attraction for people interested in the role of universities in the digital era.

By exploiting the CSP outcomes, the HEIs can be the main contributors in putting in practice the new EU strategies (e.g., new EU Cybersecurity Strategy, Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy) for helping all citizens and businesses to benefit from trustworthy and reliable digital products.

On the other hand, the CSP SMEs will exploit the CSPs outcome in order to expand their market target and build commercial opportunities in the HEI, as their new customers.

SMEs exploitation approach will be around building PPPs ensuring the sustainability and feasibility of the CSP-training modules that use their own tools. SMEs can provide to the HEIs:

- Technical support (sustainability of training infrastructures and state-of-the-art tools);
- Business and commerce, intermediation and technology-facilitating services;
- Entrepreneurial cooperation;
- Establishment of new emerging knowledge-based partnerships;
- Sharing business and research knowledge;
- Provide internal motivation for academic stakeholders to cooperate with the companies;
- Compilation of strategic, innovation driven research programs;
- Participation in joined investments, funding opportunities, dissemination and exploitation activities.

2.3.2 Collective exploitation plan and activities

The CyberSecPro (CSP) training modules can be exploited as a whole by the CSP consortium or a cluster of partners respecting the IPRs of each partner which will be reflected in the business model and pricing policy that will be adopted. The CSP collective exploitation plan will include the following issues:

1. *Market analysis and stakeholders mapping*. Research of the targeted commercial training market will include analysis of the competition, the demand, the pricing, the regulations,

and the cultural nuances. This will help to understand the market landscape and identify potential gaps and challenges.

2. *Identification of target audience*. Select the market targets and determine the target audience in the selected market(s) such as professionals in specific industries or roles, and assess their needs, preferences, and pain points. This will help to tailor CSP training program and modules and marketing messages accordingly.
3. *Localise the offering*. Adaptation requirements will be presented to the CSP training program and modules to the selected market(s), clients, the intended audience, including the language, the content, and the format. For instance, local laws and enforcement authorities (e.g., the national implementation of the NIS2 Directive or the modus operandi of data protection authorities) may be included in the tailoring of the CSP trainings;
4. *Build strategic partnerships*. Identify existing associations and consortia in line with CSP mission. Activities will be described in order to establish partnerships with organisations, such as universities, training centers, industry associations, and government agencies that are already providing similar services. Some services may be built on top of existing ones. This would allow CSP to leverage on their networks, resources, and credibility, and expand reach in the market;
5. *Marketing strategy*. A marketing strategy will be developed that focuses on CSP's unique value proposition. Research will be conducted in order to investigate the target audience through various channels, such as social media, email marketing, SEO, events, and PR.
6. *Bring value to the (local) network*. Present the activities needed to leverage the European position to show cross-border opportunities.
7. *Monitor and adjust*. Describe the activities needed to monitor CSP performance in the educational market (e.g., feedback collection from clients and other partners), and the possible adjustments that the strategy may need.

The CSP general exploitation plan will be based on the three 'C': credibility, clarity, and community. It will also provide the activities needed to enter to the new training markets e.g., media presence and directly target potential customers; collaboration with established commercial training providers to complement and enhance their offering; participation in publicly funded training initiatives for cybersecurity training.

2.4 Exploitable CyberSecPro Products

After the formation of the exploitation groups, the most important step towards developing the CSP exploitation plan is the identification of the project's key exploitable results. Several results are planned to be developed, however, three of them have been assessed as the most important exploitable assets, each of which is linked to one exploitation group. The identified exploitable results for CSP are listed in Table 2 below.

Table 2: Key CSP exploitable results and exploitation groups

Key CSP Exploitable Result	Exploitation Group
Individual training modules	Training and educational providers, industries, individual trainees
CSP studies, surveys, best practices	Policy makers
CSP training on tools for training purposes	Cybersecurity Technological partners, individual trainees, industry
CSP Bundle of training modules hosted in the CSP Dynamic Curricula Management System (DCM)	Policy makers, industries, training providers

CSP certification schema for cybersecurity training modules	Policy makers (certification stakeholders, ministries of education, National Cybersecurity Competence Centres, ENISA, ECC)

2.4.1 Syllabus of the training modules

Syllabus will be developed for the training modules accompanied with training tools with CSP assessment templates (D.2.2) for helping trainees to select.

2.4.2 Training material of CSP training modules

Training material (presentations, exercises, projects) for training modules (course seminars, summer school, hackathons) will be provided in selected Knowledge areas and topics. Training material will be adjusted also for the sectors of maritime, energy and health.

2.4.3 DSM system

The CSP dynamic syllabus system (DSM) will host the training modules of the CSP programme.

2.4.4 Schema and Certification proposal for CSP

An Analysis will be provided for various aspect for certification aspects in cybersecurity educational process. Challenges will be revealed, and proposals will be made in the certification of skills in academic educational supply. CSP will propose criteria, requirements, and a scheme for cybersecurity training services.

2.4.5 CSP recommendations and best practices

CSP will provide to policy makers and training providers recommendations and best practices for harmonising trainings in cybersecurity knowledge areas that will contribute towards closing the cybersecure skills gap and closing the chasm between academic supply and market demand.

2.5 CyberSecPro Business Planning

2.5.1 Market Analysis Methodology

According to recent research [2] most of the national authorities are involved in collaboration with foreign educational programmes that contribute to the educational quality of the country, so cooperation and support in setting national accreditation schemes, where the scheme is not present based on a common European framework, will certainly be welcomed. In order to plan how to position the CyberSecPro in the market, it is important to understand the status quo as a competitor and competitors already in the market or accepted into the CyberSecPro-related pathway, as well as possible competitors expected to enter it. Analysis should include what they offer and what sectors they target, maturity of the offer and, where possible, what the pricing strategy is. Usable information also comes in the form of any documented gaps there are in what those solutions offer. In some instances, it is possible to examine the publicly available competitor information to highlight features that those competitors consider to be either essential or meaningful for the market.

This section was completed using multiple approaches. In-depth desk-based research was performed, focusing on the novel elements of the CyberSecPro in order to examine progress and include any other new entrants that had made themselves known in the cybersecurity education domain.

Important findings came from the combination of many sources that were used to achieve a complete understanding of the market and the target audiences. The three viewpoints on insight described below will be applied by the CyberSecPro consortium:

- The Market view, which entails examining publicly accessible industry reports to identify long-term and emerging macroeconomic market trends, including projections of the market

size, market challenges, and business opportunities in the domains of cybersecurity with special focus on training tools and programs;
- The Competition view, which aims to identify potential market competitors and their product offerings with an emphasis on current and future features, market share, as well as competitive advantages and disadvantages for established players and start-ups;
- The Customers/Users view, which aims to pinpoint the primary tasks that the primary target user groups wish to accomplish and better comprehend their current pain points as well as the anticipated benefits of using the CyberSecPro approach.

Therefore, this deliverable's goal is to practice these three views and gather vital data to help the CyberSecPro consortium go in the following directions:

i. Align and fine-tune the development plan for the CyberSecPro project to the target markets' requirements and expectations;

ii. Identify the most efficient exploitation strategies for the CyberSecPro integrated solution and the main exploitable assets.

Market analysis enables CyberSecPro to determine the drivers of targeted industries and domains, the needs and expectations of targeted end-users, the general potential to enter the market, and the corresponding competing goods. To keep track of them during the project, important considerations, opportunities, influencing factors, and key actors are identified.

Market view

The purpose of the market view is to cover the scope of the project and to present the current maturity of the broader market of **cybersecurity** in order to:

- identify markets main drivers and constraints;
- identify emerging technologies and trends that may impact the markets and the targeted customers;
- fine-tune CyberSecPro offerings to potential customers;
- identify market risk and plan mitigation strategies.

Desk research was used by the project to identify the publicly available information from academic and grey literature in order to complete the aforementioned actions. Most publications included high-level insights and trends regarding the development and dynamics of each market on a global scale. Many of the industry viewpoints and current advancements were not in the public domain because of the novelty and sensitivity of this field. This demonstrates the necessity of fusing the findings of this perspective with the insight of the customers/users view.

The execution of the activities in this model spans the project lifetime, with emphasis on the final year of the project that the knowledge learnt is updated and also accommodates the latest projections of the market.

Competition view

The aim of the competitive insight's viewpoint is to evaluate the benefits and drawbacks of CyberSecPro's present and potential competitors. In order to help identify opportunities and risks, the pertinent analysis offers both an offensive and a defensive strategic perspective. Profiling combines all essential sources of competitor information into one framework to aid in successful and effective strategy planning, implementation, monitoring, and adjustment. Competitive insights, market insights, and professional opinions play a critical role in the strategic positioning of CyberSecPro in the fiercely competitive vertical markets on cloud-edge computing with sensitive data.

The objective of the competitive viewpoint is to assess the advantages and disadvantages of current and potential CyberSecPro competitors. The pertinent analysis provides a strategic perspective to help identify market opportunities and threats. It is noted that the main activities of this model occur through

desk research, in which we put emphasis on listing indicative solutions, products, services and business strategies of other initiatives that bear similarity to the CyberSecPro objectives.

Customers/Users view

With an emphasis on application areas, this viewpoint aims to incorporate the knowledge and expertise of the consortium members and industry professionals in the field of cybersecurity for a variety of business domains. These customers/users are to be represented by the use case providers who participate in the CyberSecPro project. A series of interaction sessions with the CyberSecPro use case providers and early adopters will be planned in order to build upon the desk research activities regarding the market and the competition landscape insights with the goal of creating a shared understanding among the industrial partners on the market segments that the CyberSecPro framework targets.

The various impact delivery aspects and the relative discussion topics are summarized in the following Table 3.

Table 3: Topics of discussions

Aspect	Topics of Discussions
Customer problem and pain-points	What problem does CyberSecPro solve? What are the pain points we are addressing?
	Why is the problem important?
	What is the answer we are proposing?
	Describe CyberSecPro product or service in two or three sentences. Put it in terms anybody could understand–no techno speech.
Value Proposition	Which is CyberSecPro value proposition? What is the value that CyberSecPro solution is creating?
	Why is CyberSecPro value proposition important to target audience?
Offerings Differentiation	Who are the key people with the key skills needed to do this?
	Who are our competitors?
	What do competitors offer and how does it compete against us?
	Describe how CyberSecPro products/services differ from the competitors.
Customer Identification	Which are CyberSecPro targeted markets? How large are these markets?
	Who is our target customer? Provide a fairly detailed description of the target customer (B2B and/or B2C)
	How do we communicate with our customer? How do we deliver the value proposition?
	How do we maintain the relationship with customers?
Costs & Pricing	What is a reasonable pricing model for CyberSecPro offering?
	What are the revenue streams?
	What are the main costs? Are the costs mostly fixed or variable? Do the costs change with scale?

CyberSecPro gathers information from a wide range of views thanks to the CyberSecPro consortium's multidisciplinary nature, encompassing academia, major businesses, technology vendors, and small and

medium-sized enterprises (SMEs) engaged in the development and delivery of novel solutions. The revelations that result from this method help us clarify and pinpoint CyberSecPro's competitive advantage and value offer.

2.5.2 Target Markets

Identification of solutions available as part of the status quo in the following domains:

- **Cybersecurity Market (Tools, Techniques)**
  The European cybersecurity market has witnessed remarkable growth in recent years, reflecting the increasing importance of protecting digital infrastructure and data from cyber threats. According to research and market analysis, the cybersecurity spending in Europe reached a substantial figure of €30 billion in 2020, showcasing a steady upward trend. It is expected to exceed €45 billion by 2025[3] and revenue is expected to show an annual growth rate (CAGR 2023-2028) of 9.93%, resulting in a market volume of US$63.16bn by 2028[4]. Additionally, the European Cybersecurity spending on relevant tools reached almost $47 billion in 2022[5]. The forecast five-year (2021–2026) compound annual growth rate (CAGR) is 9.4%, surpassing $66 billion in 2026. This spending includes investments in various aspects of cybersecurity, such as infrastructure, software, consulting services, and workforce training;

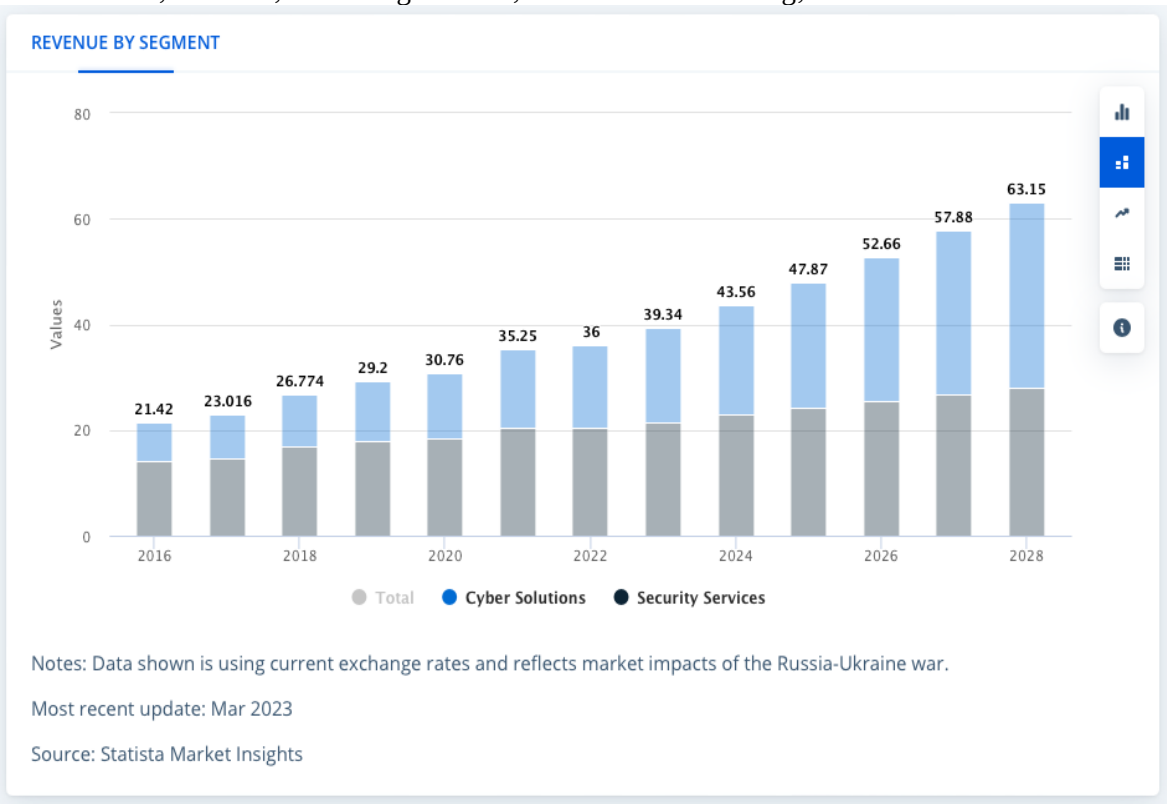

Figure 5: Data about cyber security solutions and services market

[3] https://www.orange.com/en/newsroom/news/2022/cybersecurity/cybersecurity-booming-market-europe

[4] https://www.statista.com/outlook/tmo/cybersecurity/europe

[5] https://www.idc.com/getdoc.jsp?containerId=prEUR149609822

- **Training Tools on cybersecurity**
  Alongside the market for cybersecurity solutions, the availability of training tools has also expanded significantly. The market size for cybersecurity training tools in Europe has also grown substantially. This growth reflects the growing recognition of the need for skilled cybersecurity professionals and the continuous efforts to enhance their knowledge and expertise through specialized training programs and tools. The European cybersecurity market is expected to continue its upward trajectory in the coming years, driven by the increasing digitization of businesses and the ongoing efforts to address evolving cyber threats[6]. Additionally, the European Cybersecurity spending on relevant tools will reach almost $47 billion in 2022. The forecast five-year (2021–2026) compound annual growth rate (CAGR) is 9.4%, surpassing $66 billion in 2026;
- **Training Programmes related to cybersecurity in education.**
  According to Cyberhead[7] there are 141 programmes over 26 countries across EU (Figure 6), with 76% of them being a Masters degree, ~18% a Bachelors' degree and a ~6% a Ph.D. one (Figure 7). The full list is available here[8]. Instructors will likely see higher percentage of learners focused on acquiring skills within a specific cybersecurity specialization. People who secure certain certifications typically enjoy greater job opportunities and higher salaries. Recent surveys indicate that upwards of 70 percent of cybersecurity professionals need proof of certification for their employer. Companies are also inclined to offer significant salary hikes and foot the bill for cybersecurity education and training.

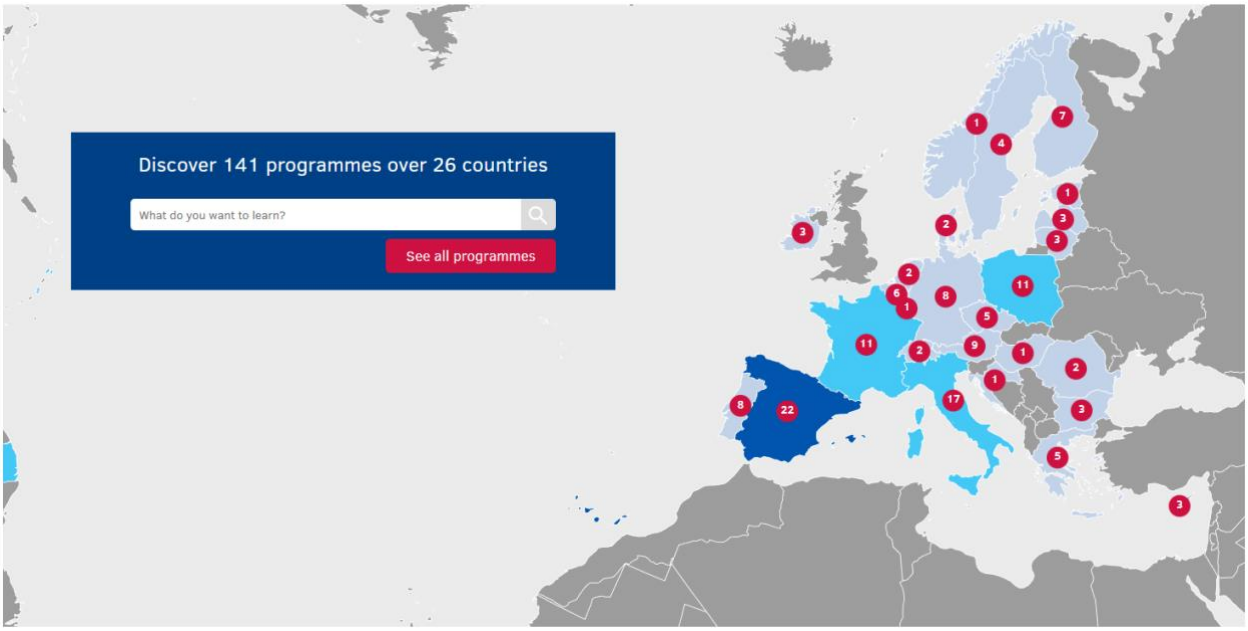

Figure 6: Distribution of the 141 cybersecurity-related courses across EU

[6] https://www.researchandmarkets.com/reports/5758517/europe-cyber-security-market-size-forecast

[7] https://www.enisa.europa.eu/topics/education/cyberhead#/

[8] https://www.enisa.europa.eu/topics/education/cyberhead#/programmes

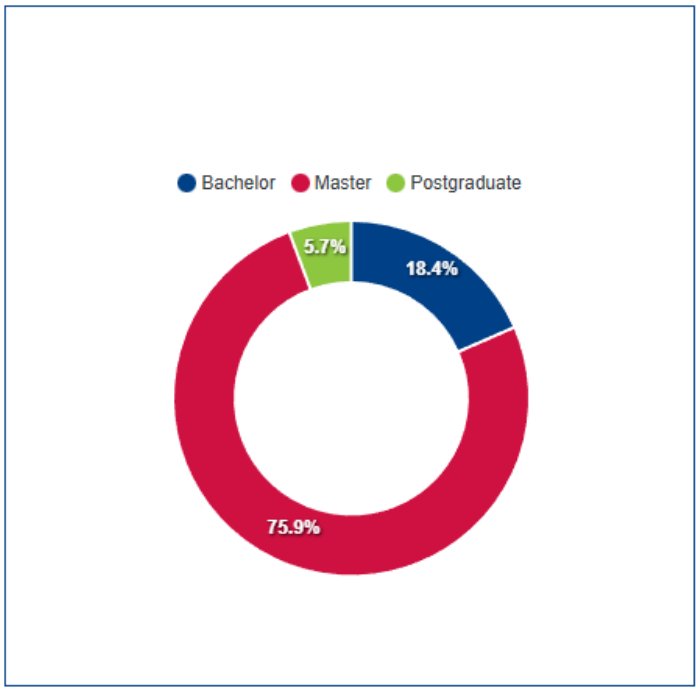

Figure 7: Characterisation of HEI available courses in cybersecurity in EU

The exploitation pathway of CyberSecPro targets a Business-to-Business (B2B) solution, targeting primarily industries. Specifically, the market segment for CyberSecPro consists of industries in the healthcare, maritime and energy domain, where the CyberSecPro sector-specific practical training material is focused;

- Healthcare Domain

Over the past two years, there has been an increase of 9.4% in the cost of healthcare breach costs, according to IBM Security's "Cost of a Data Breach Report 2022"[9]. More specifically, the average breach in healthcare increased by nearly $1 million, to reach $10.1 million in 2022, making healthcare the most expensive industry for 12 years consecutively[10]. Additionally, based on the 2018 IBM Security's report, the cost to remediate a breach in healthcare is almost three times that of other industries, making it $408 per stolen record, on average[11];

- Maritime Domain

When it comes to the maritime industry, there has been significant growth over in the digital era, opening new possibilities through the increased interconnectivity, and making it highly vulnerable to cyber incidents[12]. More precisely, it has been reported in December 2021 that over a million attacks were launched by hackers on companies globally in just the span of 4 days[13]. According to the report "Great Disconnect" (by maritime cybersecurity company CyberOwl, maritime innovation agency Thetius and law firm HFW), 44% of industry professionals reported that their organization has been the subject of a cyber-attack in the last 3 years, while 26% of seafarers are unaware of what actions are required of them during a cybersecurity incident, and 32% do not conduct any regular cybersecurity drills whatsoever[14];

- Energy Domain

According to the International Energy Agency, the energy sector accounts for around 5% of global cyber-attacks, as of 2022[15]. This is also aligned with the European Commission mandate "to increase awareness and preparedness in the energy sector" per the adoption of a sector-specific guidance in April 2019. This guidance, presented in a Recommendation and a staff working document, helps implement

[9] https://www.ibm.com/reports/data-breach

[10] https://www.linkedin.com/pulse/cyberattacks-healthcare-red-alert-conditions-remain-ben-salem-phd/

[11] https://venturebeat.com/security/ibm-report-shows-healthcare-has-a-growing-cybersecurity-gap/

[12] https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-risk-on-the-rise-in-shipping.html

[13] allianz-risk-barometer-2022-cyber-incidents.html

[14] https://safety4sea.com/report-shipowners-pay-average-of-3-1-million-as-ransoms-due-to-cyber-attacks/

[15] https://securityintelligence.com/articles/2022-industry-threat-recap-energy/

horizontal cybersecurity rules. Moreover, the clean energy for all Europeans package[16], adopted in 2019, will help transform Europe's energy systems, while also maintaining a high level of security, not least in terms of reinforcing cybersecurity of the digital transformation in the energy sector. Outside the scope of the package, the Regulation on gas security of supply ((EU) 2017/1938) also includes provisions to consider cybersecurity, as part of EU countries' national risk assessments[17].

2.5.3 Preliminary Competition Analysis

Competitor analysis was undertaken to find other products or companies, whether they are early or established, who are already solving the same problems as CyberSecPro is or are working in a similar space and may be able to easily pivot to solve the same problem. Based on our research, only three (3) frameworks are in a direct or indirect comparison with the CyberSecPro offerings.

As there is an increasing gap in cybersecurity graduates who join the cybersecurity workforce [4], some attempt on frameworks is present like the RQ Labs [5], a cybersecurity workforce skills training program which was developed using a guided emergent, co-creation design engagement between university research faculty and practicing cybersecurity professionals (see Figure 8).

Another relevant framework is the European Cybersecurity Skills Framework (ECSF), a practical tool to support the identification and articulation of tasks, competences, skills, and knowledge associated with the roles of European cybersecurity professionals[18]. According to their website: "The ECSF summarises all cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge required, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes".

The NICE Framework[19] or the Workforce Framework for Cybersecurity, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

[16] https://energy.ec.europa.eu/topics/energy-strategy/clean-energy-all-europeans-package_en

[17] https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

[18] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

[19] https://niccs.cisa.gov/workforce-development/nice-framework

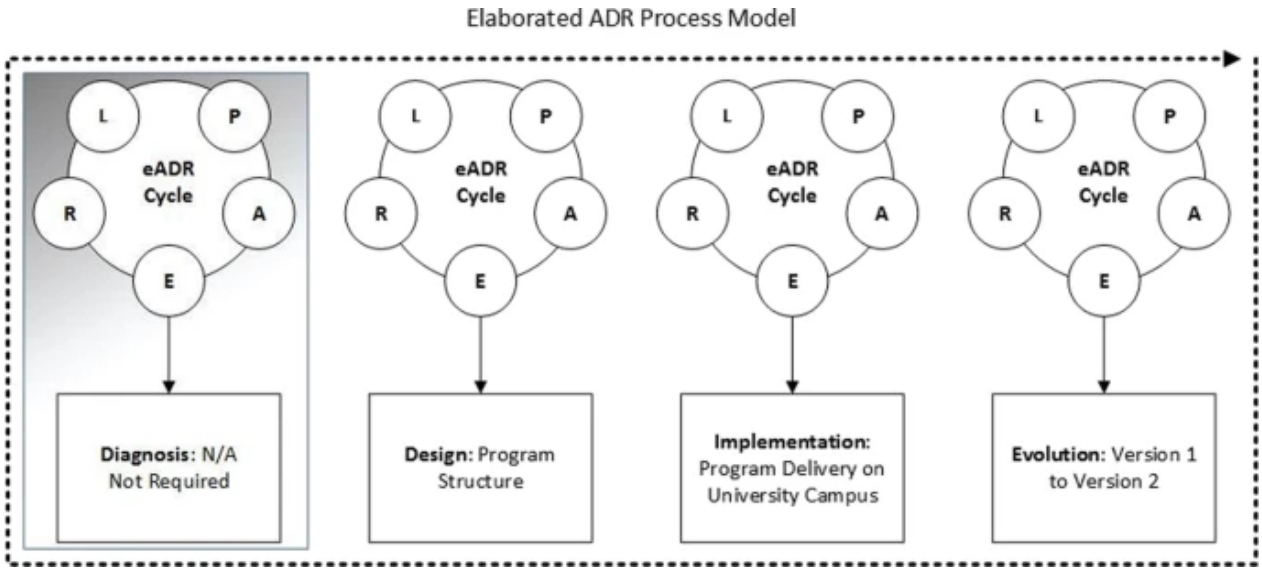

Figure 8: RQ Labs eADR process model

Table 4: List of CyberSecPro framework competitors used for market analysis

Competitor	Domain	Summary
RQ Labs	Universities and Cybersecurity Firms	Cybersecurity Workforce Training Program
European Cybersecurity Skills Framework	Cybersecurity Professionals	Provides a common understanding of the relevant roles, competencies, skills and knowledge required, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes
NICE Framework	Public, Private, and Academic	Establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed

In terms of cybersecurity training tools, there is a number of options available to the market. An indicative list is presented in Table 5.

Table 5: List of CyberSecPro training tools used for market analysis

Competitor	Cost	Features
Edapp[20]	Free	Blended training Course library Cybersecurity courses and quizzes Analytics and actionable Reports Notifications

[20] https://www.edapp.com/

Competitor	Cost	Features
ESET[21]	Free & Paid plans	Cybersecurity awareness training Phishing simulator Progress dashboards Email reminders Interactive elements
Hook Security[22]	Paid plans	Phishing simulator Feedback and progress tracker Course and video catalog Learning management system SCORM-compliant
Phised[23]	Paid plans	Automated phishing simulations Content database Measurement and tracking Scheduling
Safe Titan[24]	Paid plans	Behavior-driven training Automated simulated phishing attacks Content library Integrations Built-in protection from cyberattacks
Proofpoint[25]	Paid plans	Holistic approach and frameworks Phishing and USB simulations Knowledge assessments Reports Email security solution
KnowBe4[26]	Paid Plans	Simulated phishing attacks Content library and translated training content Mobile-friendly AI-recommended training Automated enrollment
InfoSec[27]	Paid Plans	On-demand courses Live boot camps Realistic training scenarios API integration

[21] https://www.eset.com/us/

[22] https://www.hooksecurity.co/

[23] https://phished.io/

[24] https://www.titanhq.com/safetitan/

[25] https://www.proofpoint.com/us

[26] https://www.knowbe4.com/

[27] https://www.infosecinstitute.com/

Competitor	Cost	Features
IRONSCALES[28]	Paid Plans	Integrated training and phishing simulations Video training User management Analytics and reports
Cofence[29]	Paid Plans	Phishing simulator Crowdsourced intelligence and machine learning

2.5.4 Value proposition

In this section we aim to illustrate the worth of the investment for the market system of using CyberSecPro:

Costs associated with lack of cybersecurity know-how

High costs are the result from a lack of cybersecurity know-how and skills. According to IBM Security's report, the global average cost of a data breach is $4.35 million. Compared to 2020, the average cost has increased by 12.7%. IBM additionally found that 83% of all companies will soon experience a data breach in the coming years, which means that institutions and companies of all sizes are at risk. Furthermore, in 2022, a record 83% of enterprises reported more than one breach, while the average time to identify a breach is 277 days[30].

Benefits of CyberSecPro

One of the main benefits of CyberSecPro is that the program will bridge the gap between academia and industry, by complementing and supporting current academic programs and turn the theoretical knowledge gained in the academic settings into practical skills more applicable in the various industries. Since the program's emphasis is primarily placed on practical training and is linked to innovation, it is ensured that participants will gain relevant and up-to-date cybersecurity skills, that will in turn make them more employable and open up their career prospects. By promoting cybersecurity awareness and best practices through continuous professional development, the program can contribute to creating a cybersecurity-conscious culture within organizations. Finally, through this program, collaboration and networking is also encouraged between academia, research, and SMEs, allowing professionals from various sectors to exchange knowledge and build relationships between them.

2.5.5 SWOT Analysis

This section provides a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, listing the internal strengths and weaknesses of the CyberSecPro solution as well as the opportunities and threats faced by CyberSecPro due to changes in the external environment. SWOT Analysis is a strategic planning tool for evaluating the above factors for a project or a business venture. This process allows CyberSecPro to identify internal and external factors that are favourable and unfavourable to achieve its objectives. More specifically, it provides the opportunity to:

- Evaluate the strengths of its situation;
- Define the weaknesses, which the consortium will try to minimize later on;
- Recognize the possible opportunities to be taken into account and can boost the exploitation potentials of CyberSecPro offerings;

[28] https://ironscales.com/anti-phishing-software-platform/

[29] https://cofense.com/

[30] https://venturebeat.com/security/ibm-report-shows-healthcare-has-a-growing-cybersecurity-gap/

- Recognize the possible threats and treat them in a planned and organized way.

The following SWOT analysis diagram was derived from the results of the previous sections regarding the market insights and competitors' landscape, supplemented by our vision of project's outcomes and the clear understanding of market potentials recognizing the strength and weaknesses of the consortium, as well as the opportunities and the threats of CyberSecPro initiative.

As with many means of analysing a start-up company, the SWOT analysis[31] should be kept up to date. The aim is to be able to prioritise the strengths, weaknesses and opportunities and threats. Where factors can be made more specific with added facts, probabilities of occurrence, and by being written to be action oriented, this should be done.

With the addition of the competitor knowledge benchmarking can be introduced. This allows articulation of the factors that are the strengths or weaknesses in comparison to the competitors.

Table 6: SWOT analysis

Strengths	**Weaknesses**
• Strong Consortium Partners' Presence in Cybersecurity Domain. • Higher levels of expertise. • Proven experience in online and offline course training and consultation by HEIs and Cybersecurity SMEs. • Different modules covering different aspects of cybersecurity. • Access to cutting-edge cybersecurity tools.	• Need for significant use of resources. • Adaptability of CyberSecPro to rapidly evolving trends in cybersecurity landscape.
Opportunities	**Threats**
• Creation of formal training program to upgrade and ensure technological controls and improve the competency of cybersecurity workforce. • Increasing demand for cybersecurity due to the increased risk that comes with the rapid technological advances. • Partnering with industry leaders and the EU or government agencies, can provide access to additional resources.	• Competitive landscape, many different cybersecurity tools offering similar services. • Compliance and regulatory requirements vary from sector to sector.

2.5.6 Preliminary Business modeling

The business model of CyberSecPro is considered to be a multi-sided one, meaning that there is more than one type of customer that may have an interest in the solution. A preliminary business plan will be drafted by the end of the project for identifying the market size, the potential revenues and the costs in the medium term, but the consortium has already prepared a business model canvas at the project level, which is a strategic framework depicting key elements in the CyberSecPro value proposition, infrastructure, customers and finances (cost structures and revenue streams) in order to achieve the expected impact on the long term.

[31] https://www.mindtools.com/amtbj63/swot-analysis

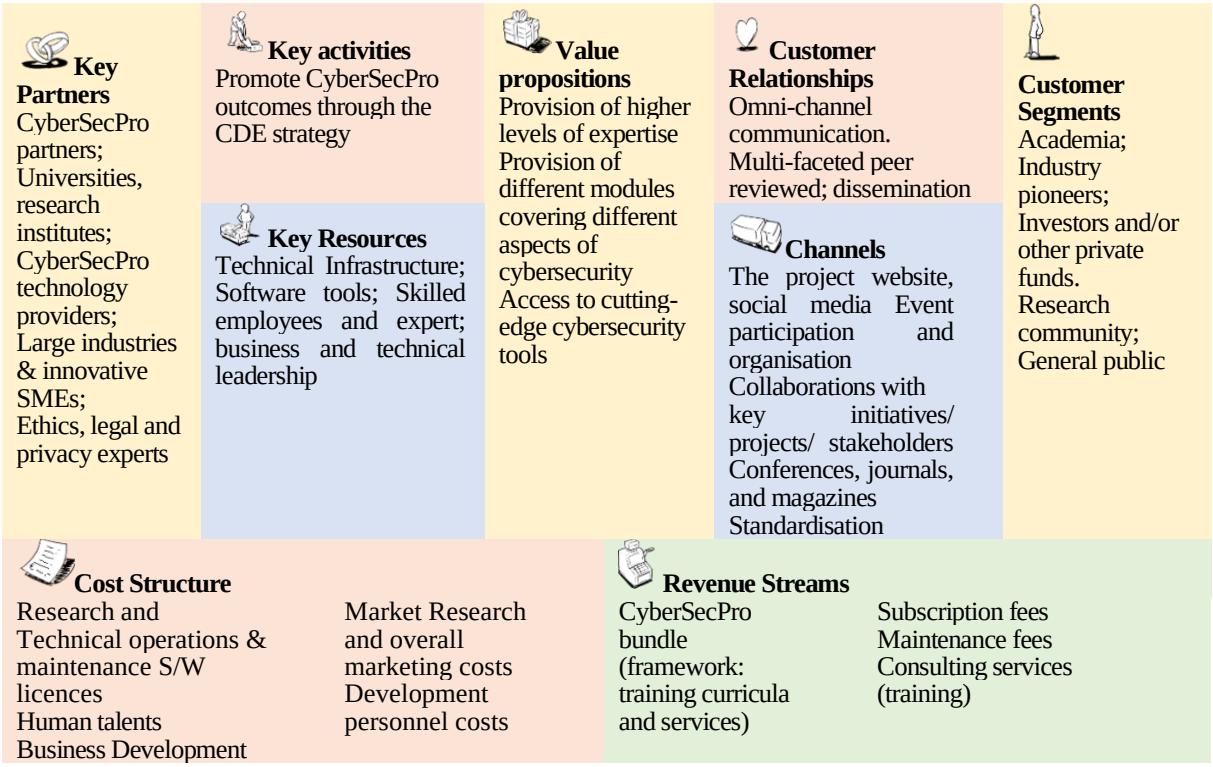

Figure 9: Business canvas

2.5.7 Individual exploitation plans

Alongside the overall project's exploitation plan, each consortium partner has their own customized exploitation plan, which serves as a valuable supplement to the project's plan. This section provides a summary of the exploitation strategy for each partner. It is important to emphasize that project partners should regularly update their plans to align with the latest consensus on exploitation at the project level and incorporate any changes in their individual exploitation strategies and methods at the partner level.

GUF

In the context of CyberSecPro, GUF is interested in exploiting the educational and training material and experiences for its teaching of cybersecurity in its business informatics, business, informatics, economics, and business didactics master programmes, doctoral studies, bachelor courses and as appropriate other educational activities it performs. A special focus is on integrating cybersecurity education and training into mainstream business informatics courses both for general, business, informatics, economics, and business didactic programmes as well as for specific activities.

IMT

Exploitation of CyberSecPro results will happen within our activities related to cybersecurity education. As a public institution, we deliver not-for-profit cybersecurity programmes at the M2 level, both in the engineering curriculum and in the research master of Institut Polytechnique de Paris. We may leverage the activities of CyberSecPro in the design of new courses or updates to existing courses. We also run, and are currently expanding, for-profit education programmes on cybersecurity, and may leverage the activities of CyberSecPro in the design of these new programs. Finally, Institut Mines-Télécom is operating the "Train Cyber Experts" project within the framework of France2030. This project aims at developing new content for cybersecurity courses. Communication channels will be opened between projects to mutually inform on activities.

LAUREA

LAUREA plans to focus on following key exploitation domains with CyberSecPro development, results and deliverables:

- Leveraging benefits of the CyberSecPro education and training materials, development work and deliverables into Laurea's education and training programmes;
- Creating partnerships with the European and allied partners and communities that can help LAUREA and CyberSecPro scale up;
- Publishing whitepapers, case studies, research papers, news items and other materials that showcase the benefits of the CyberSecPro tasks outcomes and deliverables;
- Organizing, participating and partnering events such as conferences, webinars, and workshops to educate potential target group and partners about CyberSecPro deliverables, services and solutions;
- Building partnership and participating communities of the creative people, researchers, and experts to share knowledge and best practices;
- Explore various possibilities to gain new know-how and LAUREA gain the skills and knowledge needed to improve the operations;
- Creating a strong online presence, including CSPro social media and a website, to help LAUREA, partners and EU innovation to reach a wider audience and engage with potential customers and partners.

TUC

TUC has adopted an evolving strategy towards promoting the commercial exploitation of R&D results by providing services, licensing specific products to industrial partners, contracting with industrial partners to jointly develop new products, and participating in start-up / spin-off companies and joint ventures. In the research/academic domain, TUC has a tight integration with Telecommunication Systems Institute (TSI) and in collaboration with the said institution, it will develop new courses (and enhance existing ones) within the existing undergraduate and graduate programs related with the CyberSecPro results. Additionally, TUC expects that it will be able to enhance the master and PhD with the trainings and in the topics related to the CyberSecPro project. TUC in collaboration with the TSI have the capacity to organise talks, technical presentations and seminars on the topics of CyberSecPro project. Additionally, the best practices, trainings and know-how developed within the project in order to either enhance and update existing undergraduate and postgraduate courses. In a planned revision of the academic curriculum, TUC aims to propose the introduction of new courses specifically targeting the security topics. Last but not least, several theses (at the master and PhD level) will be formulated so that a strong research team on cybersecurity can be formed in order to support the activities of future projects.

TUBS

TUBS is committed to maximizing the exploitation of the outcomes and knowledge gained from the CyberSecPro project. TUBS aims to leverage the project's results in several ways, primarily through integration into its curricula and research activities. This includes the incorporation of the project's findings into relevant academic courses, ensuring that the next generation of cybersecurity professionals' benefits from the project's state-of-the-art research and training programs.

TUBS will also exploit the project's outcomes to strengthen its position as a leading institution in cybersecurity. It will use the project's results to enhance its research capabilities, form new collaborations, and attract more funding for further research and innovation in cybersecurity.

As a participant in the project, TUBS will actively participate in the CyberSecPro training program, providing students and staff with new opportunities for learning and development. Furthermore, TUBS plans to exploit the project's outcomes to strengthen its ties with industry partners, enhance its services to businesses, and contribute to societal advancement in cybersecurity. Lastly, TUBS will seek to

publish findings from the project in top-tier journals, furthering the reach and impact of the project's results.

UCY

UCY considers exploiting the results of the project in educational and training activities related to established university courses and other potential trainings organised in the form of workshops and summer schools.

UMA

In the context of CyberSecPro, UMA is interested in taking advantage of the material produced and the experience gained to improve the teaching of cybersecurity in its different educational programs. Specifically, UMA is interested in adapting the training tools and practical exercises proposed throughout the project to adapt them in at least one or two advanced courses of its new BSc. Degree in "Cybersecurity and Artificial Intelligence", where a greater specialization and practical approach is expected. Therefore, UMA will pay special attention to the integration of materials developed in the project, reviewing or putting into practice those tools and methodologies learned, and adapting (as much as possible) those activities or exercises that have a more practical and useful approach for future cybersecurity experts.

CNR

In the ambit of CyberSecPro, CNR is interested in exploiting the training material for the cybersecurity masters, PhD schools and other training activities it performs. CNR in particular, runs a master degree in cybersecurity with the University of Pisa and several summer and winter schools. CNR also runs the cybersecurityosservatorio.it that holds several cybersecurity services and training could be one of this.

COFAC

COFAC will maintain an online presence, issuing policy briefs, engaging with industry partners, and establishing media relations, promoting a continuous evaluation to optimal impact. COFAC will include results of CyberSecPro project results into Summer Schools, Advanced Courses, e.g., BSc., MSc. Professional MSc. and Doctoral degrees in Computer Sciences, Business Management, Communication and Cybersecurity, available in the multiple HEI within the group and create and set available new national and international educational offer.

SINTEF

SINTEF's company vision is "technology for a better society", and it is an important aspect of its societal role to contribute to the improvement of cybersecurity skills of technology providers and security of everyone's life. SINTEF acts as an incubator, commercialising technologies through the establishment of new companies. SINTEF also collaborates closely with educational institutions to educate students with skills according to industry needs. Its exploitation strategy is to utilize CyberSecPro to:

1) Improve its cybersecurity research lab: SINTEF's dedicated research lab focuses on applying cutting-edge cybersecurity skills and technologies;

2) Offer cybersecurity training programs and tools: SINTEF could further develop and offer new cybersecurity training programs to both students and professionals;

3) Partner with industry leaders: The institute could partner with leading cybersecurity firms to gain insights into industry trends and best practices. This could help the institute stay on the cutting edge of cybersecurity research and develop skills that are in high demand;

4) Support our ongoing cybersecurity research: SINTEF is conducting research in areas such as machine learning, artificial intelligence, and blockchain, with a focus on developing new cybersecurity solutions. Staying up-to-date is important to attract funding from government agencies and industry partners;

5) Host cybersecurity events: SINTEF could host cybersecurity events such as hackathons and cybersecurity conferences. These events could bring together cybersecurity professionals, students, and researchers from around the world, helping to build the institute's reputation as a leading cybersecurity research centre;

6) Collaborate with other academic institutions: SINTEF plans to collaborate with other educational and research institutions to share knowledge and resources. This could help to accelerate the development of cybersecurity skills and technologies, benefiting both the institute and the wider cybersecurity community;

7) Improve the cybersecurity of critical domains: SINTEF aims to expand the research results of CyberSecPro to the key domains where security is a cornerstone of the digitalisation effort, such as critical infrastructures. Here, there is an increasing demand for competence and educational programmes for cybersecurity.

UNINOVA

UNINOVA will exploit the results of the project through the organisation of seminars and summer schools on Cybersecurity, mainly focused on companies' executives, aiming to invite national and international experts to conduct these events. UNINOVA will also exploit the results of the DCM solution, by reusing it in future projects and trying to capitalise on the development results of the solution so as to analyse the feasibility of creating a spin-off company from these results.

UPRC

UPRC already offers 2 cybersecurity Masters programs and courses in various areas. UPRC will enhance the practical aspects of these courses. UPRC aims to attract more students from the market. UPRC also participates into the Erasmus+ program, and it aims at harmonising the syllabus so the students will widen their mobility options.

APIRO

APIRO is interested in exploiting the experience, methods, practices and tools developed as part of the CyberSecPro project in its relevant training service offerings. Moreover, since APIRO also offers audit services and is closely connected to the certification industry, aims to further exploit the experience, methods, practices and tools developed as part of the CyberSecPro project on certification of cybersecurity skills.

C2B

Few audiences have been identified as:

- The European Coastguards Functional Forum (ECGFF);
- The Northern Atlantic Coast Guards Forum (NACGF) A first presentation of the project has been provided in February 2022. Future presentations will be provided to theses audiences but C2B foresees also to conduct - presentation of risks and mitigations - development of a training platform, a program and on hands training on a dedicated AIS platform - inclusion of Cybersecurity education and training within the Border guards SQF - Assessment of the previous achievements and presentation to maritime agencies (EMSA, FRONTEX, EFCA,...).

FP

Focal Point recognizes the potential of the expected project’s results and the value they will offer to its own training services, as FP seeks to provide the most comprehensive and effective cybersecurity training to its target groups. In order to fully leverage the outcomes of the project, FP plans to offer a series of enriching seminars and trainings on Cybersecurity, which will be tailored primarily towards executives in various industries, with a focus on providing invaluable insights and knowledge relevant to today's ever-changing technology climate.

ITML

ITML aims to exploit the outcomes of CyberSecPro project to enhance its market position with respect to cybersecurity approaches and solutions with an emphasis on training activities. To that end, ITML envisions to demonstrate and further advance the functionalities of Security Infusion (proprietary technology of ITML) which stands as an end-to-end cybersecurity framework (from the edge to the cloud) and bring it closer to the market through the end-user driven experiments executed within CyberSecPro.
The topics or domains of interest regarding the technological offering as a cybersecurity training tool are real-time security monitoring and alerting, vulnerability identification, and cybersecurity awareness. The activities and the overall approach of ITML for the individual exploitation plan is based on the continuous and active engagement with other research and technology providers, other cybersecurity companies, Higher Education Institutions, Research Institutes, and Universities.

MAG

MAG aims to strengthen its activities in the cybersecurity educational market. Specifically, it intends to exploit the CSP training opportunities serving the needs of internal employees (of the MAGGIOLI group) and the needs of its customer employees, mainly public servants.

SGI

SGI would initially focus on local universities to get PMF. SGI has already identified an initial list including relevant contacts, and will after the event 26th Sept. 2023 start to reach out to explore its potential. Furthermore, SGI is discussing with two non-profit member organisations to see whether we can create an offer more directly to SMEs.

SLC

As a cybersecurity related solution provider, SLC supports CyberSecPro with the development of professional cybersecurity practical training program. SLC aims to tackle the challenges identified by the CyberSecPro relating to lack of quality education and development of skill human resource tailoring Knowledge Areas (KA) in demand including Risk assessment and management, vulnerability assessment, threat intelligence and incident response, and Privacy-by-design. In this context, SLC will develop advanced and state of the art training materials in the above mentioned KAs targeting professional and HEI institutions. Initially, as a part of exploitation approach, SLC will develop training materials and offer training to the targeted audience. Later on, SLC plans to publish papers relating to the lesson learn from the cybersecurity training and adoption of new solutions to different venues such as IEEE S&P, USENIX Security, ACM CCS, ACM SIGCOMM, IEEE INFOCOM, USENIX NSDI.

Trustilio

Trustilio will utilise the expertise gained in the CSP in order to enhance the commercial and personalised training offers. It will exploit and communicate the outcomes to various standardisation and policy events and activities that participates. CSP will help the company to gain new grounds in the consulting and education market.

ZELUS

Exploitation of the results is a crucial aspect of ZELUS's involvement in the CyberSecPro project. The main objective is to ensure that the project outcomes and outputs - particularly the innovative SmartViz toolkit, yield tangible benefits and offer a valuable contribution to both the cybersecurity landscape and ZELUS's own business operations. To begin with, ZELUS plans to integrate the findings and improvements derived from the CyberSecPro project into its existing and future product offerings. The SmartViz toolkit will be further developed and refined based on its application within the project, ensuring that it remains at the cutting edge of data visualization for cybersecurity. Furthermore, ZELUS will leverage the project's outcomes to strengthen its market positioning, using the demonstrated capabilities and results to attract new customers, foster partnerships, and enter new market segments.

This includes promoting the SmartViz toolkit as a proven solution for cybersecurity analysis and threat hunting, backed by its successful application within the CyberSecPro project. Moreover, ZELUS intends to exploit the training and skill development components of the CyberSecPro project to enhance the competencies of its own staff. This not only supports personal development but also ensures that the company remains equipped with the most recent cybersecurity knowledge and skills. This will enable ZELUS to continue offering top-class, secure solutions to its customers, underscoring its dedication to innovation and cybersecurity.

UNSPMF

UNSPMF plans to exploit the CyberSecPro results in several ways. UNSPMF hosts a data science master program that is unique in the region; we plan to open novel courses within the program related with the CyberSecPro results. Based on the results achieved during the project, UNSPMF expects to open master and/or PhD theses with tentative topics on advancing distributed and parallel optimization and ML algorithms for threat detection.

ACEEU

ACEEU as an international quality assurance provider with a focus on increasing university engagement with business and society as well as entrepreneurship is not specialised in the field of cybersecurity, but rather supports the project from a horizontal perspective of ensuring that the developed training materials are in line with market needs and that the demand can be addressed by the CSP results being sustained and exploited after the project ends. Thus, ACEEU itself is interested in exploiting the tools and methods that will be developed and used in the project to ensure the market-oriented training development. Supporting universities and other organisations in similar challenges, ACEEU is interested in sharing the learnings and tools across Europe with the ultimate goal being to support (higher education) institutions in becoming more relevant for business and society as a whole.

3 Conclusion

This deliverable describes the dissemination, communication and exploitation plan of the CyberSecPro project, which will mainly cover dissemination, communication, and exploitation approaches. The plan defines an integrated approach that strategically targets the activities of dissemination, communication, exploitation, and it is fully embedded in the project's work plan, to enlarge the impacts of the project in the training and education activities for cybersecurity.

Within this deliverable, Section 1 defines the dissemination and communication objectives and approaches and analyses the available channels to reach CyberSecPro stakeholders for achieving maximum impacts. Then, Section 2 contains a preliminary analysis of business models, and it also analyses the business environment, the value proposition of the project results, and the initial foreseen options and scenarios for sustainability. Besides, it includes the IRP management.

In conclusion, this document serves as guidance for all the dissemination, communication, and exploitation activities of consortium members, to promote the project and foster wider communication and deeper impact. The plans will be regularly updated to reflect the latest development of CyberSecPro's methodology for dissemination, communication, and exploitation.

References

[1] G. Secundo, S. E. Perez, Ž. Martinaitis, K. H. Leitner, "An Intellectual Capital framework to measure universities' third mission activities", *Technological Forecasting and Social Change*, Volume 123, 2017, Pages 229-239, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2016.12.013.

[2] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?," *Educ Inf Technol*, vol. 27, no. 3, pp. 3011-3036, Apr. 2022, doi: 10.1007/s10639-021-10704-y.

[3] B. J. Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training," *Technology in Society*, vol. 67, p. 101769, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.

[4] C. Catal, A. Ozcan, E. Donmez, and A. Kasif, "Analysis of cyber security knowledge gaps based on cyber security body of knowledge," *Educ Inf Technol*, vol. 28, no. 2, pp. 1809–1831, Feb. 2023, doi: 10.1007/s10639-022-11261-8.

[5] C. Daniel, M. Mullarkey, and M. Agrawal, "RQ Labs: A Cybersecurity Workforce Skills Development Framework," *Inf Syst Front*, vol. 25, no. 2, pp. 431–450, Apr. 2023, doi: 10.1007/s10796-022-10332-y.

Annex A: Planned KPIs

Expected outcomes and KPIs from proposal and DoA.

CyberSecPro Impact Areas	Impact Pathway	Type of indicator (impact)	CybeHot DeliveryContribution and KPIs to monitor Impact
Innovation	Design and Implement training modules and simulated test beds	Short-term	Innovative, training modules (cyber ranges, cyber exercises, decathlons, summer schools, sector-specific seminars) will be the necessary bundle that will provide hands-on training on cybersecurity, accountability and liability, issues necessary for a trusted digital market and industry. **KPIs: 530 trainees will be trained and mentored**
Business enhancement	Upscaling security start-ups and SMEs	Short-term	CyberSecPro partners offer cutting-edge security technologies and consultancy services. The partnership of these companies with the HEIs in the consortium will enhance their business since they will always be informed on the research paths related to trustworthiness in the digital world, utilizing the experience of the professors. Furthermore, the CyberSecPro trainees (students, researchers) will be armed with the necessary knowledge to help the companies to enhance their existing products and innovate further. **KPIs: 5 enhanced /new cybersecurity related business models**
Education enhancement/ Development of cyber work-force	Close the cybersecurity skills gap	Mid-term	The sustainable, collaborative training model proposed by CyberSecPro will decrease the cybersecurity skills gap, enhancing the scale and scope of student engagement activities. Prepare the students to join the workforce of the competitive Digital Single Market (DSM); Provide cybersecurity competencies (skills, knowledge, values) needed by the EU industrial

			sector in response to an ever-changing world; Enhance the students soft skills needed in the competitive digital markets; Adopt inclusive, non-bias and gender-balanced pedagogical methods to raise the students **KPI: 60 Cybersecurity trainees joined the cybersecurity workforce.**
High Education and Research Institutions Advancement	Improve the infrastructures/operations/ and services to support the training needs of the digital transformation	Mid/ Long-Term	CyberSecPro upscales the HEI to serve the needs of the digital transformation by: developing state of the art digital laboratories, testbeds, platforms, inter- and multi- disciplinary support structures, testbeds to foster innovation; by improving organizational units to develop collaborations for technology transfer by establishing new collaborations and enhancing the nature, content and types of collaborations with external partners, including businesses, industries, SMEs. Embedding entrepreneurship deeply into the educational system will offer the opportunity to work together on sharing practical research contributing to real-life needs. Harmonization of cybersecurity programs/ courses using ECTS will be feasible. **KPIs: a minimum of 80 academic members will be trained in new technological tools. More than 10 physical and virtual training labs will be enhanced/ established with state-of -the art technological training tools. More than 50 applied research papers will be published.**
SMEs scale-up	Boost the innovation efforts of the SMEs	Mid-term	The research culture of the HEI will enhance the innovation efforts of the SMEs. The collaboration proposed by CyberSecPro with the HEIs will easily transform innovation-driven research to innovative products. The SMEs will benefit by offering internships to attract talented CyberSecPro

			graduates. **KPIs: 8 start-ups/scale-ups will be supported**
Economic/Business	Support of SMEs/Start-ups and scale-ups	Mid-term	The SMEs/start-ups that participate in the CyberSecPro will be further exposed to the research ecosystem and capable workforce. **KPI: At least 4 SMEs improved their revenues, at least 10 trainees joined the SMEs.**
Developing innovation ecosystems	Active partners /Collaborators	Short-term	CyberSecPro will build synergies with various industries, organisations, governments, SMEs to ensure the sustainability of the training modules in terms of infrastructures, trainers, and trainees. KPIs: At least 30 organizations from various industries and digital ecosystems have signed agreements with CyberSecPro HEIs to be involved in the practical training process (either as trainers or trainees). **KPIs: At least 10 PPP agreements have been signed.**
	Sustainable partnerships	Mid-term	Consortium Agreement, contracts / long-term partnership agreements between the CyberSecPro partners will be signed in order to ensure the sustainability of the practical trainings and collaboration. **KPIs: 10 organisations will participate in sustainable and institutionalized partnerships.**
	Financial Sustainability	Mid-term	CyberSecPro will develop a sustainable business model and pricing policy of the trainings exploring all different options (e.g., leveraging investments, fees, sponsorships, scholarships, donations, national and EU funding, commercial agreements). **KPIs: More than 80 registrations have been waived**
Policy Impact	Addressing EU policy	Mid-term	CyberSecPro directly contributes to the EU industrial policy since it reskills and develops a capable cyber workforce. CyberSecPro also supports the implementation of the EU security Union strategy and the

			Digital Single Market strategy since all aspects of security will be covered. Addressing the shortage of specialists in cybersecurity, Europe will stay in the lead in the areas where it is currently strong (networking, 5G, IoT), will play a leadership role in the AI revolution and will establish broad trust in digital ecosystems. **KPIs: At least 10 training topics related to the implementation / practicing of cybersecurity policies.**
Marketing Impact	Upskilling cybersecurity marketing capabilities	Long-term	By strengthening human capital in cybersecurity practices, innovative and entrepreneurial skills both at individual and organizational levels and fostering the creation and diffusion of practical cybersecurity knowledge and innovation openly within industries and society. **KPIs: All EU industries/SMEs are compliant with the cybersecurity strategy**
Addressing EU policy priorities through R&I	Bring deep tech digital R&D results to the market in areas strategic for Europe	Mid/Long-term	CyberSecPro sustainable, continuously updated practical training will help workforce to become skillful in addressing cybersecurity challenges and in return the EU Digital Single Market (DSM) and industries will produce innovative, competitive trustworthy products and services serving the EU citizens values. The innovation of the new EU products (e.g., AI/Iot/HP/Cloud-based products, data platforms and digital services) will be based on their security and privacy. **KPIs: Most EU ICT products are certified (full implementation of the Cybersecurity Act directive)**
	Increased digital talent development in Europe	Long-term	CyberSecPro enhances the EITs to dynamic training enablers in addressing the emerging cyber challenges, industrial, DSM, societal and entrepreneurs' needs. CyberSecPro is upskilling the existing and developing the new digital workforce, creating digital talents that will design the

			innovative EU products. **KPIs: There is not cybersecurity skills gap in EU**
	Increased digital upskilling of European professors	Mid-term	The collaboration of the HEIs with the security SMEs will enhance the European professionals to build the practical competencies needed to keep the pace of fast- paced digital technology development. The SMEs will provide real life problems and cybersecurity challenges to use in the training process as well as the experience gained from their clients so the professors will gear their research in contributing towards industrial and entrepreneurial innovations. **KPIs: 70% of the EU academic programs offer practical cybersecurity, knowledge, capabilities, and skills.**
	Increased gender equality in digital Education in Europe	Mid/Long-term	CyberSecPro adopts an inclusive, non-discriminating approach where all people (independently of gender, economic and physical status) can participate by attracting additional financial support (e.g., scholarships, internships), use digital tools/interfaces where people with disabilities can use, training non-bias material will be carefully built. **KPIs: more than 150 trainees are women and no-binary.**
	More learners benefitting from educational content	Long-term	CyberSecPro proposes a program blending at least 28 new training modules to increase the number and type of trainers. The ECTS grading scale that will be used to embrace the modules into existing programs will enable mobility among EU training institutions. **KPIs: The total trainees will be: 30% students, 10% academic personnel, 3% employers, 17% employees, 10% practitioners, 20% developers, 10% officers from at least 5 Member States.**

	Supporting European regulation and digital standards	Mid/Long-term	CyberSecPro hands on training program consists of practical exercises in the understanding and practicing the compliance of EU legislation related to digital trust (e.g., GDPR, NIS, NIS II, Cybersecurity Act, Liability Act, Chips Act), proposal and initiatives (e.g., EU Artificial Intelligence proposal, ENISA recommendations and guidelines for the security of SMEs and EU industries). **KPIs: 530 trainees will learn how to implement EU cybersecurity standards, policy, and regulator principles.**
Sector Specific Impacts	Maritime, health and energy market and Industries will upscale their cybersecurity practices	Long-term	CyberSecPro will collaborate with stakeholders from these critical economic sectors to ensure that the training material used includes real-life security challenges and practical training in how to implement cybersecurity policies and regulations in their business. **KPIs: All critical infrastructures in these sectors are NIS and GDPR compliant. All products are certified and embed the security and privacy by design principles**

Dissemination and communication of the project and its results

The CyberSecPro consortium has conceived a unifying strategy for communication, dissemination, exploitation and business growth (CDEB), considering and trying to maximise the potential of cross-fertilisation between these activities, fostering the combined effects of general communication, dissemination of specific peers'-driven messages, exploitation of new knowledge and ultimately diversification and business expansion through advanced (multi-access, multi-level, multi-disciplinary) training services addressing the cybersecurity needs of the whole spectrum of industries, SMEs and governments in all business sectors (business growth).

The strategy is structured based on the following steps:

1. Set the objectives;
2. Identify the target groups;
3. Engage channels;
4. Set communication roles and responsibilities within the consortium;
5. Monitor impacts;
6. Link to the external EU agenda;
7. Define market penetration/development strategy.

CDEB objectives, planned measures and KPIs to monitor CDEB impact delivery

One of the project's cross-cutting objectives is to develop a central reference point around the project and sustain it throughout its duration and beyond. Our CDEB plan has four objectives, each of which requires accompanying communication measures and KPIs to monitor success, as detailed below:

CDEB Objective 1 | Raise national and international awareness of the project and its objectives and the ways in which to participate in CyberSecPro hands-on training activities. Drive demand among individual trainees and world class trainers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators

- **Measure 1.1**: A CyberSecPro observatory will be set up to monitor the effectives of the communication strategy implemented using the following dissemination instruments: newsletters, websites / social media of the partners/external stakeholders/ participating industries, educational for a/promotions, industrial exhibitions
    - **KPIs**: >20 website visitors monthly or 720 totally during the project lifetime; >1000 site access times annually or3000 totally during the project lifetime; >10 push announcements and >5 new followers in Twitter/LinkedIn monthly or 180 totally during the project lifetime; >20 re-tweets and >30 LinkedIn profile views monthly or 1080 totally during the project lifetime;
    - **Target group**: students, professors, researchers, security officers, administrators, developers, integrators, auditors, stakeholders from the education/maritime/health/energy ecosystem.
- **Measure 1.2**: A regular e-newsletter will be sent to ensure that core information on project progress, achievements and next steps are shared. The newsletter will seek to strengthen networking and loyalty of interested stakeholders.
    - **KPI**: >8 e-newsletters with technical activities by the end of the project;
    - **Targeted group**: Actors from the maritime/health/energy/education sectors (European and non-European), students, researchers and academics and the participants in the digital ecosystems all being part of the CyberSecPro partners' network.
- **Measure 1.3**: A communications starter pack will be produced early on M2 for partners to ensure consistency in developing a project brand. This will also include a preliminary list of external events at which partners are representing the project.
    - **KPIs**: A full guide about CDEB strategy, measures and planned actions distributed to all project partners;
    - **Targeted group**: Project partners to identify events of interest and promote the project's outcomes.
- **Measure 1.4**: A regular update of the communication, dissemination and exploitation plan with lessons learnt will take place every year M12/M24/M36. This includes breakdown of target stakeholder groups, a timeline of key EU/international related events, consultations and policy milestones over the lifetime of the project, with a clear strategy for planned ways to engage with these.
    - **KPI**: 3 versions of the CDEB plan;
    - **Targeted group**: Project partners in order to better organize CDEB actions.
- **Measure 1.5**: Early contact with key work groups (e.g. consortia from similarly themed projects, digital skills initiatives, EC institutions) will be incrementally made to discuss collaboration opportunities through scoping ways to foster the project impacts.
    - **Target group**: Participants, project partners and relevant stakeholders active in Horizon EU/ CEF/ENISA, Erasmus+, COSME, DG EMPL, DGCNECT projects and initiatives

related to cybersecurity digital skills to initiate synergies and collaborations for results promotion, co-organise events and formulate an enhanced educational agenda that can link to external agendas (e.g. the EU agenda);

- **KPIs**: >10 similarly themed projects and initiatives identified; >5 jointly organized workshop.

- **Measure 1.6**: The CyberSecPro partners will carefully select publication venues based on their scientific excellence and impact privileging where possible open access publishing. Indicative journals and conferences and that will be targeted include: Journal of the Learning Sciences, International Journal of Computer-Supported Collaborative Learning (Springer), Computer Supported Cooperative Work (Springer), Journal Cybersecurity (Springer), Journal of Cybersecurity (Oxford Academic), International Journal of Critical Infrastructure Protection (Elsevier), Journal Computers & Security (Elsevier), Transactions on Artificial Intelligence (IEEE), Journal of Machine Learning (Springer), Journal of Machine Learning Research (Microtome), Journal on Data Quality (ACM), Journal of Surveillance, Security and Safety, Journal of Marine Science and Engineering, International Journal of Maritime Crime and Security, International Security, International Journal of Smart Security Technologies, International Conference on Maritime Security, Maritime Security and Coastal Surveillance Conference, Maritime Reconnaissance and Surveillance Technology Conference, Cyber and Space Security conference, etc.
  - **KPIs**: >15 publications in international referred publications; >6 publications in international magazines; >20 conference/ scientific events/ industrial for presentations;
  - **Target group**: The scientific community conducting core or application research on advancing in order to enable future advancements in cybersecurity trainings and inspire innovation further research based on the project's concept and results.

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

- **Measure 2.1**: CyberSecPro aims to find mechanisms for better feed-in from the project to the EU priorities on digital skills and especially in cybersecurity capabilities and skills. This will be achieved through initiating scoping activities with key working groups to open up discussion around some of the aspects (e.g., cyber ranges, digital Hubs) being funded by the European Commission in order to ensure that a variety of voices are present. These discussions aim to provide education priority recommendations for specific topics such as: interoperability, sharing cyber exercises, homogenizing the curricula, development of green, energy and cost-efficient training infrastructures.
  - **KPIs**: >1000 downloads of high-quality electronic brochures with the technical approach and activities; >1 new discussion per month in LinkedIn;
  - **Targeted group**: Universities, Ministries of Education/Maritime/Health/Energy, Industry associations, technology clusters and other innovation communities to include the project's results to collaborative activities (roadmap, white papers, position papers), disseminate the results to their members and enable bilateral participation in events for knowledge exchange.
- **Measure 2.2**: A website with a dedicated private partner space will host key information produced by the project from M2, including reports, 5-min videos created for You-Tube, infographics, webinar downloads, as well as summaries of all activities and ways to get involved.
  - **KPIs**: >30 downloads monthly; >150 views of 5-min videos in You-Tube by the end of the project;

- **Targeted group**: Industry actors, research and academic community and the general public.

- **Measure 2.3**: A series of in person-events will be organised including: three (3) open INFO days (M10, M18, M26), a technology showcase event in M24, workshops, virtual participation tools, e.g. live streaming, and a panEuropean (final event) conference in M36 to present results of the project.
  - **KPIs**: >5 events (up to 25 participants) and >3 events (25-100 participants) organized by the end of the project; >40% of the participants in each event attracted and registered as contacts;
  - **Target group**: All industry actors, research and academic community, ICT and domain experts.
- **Measure 2.4**: Public consultation and policy events involving policy makers and relevant working groups (identified through e.g. policy fellowship schemes) will be closely monitored and results will be presented in open national and international networking events in order to boost reciprocal relationships between students, academics, sectoral specialists, researchers, industry and policy makers (e.g. Ministries of Education) focusing on crucial advance trainings of digital skills. The aim is to let them know the progress accomplished in CyberSecPro and influence them to capitalize on the project results and on the demonstrator outcomes and best practices identified.
  - **KPIs**: >50 hard copies distributed in >5 events; engagement of >7 policy making bodies;
  - **Target group**: Policy makers (national ministries, governmental officers, councils, EU, National, Regional and Local Authorities (NRLA), Regulatory Agencies, Standardisation Organisations e.g., ETSI, CEN, ISO), EU Institutions and agencies (e.g. DG CNECT, DG EMPL, ENISA, JRC, ECSO) to evaluate the project's Social-Technological, Economic-Environmental-Political (STEEP) aspects, define future training, education, research and innovation directions and provide input for standardization activities.

CDEB Objective 3 | Work to deliver and monitor project impacts as related to exploitation of outputs.

- **Measure 3.1**: Presentation of the results to engage different stakeholders for exploitation of the outputs through project visits to education and industrial open days and networking events, organization of workshops, participation Associated with document Ref. Ares (2022)7790839 - 11/11/2022 Call: DIGITAL-2021-SKILLS-01 43 to selected EU Annual Meetings, conferences and exhibitions (e.g., International Cyber Expo, Undersea Defense Technology event, Border Security Expo, Eurosatory). Engagement will be particularly strengthened by suggestions coming from the CyberSecPro partners, especially the pilot partners, as well as the technical partners after analysing the relevance of their contact network members to the project and ad-hoc identification processes.
  - **Target group**: Enterprises in the higher education/cybersecurity/health/maritime /energy /ICT domains as well as sectoral specialist, ICT operators, security systems providers; these include (i) the end-users of the project for commercial exploitation of the results by incorporating these into their standard flowcharts, (ii) the industrial partners of CyberSecPro for technological exploitation of the results, developing and delivering training programs and/or services built on top of the project training material and modules, (iii) companies outside the consortium that will mainly capitalize on the technological exploitation model, (iv) education and research organisations for exploiting the research results to re-utilise the know-how in future research activities or founding spin-offs and start-ups to commercially exploit the developed training program , (v) investors from the private or public sector that are interested in investing in the delivery of the innovations to the market;

- **KPIs**: Participation in >10 small and large-scale events by the end of the project; >2 events organized with >100 attendees; >20% of participants engaged for further exploitation.

- **Measure 3.2**: Internal Consortium monthly emails will be sent to inform about project progress, upcoming events, round-table discussions and dissemination and exploitation opportunities.
  - **KPI**: >15 emails with rich information on project progress and DE events & opportunities;
  - **Target group**: Project partners.

- **Measure 3.3**: Quarterly reports will be compiled to monitor the results and update the CDEB plan. These will include a set of KPIs that will be regularly updated in order to quantitively monitor the expected impact of the proposed measures. These KPIs will be also leveraged to evaluate marketing effectiveness, validate market potential and key insights.
  - **KPI**: 6 reports published with CDEB KPIs that are continuously updated;
  - **Target group**: Project partners

CDEB Objective 4 | Accelerate business growth through direct and indirect integration of the project's benefits.

- **Measure 4.1**: Training workshops relevant to the project's training approach and achievements will be organized internally in each partner organization to build staff capacity. Training Need Assessment will be conducted and capacity development will be assessed at the end of the workshop.
  - **Target group**: Project partners;
  - **KPIs**: >80 internal trainees for becoming familiar with the CyberSecPro training tools and program.

- **Measure 4.2**: Partners (especially SMEs) will seek to join forces with other HEIs and businesses in order to promote the new hands-on training programme to new universities or existing customers or launch them in new sectors or geographical areas. This will be achieved through participation in international networking events (e.g. International Cyber Expo, Undersea Defense Technology event, Border Security Expo, Eurosatory etc.), as well as through marketing channels (email marketing, social media, business websites).
  - **KPI**: ≥10 partnership formed with key business in the field by the end of the project;
  - **Target group**: Project partners, health/energy/maritime specialists, partners' existing clientele.

Competitiveness and benefits for society

Societies are continuously threatened by catastrophic attacks with severe impact to their daily professional, business and personal activities.

The accelerated digitalisation in all economic sectors put our critical infrastructures, cyberspace and lives in danger. The cybersecurity and privacy dimensions of the emerging technologies (e.g. AI, IoT, Blockchain, IoT, 5G, supply chains, Digital twins) are becoming ever more compelling in a world where "everything is connected with everything". A skilled workforce is needed in EU to address the upcoming challenges. No one can be left behind in this effort to enhance practical cybersecurity capabilities. The HEIs have gained the necessary trust for becoming the main cybersecurity practical training providers. The CyberSecPro project will help HEIs to strengthen their educational role in the demanding digital transformation era by opening their activities, mandate and collaborations with the private sector, industries and the DSM.

The society will only benefit for this new enhanced HEI mission helping people to have the appropriate capabilities to join right after their studies the cybersecurity workforce that so much is needed; to upskill

the existing workforce and develop the new work force capable to address the technological and ethical cybersecurity challenges that the accelerated digitalisation brings.

Only a skilled workforce can design, develop and integrate EU trustworthy, novel ICT products based on security and privacy by design principles promoting the European democratic and ethical values in the competitive global markets.

Europe will remain pioneer in the important sectors of maritime, health and energy only if the workforce is prepared to address the upcoming cybersecurity.