CYBERSECPRO:
DIGITAL EUROPE PROGRAMME

CyberSecPro: An Approach to cybersecurity training and skills enhancement

Prof. Christos Douligeris, University of Pireaus, Greece, cdoulig@unipi.gr
Slides prepared in cooperation with Prof. Paresh Rathod, Thematic Leader (Cybersecurity), Laurea University, Finland

CyberSecPro

Co-funded by the European Union

CyberSecPro rationale

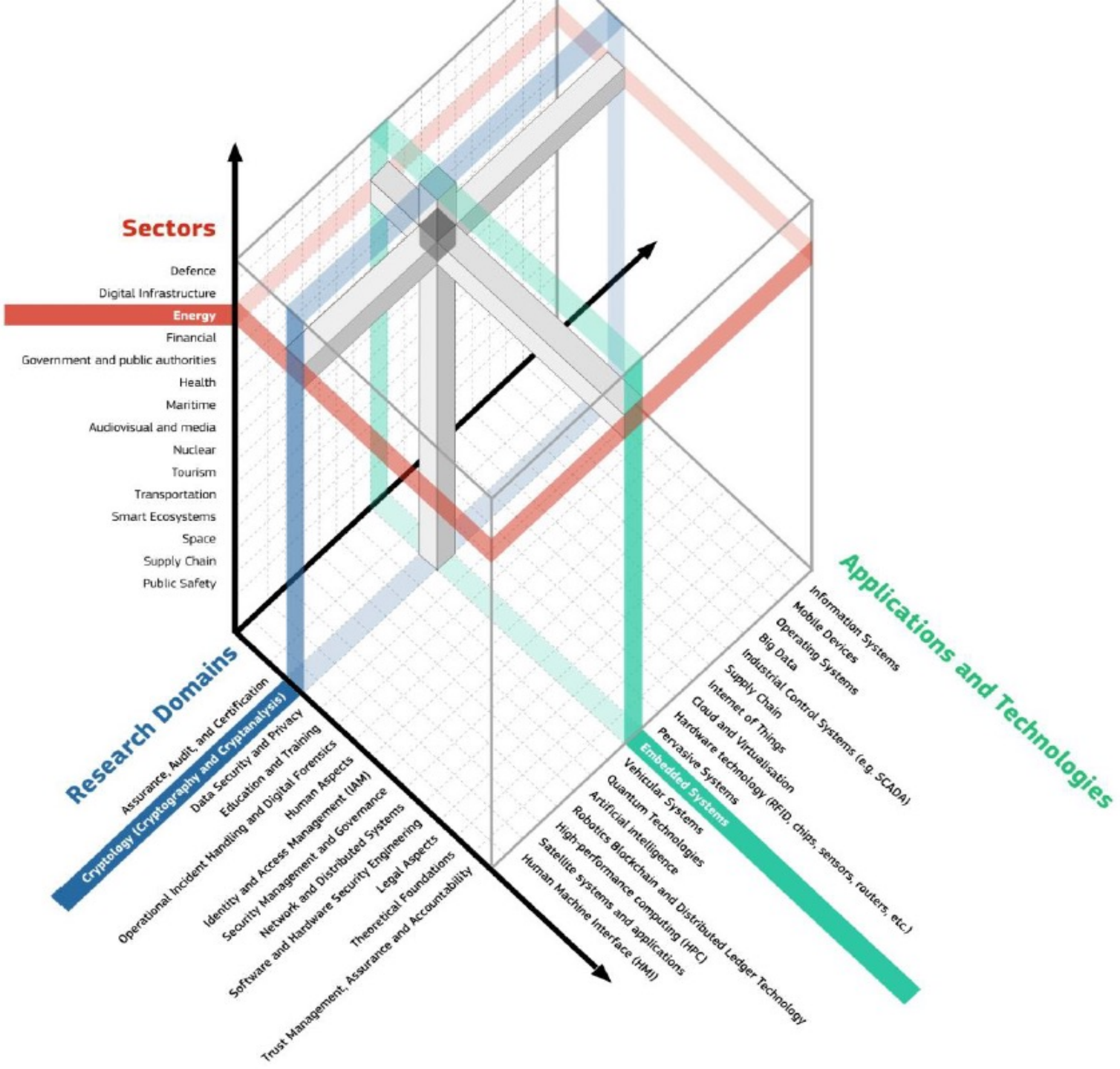
- **CyberSecPro**'s project ambition is to enhance the role of the Higher Education Institutes (HEIs) in offering hands-on and working-life skills for driving a trustworthy digital transformation in critical sectors of the economy including the energy, health and maritime sectors.
- Higher Educational Institutions need to become the main providers of cybersecurity dynamic capabilities and practical skills through the offering of flexible practical training modules in knowledge areas that are needed in the maritime sector.
- Fostering collaboration of the universities with all business sectors, will provide the necessary boost to sustainable and effective practical cybersecurity training programs based on state-of-the art technological training tools, real-life based training material and digital-driven pedagogical approaches.
- By establishing a unique Learning Factory, **CyberSecPro** will be an authentic environment to link innovation, research, industry, academia and SME support.

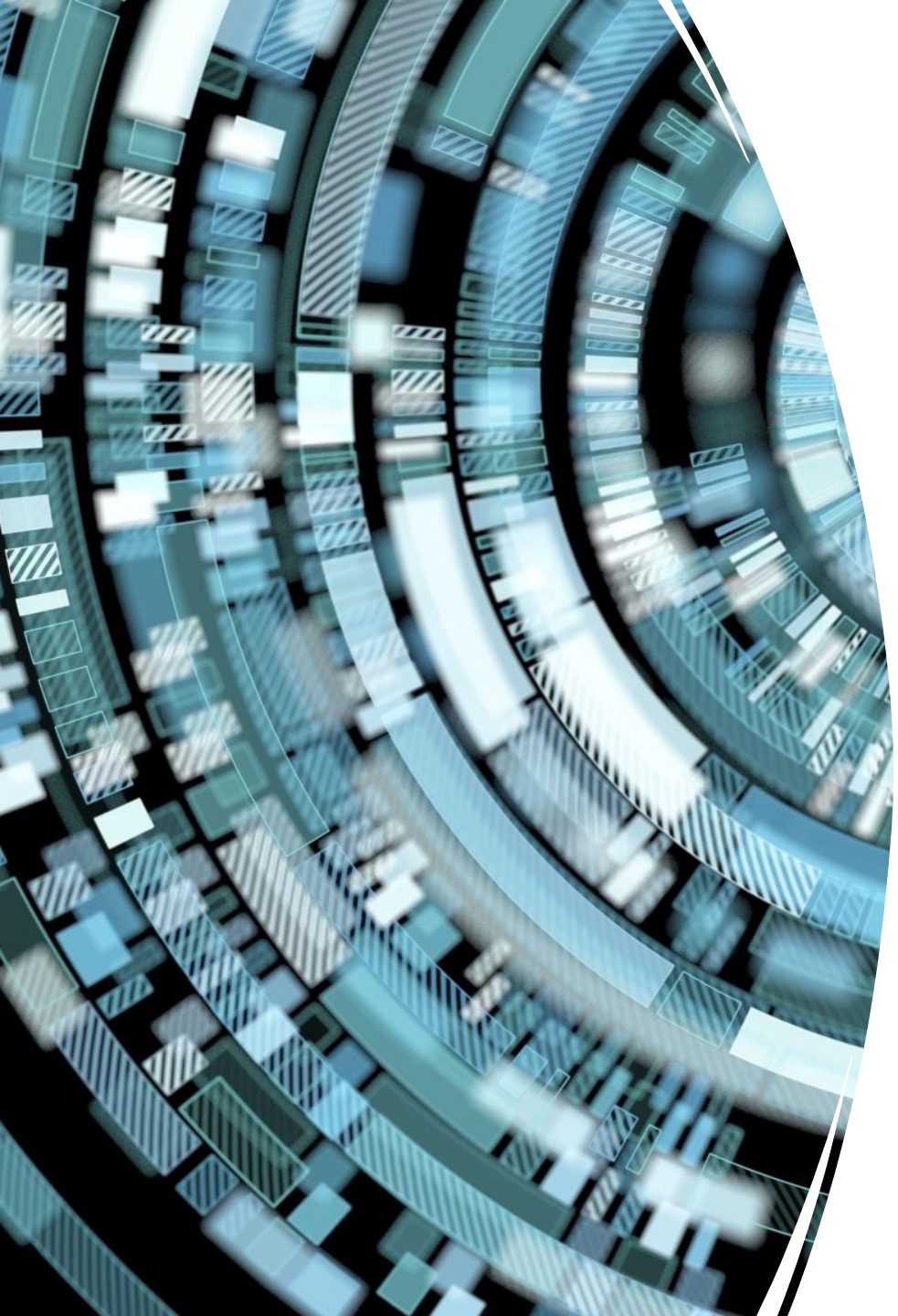
CyberSecPro Rationale (cont.)

- The **CyberSecPro** collaboration among the HEIs and the private sector (security companies) will enhance the role of the HEIs by bringing them closer to the markets' and industries' – including the maritime sector - needs and by opening-up to society.
- **CyberSecPro** will prepare learners (students, administrators, employees, professors, developers, integrators, and manufacturers) to become the workforce needed to address the emerging needs given the evolving digital threat landscape and challenges.
- HEIs will embrace the needs of a variety of training including personnel, administrators, engineers, developers, integrators, and security and privacy officers from all economic sectors.

CyberSecPro Rationale (cont.

- **CyberSecPro** shares European Commission's Joint Research Centers4 methodological view that Cybersecurity is a three-dimensional science that supports all sectors, 14 domains, applications and technologies





CyberSecPro main domains

- CyberSecPro will drive the HEIs to further enhance their cooperation with the private sector, in order to become the main suppliers of the necessary market-oriented cybersecurity skills and working-life practices required in the digital transformation, via providing hands-on trainings in the following six (6) cybersecurity domains:
    1. *Data Security and Privacy*
    2. *Operational Incident Handling and Digital Forensics*
    3. *Security Management and Governance*
    4. *Software and Hardware Security Engineering*
    5. *Security Measurements*
    6. *Human Aspects*

CyberSecPro Objectives

- **Obj 1 – Market Analysis of Cybersecurity Practical Skills and Values**
- **Obj 2 – Building Public Private Partnerships (PPPs) for Sustainable hands-on Cybersecurity Training**
- **Obj 3 – Employ State-of -Art- technological Training Tools**
- **Obj 4 – Build Market Oriented Learning Models**
- **Obj 5 – CyberSecPro program operation and Evaluation**
- **Obj 6 – CyberSecPro as a best practice-Certification Scheme for Practical Cybersecurity Training Programmes**

CyberSecPro Market Analysis

To conduct market analysis of cybersecurity practical skills and values: **Assess cybersecurity skills, and competencies needed in the market**

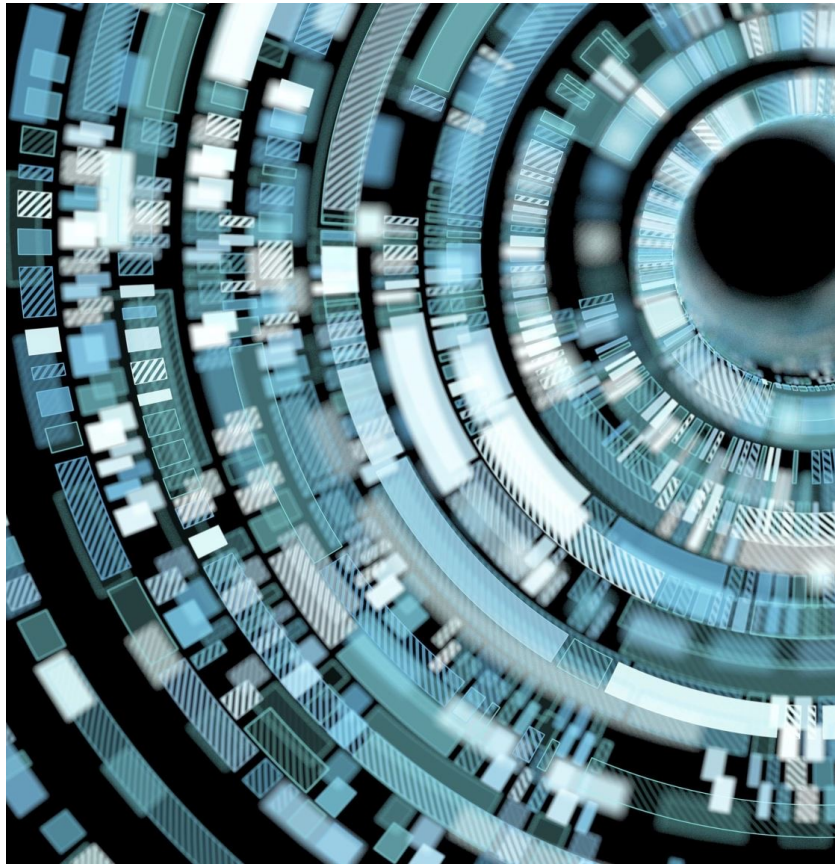
To analyse the practical skills offered in EU academic programmes: **Assess practical cybersecurity skills offered by EU academic programmes**

To analyse technological tools and academic trainings: **Assess practical tools and professional skills offered by EU academic programmes**

Prepare a CSP professional training programme

CyberSecPro Market Study Data

- The survey asked about the respondents' work organisations to establish survey demographics. The results show that:
  - **23 % of respondents worked at large organisations**
  - **2.9 % were professional practitioners**
  - **8.6 % worked for government organisations,**
  - **35.4 % worked at a university or research institute, and**
  - **27.6 % were in small and medium-sized enterprises (SMEs)**



CyberSecPro Report Released

Download our study on skills gaps in practical cybersecurity

As part of CyberSecPro's analysis, the consortium undertook a detailed analysis of the needed skills and competencies in EU cybersecurity to inform the development of education and training materials.

Download report

https://cybersecpro-project.eu/

CyberSecPro Practical Skills Gap in Europe

Source: Authors - CyberSecPro-D2.1 Report: Cybersecurity Skills Gaps in Europea

CyberSecPro Practical Skills Gap in Europe

Table 22: Knowledge Area Prioritisation for All Sectors

Knowledge Areas	Health	Energy	Maritime	ICT	Other
Penetration Testing	In demand	In demand	High demand	High demand	High demand
Cybersecurity Tools/Technologies	In demand	In demand	In demand	High demand	High demand
Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	In demand	In demand	In demand	High demand	In demand
Cybersecurity Management Systems: CS Management and Processes	In demand	In demand	High demand	High demand	High demand
Risk Assessment and Risk Management	In demand	In demand	In demand	High demand	In demand
Emerging Technologies	In demand	In demand	In demand	High demand	
Cybersecurity Regulations and Compliance	In demand	In demand	In demand	High demand	In demand
Cybersecurity Education and Training	In demand	In demand	In demand	In demand	In demand
Incident Response	In demand	In demand	In demand	In demand	In demand
Communications and Network Security: Network Security Controls	In demand	In demand	In demand	In demand	In demand
Cybersecurity Forensics	In demand	In demand	In demand	In demand	In demand
Cloud Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity for Artificial Intelligence and Machine Learning	In demand	In demand	In demand	In demand	In demand
Cybersecurity Architecture	In demand	In demand	In demand	In demand	In demand
Data Protection and Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity Engineering	In demand	In demand	In demand	In demand	In demand

CyberSecPro Practical Skills Gap in Europe(cont.)

Table 23: Hands-on Skills Prioritisation for All Sectors

Hands-on Skills	Health	Energy	Maritime	ICT	Other
Penetration Testing	In demand	In demand	In demand	High demand	In demand
Cybersecurity Threat Management	In demand	In demand	In demand	High demand	In demand
Risk Assessment and Risk Management	In demand	In demand	In demand	High demand	In demand
Cybersecurity Regulations and Compliance	In demand	In demand	In demand	In demand	In demand
Cybersecurity Education and Training	In demand	In demand	In demand	In demand	In demand
Incident Response	In demand	In demand	In demand	In demand	In demand
Communications and Network Security: Network Security Controls	In demand	In demand	In demand	High demand	In demand
Cybersecurity Forensics	In demand	In demand	In demand	In demand	In demand
Cloud Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity for Artificial Intelligence and Machine Learning	In demand	In demand	In demand	In demand	In demand
Cybersecurity Architecture	In demand	In demand	In demand	In demand	In demand
Cybersecurity Engineering	In demand	In demand	In demand	In demand	In demand
Programming Skills	In demand	In demand	In demand	In demand	In demand
Operating Systems	In demand	In demand	In demand	In demand	In demand
Communication and Teamwork (soft skills)	In demand	In demand	In demand	In demand	In demand
Software Design Skills	In demand	In demand	In demand	In demand	In demand
Management Skills (soft skills)	In demand	In demand	In demand	In demand	In demand
Legal Training and Auditing	In demand	In demand	In demand	In demand	In demand
Software Security	In demand	In demand	In demand	In demand	In demand
Network and System Administration	In demand	In demand	In demand	In demand	In demand
Analytical and Critical Thinking (Soft skills)	In demand	In demand	In demand	In demand	In demand

CyberSecPro Maritime specific findings

- **Lack of awareness of maritime cybersecurity risks.**
  - Many maritime professionals are not aware of the specific cybersecurity risks facing the maritime industry. This can make them more vulnerable to attacks.
- **Lack of technical cybersecurity skills.**
  - Many maritime professionals do not have the technical cybersecurity skills they need to protect their organizations from cyberattacks. This includes skills such as network security, application security, and incident response.
- **Lack of experience in responding to cyberattacks.**
  - Maritime companies often lack experience in responding to cyberattacks. This can lead to delays in detecting and responding to attacks, which can increase the damage caused by the attack.

CyberSecPro Maritime specific findings

- Provide maritime professionals with cybersecurity training.
  - This training should cover both the technical and non-technical aspects of cybersecurity. It is also important to make sure that the training is relevant to the specific needs of the maritime industry.
- Develop cybersecurity certifications for maritime professionals.
  - This will help to ensure that maritime professionals have the necessary skills and knowledge to protect their organizations from cyberattacks.
- Encourage maritime companies to invest in cybersecurity training for their employees.
  - Maritime companies should also make sure that they have a cybersecurity plan in place and that employees are regularly trained on the plan.
- Promote collaboration between the maritime industry and the cybersecurity community.
  - This will help to ensure that maritime companies have access to the latest cybersecurity information and best practices.

Why is CyberSecPro important for the industry?

What we are working on

CyberSecPro Analysis

We analyse the EU Cybersecurity market to build education and training materials that individuals and organisations need.

CyberSecPro Events

We undertake a lot of education, training and dissemination events to spread and apply our knowledge and results.

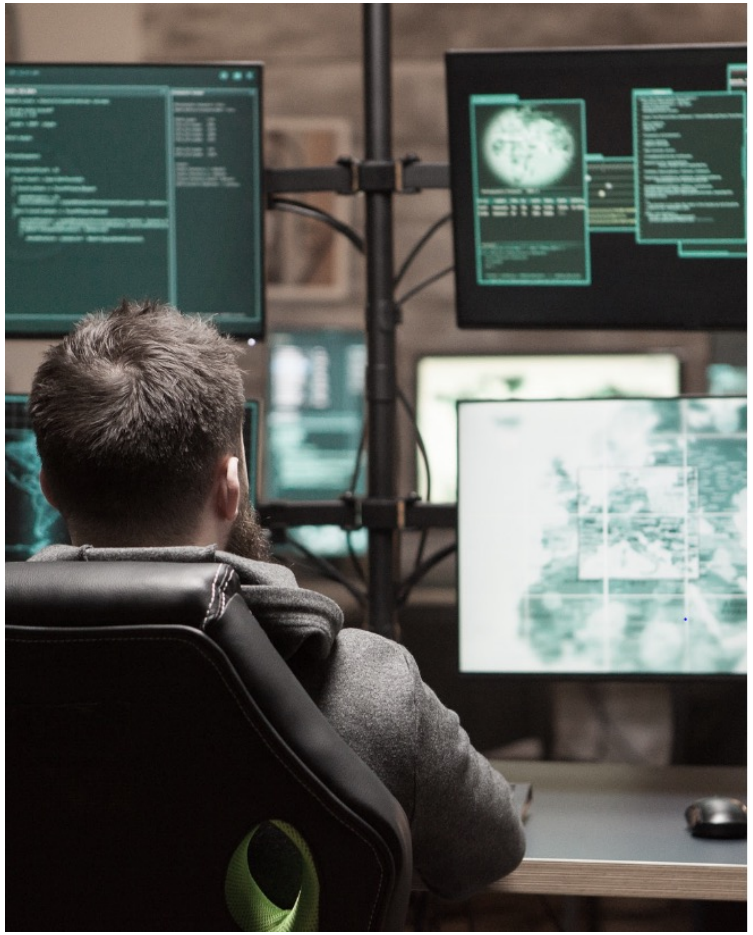
CyberSecPro Training Materials

We develop a large variety of materials that can be used by educators and trainers in cybersecurity.

CyberSecPro Certification

We develop a certification scheme to recognise cybersecurity competencies.

Why is CyberSecPro important for the industry?



OUR AMBITION

Shaping the future of EU cybersecurity.

We aim to contribute to the advancement of cybersecurity education and training by:

- **Developing material for theoretical and practical skills development**
- **Training and certifying students and professionals**
- **Promoting partnerships**

Why is CyberSecPro important for the industry?

- We are living in the Era of Cooperation, Collaboration, and Partnership
- Leaving you with thought: “Let's cooperate, not compete, to consolidate cybersecurity for goods.”

THANK YOU

FOR YOUR ATTENTION

cybersecpro-project.eu

CyberSecPro

Co-funded by
the European Union