EUROPEAN CYBERSECURITY SKILLS WORKSHOP

20-21 NOVEMBER 2025

BRUSSELS BELGIUM

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
Brussels

CyberSecPro - training courses aligned to ECSF

Chatzopoulou Argyro
APIROPLUS SOLUTIONS

CyberSecPro · CYBER SYNCHRONY · IANUS TECHNOLOGIES · INFOTREND CO LTD · RESEARCH CENTER UNIVERSITY OF PIRAEUS · GRUPPO Maggioli · NERO advaNced cybErsecurity awaReness ecOsystem for SMEs · trustilio Enhance your Trustworthiness

The CYBERSECPRO project

CYBERSECPRO

The challenge:

EU Higher Education Institutions (HEIs) have more than **128 cybersecurity** academic programs (undergraduate and graduate) as identified by ENISA (CyberHEAD), JRC (ATLAS) and a variety of reports. These academic programs, with their **static curricula**, do not provide the dynamic capabilities and emerging skills needed in the market.

The solution:

Fourteen (14) HEIs and thirteen (13) security companies from sixteen (16) EU countries propose the **agile CyberSecPro professional cybersecurity practical and hands-on training program** that complements, supports, and advances the existing academic programs by linking innovation, research, industry, academia and SME support.

CyberSecPro is 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 HADEA. Neither the European Union nor the granting authority can be held responsible for them. Project Agreement no. 101083594

Rationale

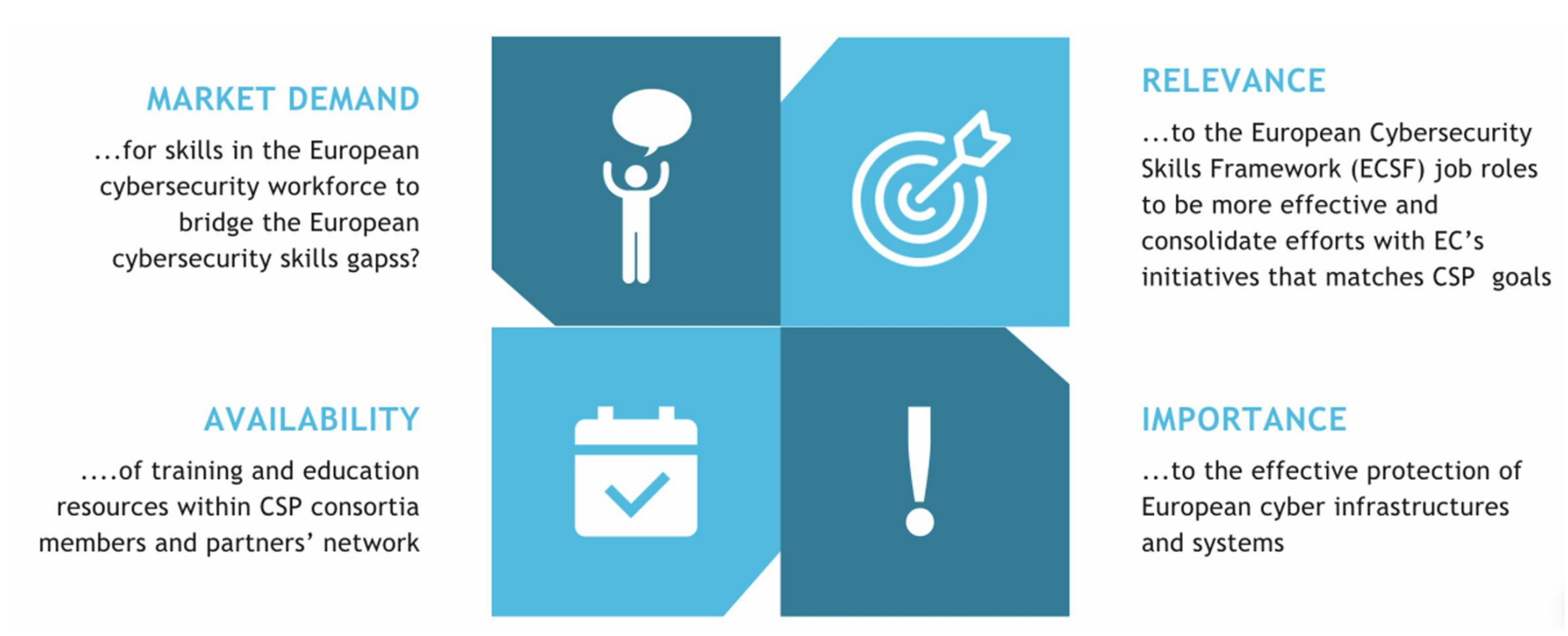
- Practical cybersecurity skills and capabilities are needed (to complement cybersecurity knowledge and research efforts)
- Prepare the next generation workforce and upskill the existing workforce
- Link innovation, research, industry, academia and SME support
- Build PPPs to offer sustainable practical trainings in the HEIs and training centers
- Close the gap between training offerings and mar demands
- Use and further develop cybersecurity professional role profiles and skills frameworks like the ENISA European Cybersecurity Skills Framework (ECSF)

Rationale

CYBERSECPRO

- Practical cybersecurity skills and capabilities are needed (to complement cybersecurity knowledge and research efforts)
- Build PPPs to offer sustainable practical trainings in the HEIs and training centers
- Prepare the next generation workforce and upskill the existing workforce
- Close the gap between training offerings and market demands
- Link innovation, research, industry, academia and SME support
- Use and further develop cybersecurity professional role profiles and skills frameworks like the ENISA European Cybersecurity Skills Framework (ECSF)

Selection criteria



MARKET DEMAND

...for skills in the European cybersecurity workforce to bridge the European cybersecurity skills gapss?

RELEVANCE

...to the European Cybersecurity Skills Framework (ECSF) job roles to be more effective and consolidate efforts with EC's initiatives that matches CSP goals

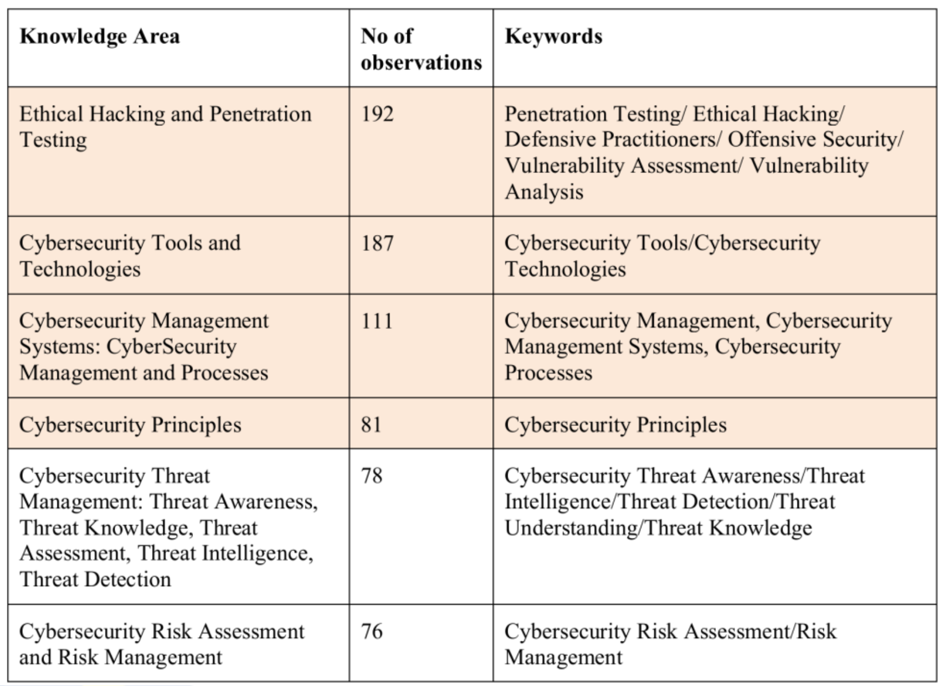
AVAILABILITY

....of training and education resources within CSP consortia members and partners' network

IMPORTANCE

...to the effective protection of European cyber infrastructures and systems

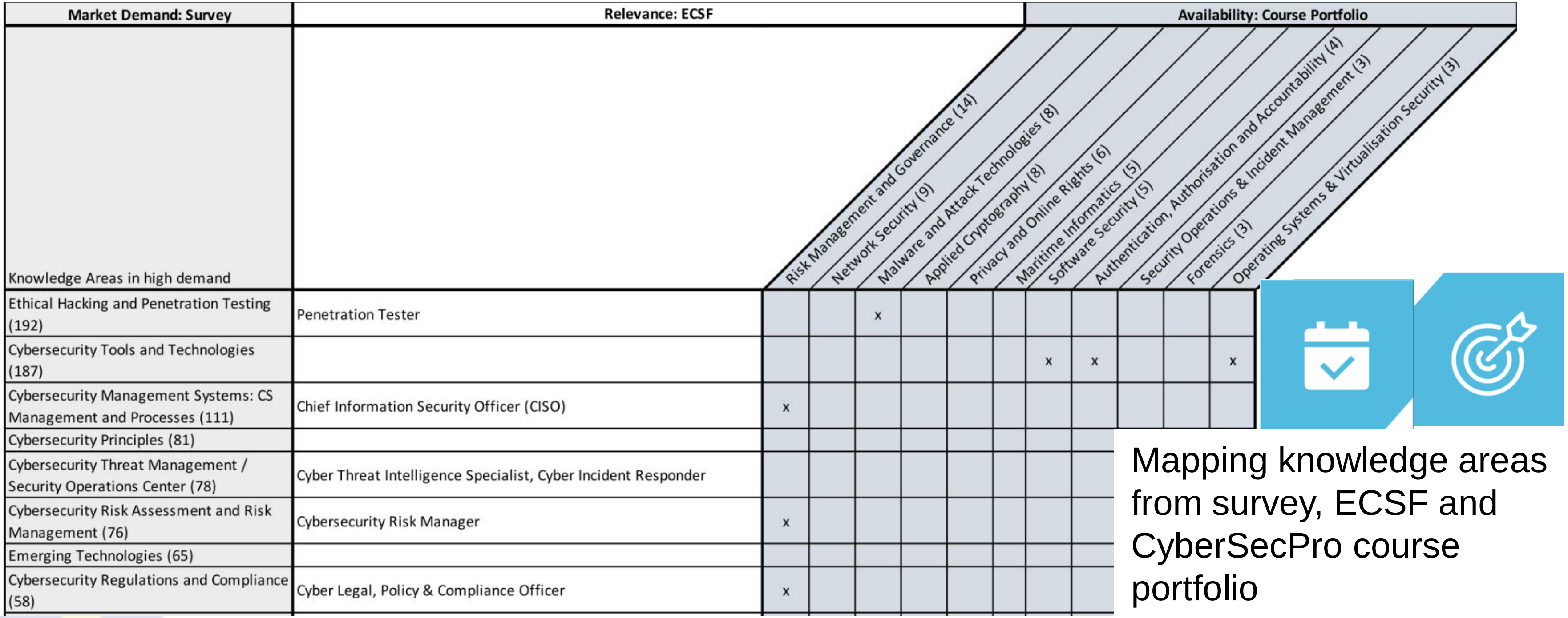
How (market survey)



Knowledge Area	No of observations	Keywords
Ethical Hacking and Penetration Testing	192	Penetration Testing/ Ethical Hacking/ Defensive Practitioners/ Offensive Security/ Vulnerability Assessment/ Vulnerability Analysis
Cybersecurity Tools and Technologies	187	Cybersecurity Tools/Cybersecurity Technologies
Cybersecurity Management Systems: CyberSecurity Management and Processes	111	Cybersecurity Management, Cybersecurity Management Systems, Cybersecurity Processes
Cybersecurity Principles	81	Cybersecurity Principles
Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	78	Cybersecurity Threat Awareness/Threat Intelligence/Threat Detection/Threat Understanding/Threat Knowledge
Cybersecurity Risk Assessment and Risk Management	76	Cybersecurity Risk Assessment/Risk Management

Knowledge areas from market demand survey

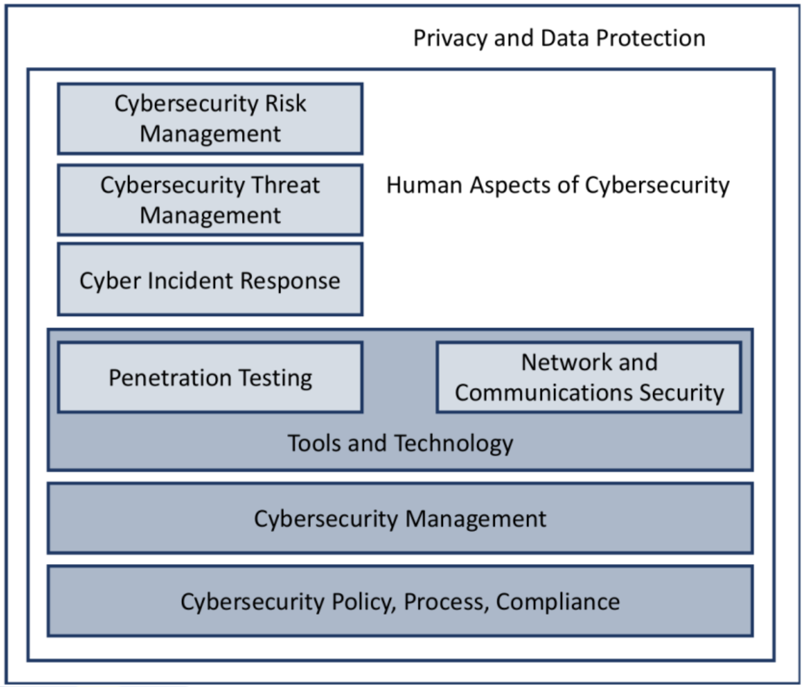
How (cross mapping)



Market Demand: Survey	Relevance: ECSF	Availability: Course Portfolio										
Knowledge Areas in high demand		Risk Management and Governance (14)	Network Security (9)	Malware and Attack Technologies (8)	Applied Cryptography (8)	Privacy and Online Rights (6)	Maritime Informatics (5)	Software Security (5)	Authentication, Authorisation and Accountability (4)	Security Operations & Incident Management (3)	Forensics (3)	Operating Systems & Virtualisation Security (3)
Ethical Hacking and Penetration Testing (192)	Penetration Tester			x								
Cybersecurity Tools and Technologies (187)								x	x			x
Cybersecurity Management Systems: CS Management and Processes (111)	Chief Information Security Officer (CISO)	x										
Cybersecurity Principles (81)												
Cybersecurity Threat Management / Security Operations Center (78)	Cyber Threat Intelligence Specialist, Cyber Incident Responder											
Cybersecurity Risk Assessment and Risk Management (76)	Cybersecurity Risk Manager	x										
Emerging Technologies (65)												
Cybersecurity Regulations and Compliance (58)	Cyber Legal, Policy & Compliance Officer	x										

Mapping knowledge areas from survey, ECSF and CyberSecPro course portfolio

Overview of CyberSecPro knowledge areas



Privacy and Data Protection

Cybersecurity Risk Management

Cybersecurity Threat Management

Cyber Incident Response

Human Aspects of Cybersecurity

Penetration Testing

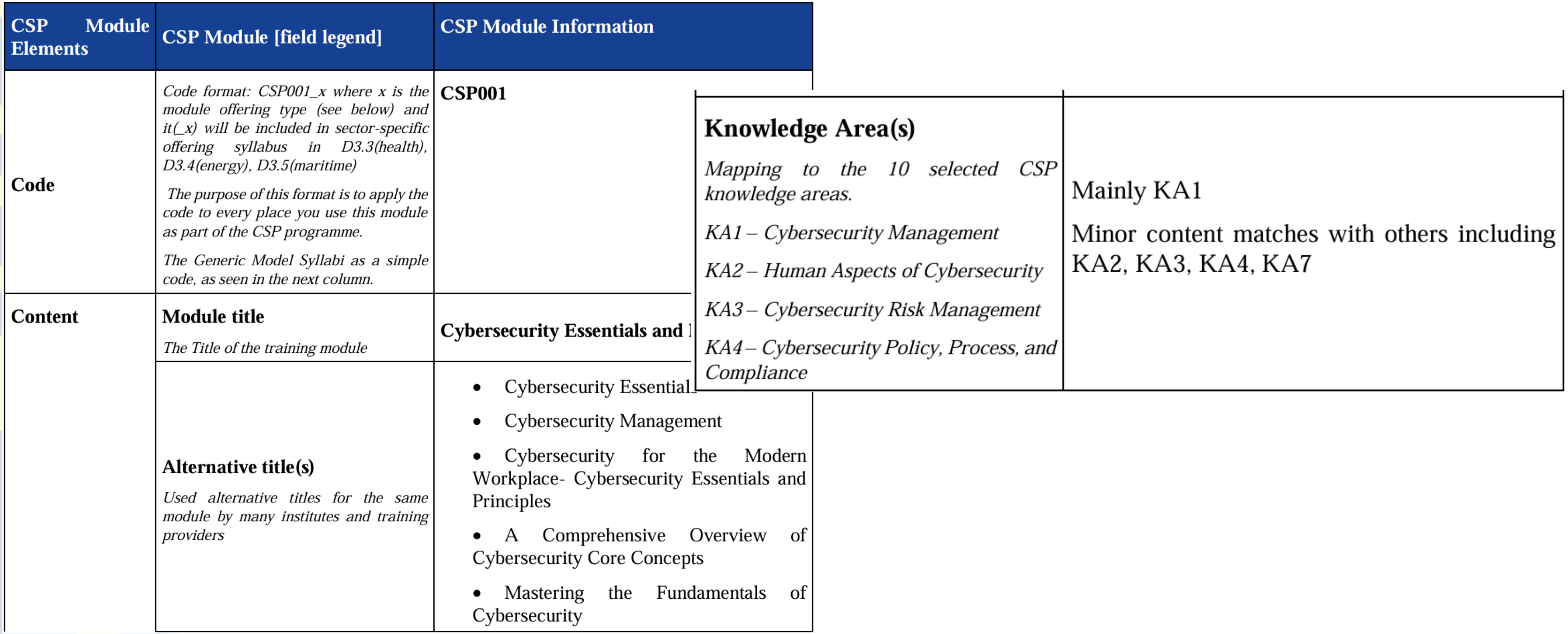
Network and Communications Security

Tools and Technology

Cybersecurity Management

Cybersecurity Policy, Process, Compliance

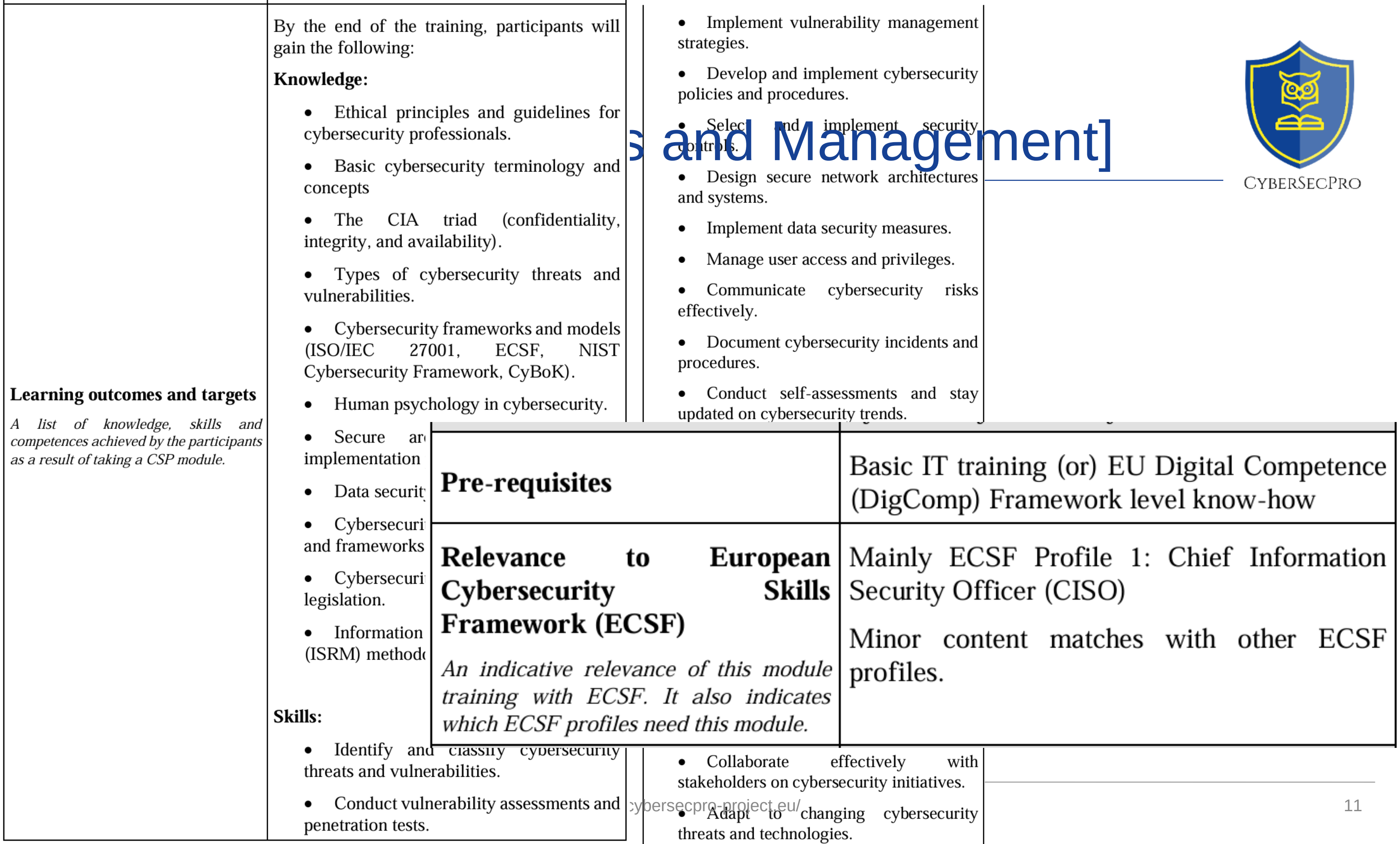
Example
[Cybersecurity Essentials and Management]



CSP Module Elements	CSP Module [field legend]	CSP Module Information
Code	*Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)* *The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.* *The Generic Model Syllabi as a simple code, as seen in the next column.*	**CSP001**
Content	**Module title** *The Title of the training module*	**Cybersecurity Essentials and**
	Alternative title(s) *Used alternative titles for the same module by many institutes and training providers*	- Cybersecurity Essential - Cybersecurity Management - Cybersecurity for the Modern Workplace- Cybersecurity Essentials and Principles - A Comprehensive Overview of Cybersecurity Core Concepts - Mastering the Fundamentals of Cybersecurity

Knowledge Area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance*	Mainly KA1 Minor content matches with others including KA2, KA3, KA4, KA7

s and Management]



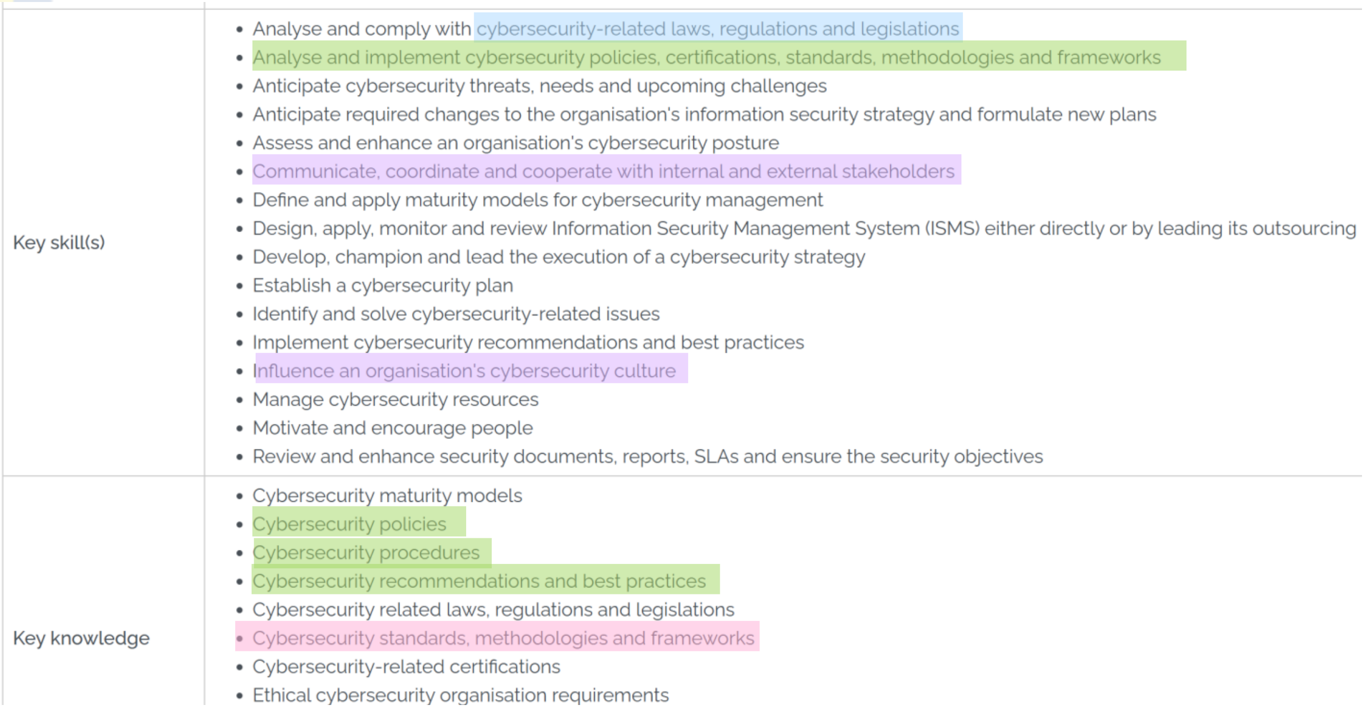
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module.*	By the end of the training, participants will gain the following: **Knowledge:** • Ethical principles and guidelines for cybersecurity professionals. • Basic cybersecurity terminology and concepts • The CIA triad (confidentiality, integrity, and availability). • Types of cybersecurity threats and vulnerabilities. • Cybersecurity frameworks and models (ISO/IEC 27001, ECSF, NIST Cybersecurity Framework, CyBoK). • Human psychology in cybersecurity. • Secure ar implementation • Data securit • Cybersecuri and frameworks • Cybersecuri legislation. • Information (ISRM) methodo **Skills:** • Identify and classify cybersecurity threats and vulnerabilities. • Conduct vulnerability assessments and penetration tests. • Implement vulnerability management strategies. • Develop and implement cybersecurity policies and procedures. • Select and implement security controls. • Design secure network architectures and systems. • Implement data security measures. • Manage user access and privileges. • Communicate cybersecurity risks effectively. • Document cybersecurity incidents and procedures. • Conduct self-assessments and stay updated on cybersecurity trends. • Collaborate effectively with stakeholders on cybersecurity initiatives. • Adapt to changing cybersecurity threats and technologies.

Pre-requisites	Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.*	Mainly ECSF Profile 1: Chief Information Security Officer (CISO) Minor content matches with other ECSF profiles.

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

CHIEF INFORMATION SECURITY OFFICER (CISO)

CYBERSECPRO



Key skill(s)	• Analyse and comply with cybersecurity-related laws, regulations and legislations • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Anticipate cybersecurity threats, needs and upcoming challenges • Anticipate required changes to the organisation's information security strategy and formulate new plans • Assess and enhance an organisation's cybersecurity posture • Communicate, coordinate and cooperate with internal and external stakeholders • Define and apply maturity models for cybersecurity management • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Develop, champion and lead the execution of a cybersecurity strategy • Establish a cybersecurity plan • Identify and solve cybersecurity-related issues • Implement cybersecurity recommendations and best practices • Influence an organisation's cybersecurity culture • Manage cybersecurity resources • Motivate and encourage people • Review and enhance security documents, reports, SLAs and ensure the security objectives
Key knowledge	• Cybersecurity maturity models • Cybersecurity policies • Cybersecurity procedures • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity standards, methodologies and frameworks • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements

Cybersecurity Essentials and Management

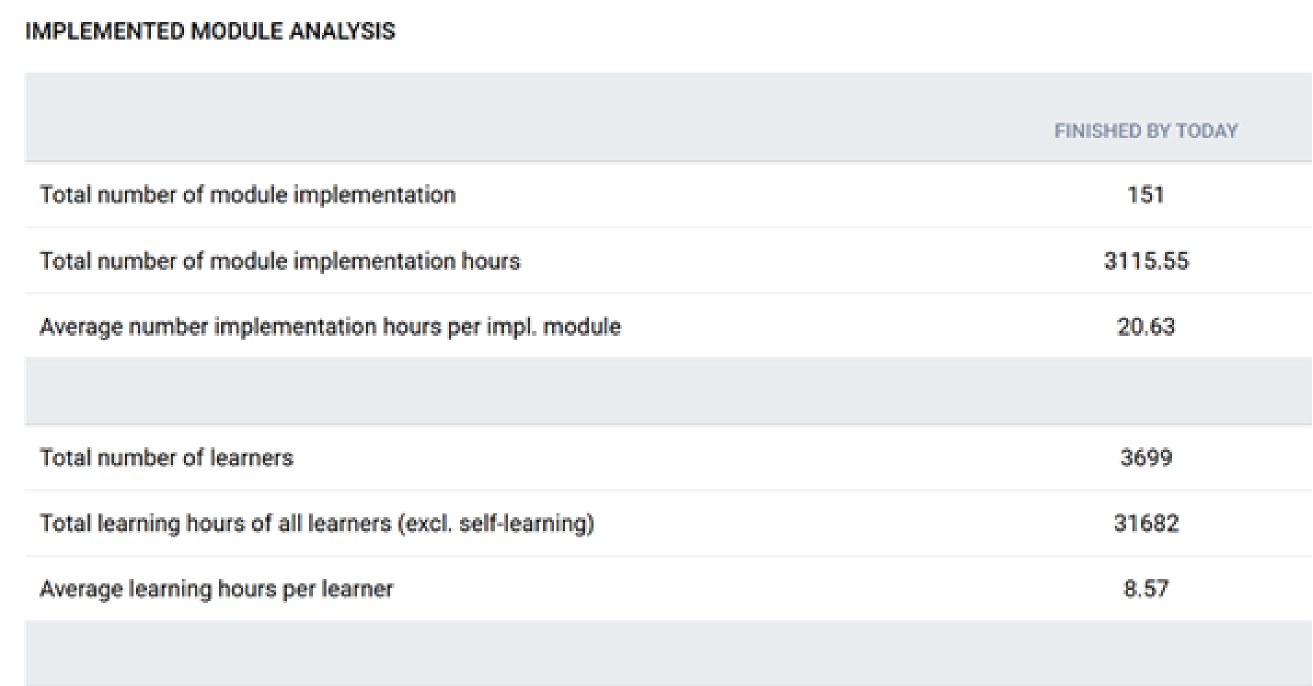
Knowledge:

- Ethical principles and guidelines for cybersecurity professionals.
- Basic cybersecurity terminology and concepts
- The CIA triad (confidentiality, integrity, and availability).
- Types of cybersecurity threats and vulnerabilities.
- Cybersecurity frameworks and models (ISO/IEC 27001, ECSF, NIST Cybersecurity Framework, CyBoK).
- Human psychology in cybersecurity.
- Secure architecture design and implementation principles.
- Data security and privacy principles.
- Cybersecurity governance practices and frameworks.
- Cybersecurity laws, regulations, and legislation.
- Information security risk management (ISRM) methodologies.

Skills:

- Identify and classify cybersecurity threats and vulnerabilities.
- Conduct vulnerability assessments and penetration tests.
- Implement vulnerability management strategies.
- Develop and implement cybersecurity policies and procedures.
- Select and implement security controls.
- Design secure network architectures and systems.
- Implement data security measures.
- Manage user access and privileges.
- Communicate cybersecurity risks effectively.
- Document cybersecurity incidents and procedures.
- Conduct self-assessments and stay updated on cybersecurity trends.

CyberSecPro in numbers

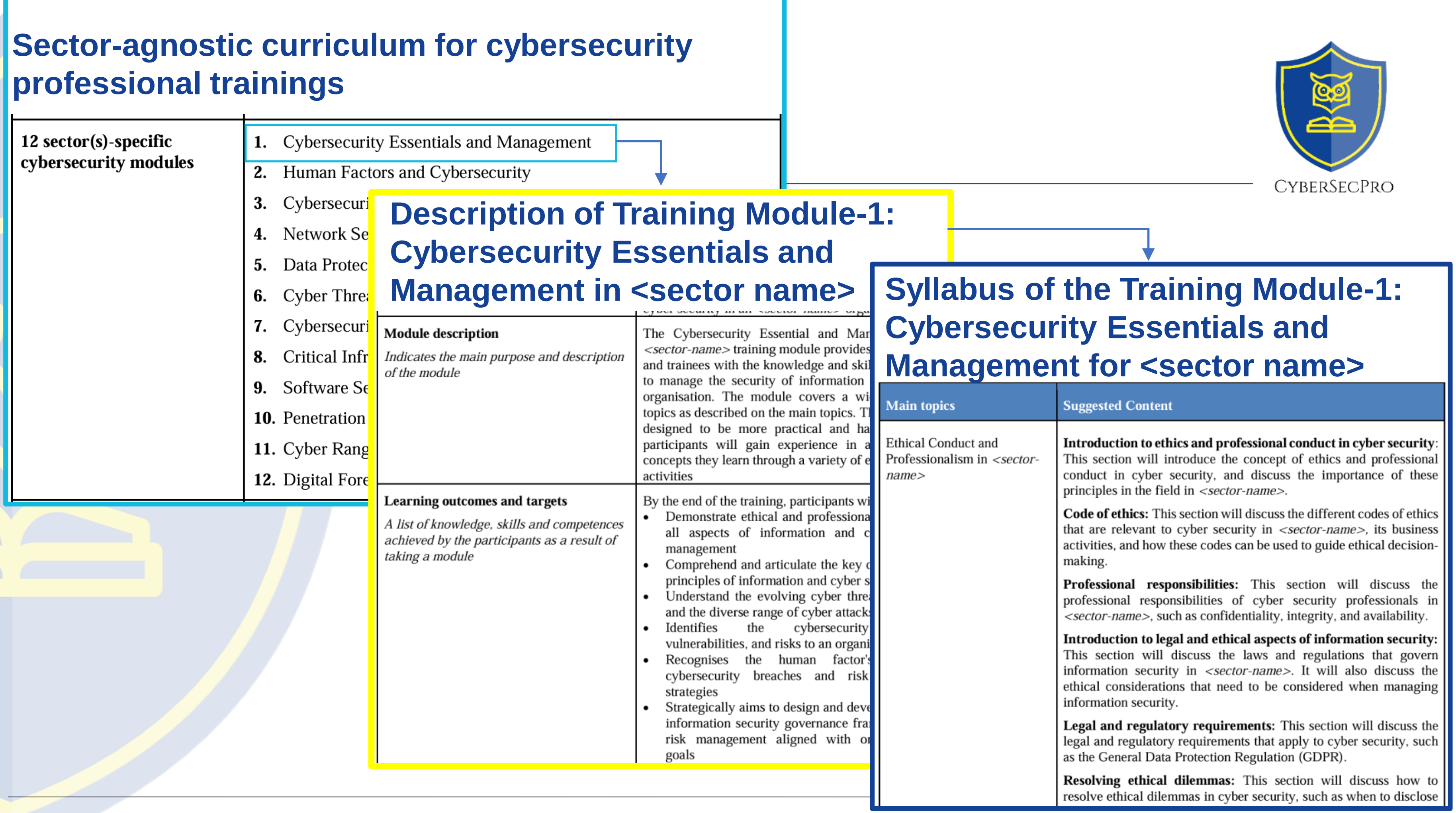


IMPLEMENTED MODULE ANALYSIS

	FINISHED BY TODAY
Total number of module implementation	151
Total number of module implementation hours	3115.55
Average number implementation hours per impl. module	20.63
Total number of learners	3699
Total learning hours of all learners (excl. self-learning)	31682
Average learning hours per learner	8.57

CyberSecPro certification schemes

- We propose a market-driven Industry/Market-specific cybersecurity schemes that can be used for establishing a cybersecurity professional program and /or modules.
- **Sector-agnostic curriculum** for cybersecurity professional trainings
- **Descriptions** of the 12 **sector-specific modules**
- **Syllabi** of the 12 **sector-specific modules**



Sector-agnostic curriculum for cybersecurity professional trainings

12 sector(s)-specific cybersecurity modules	**1.** Cybersecurity Essentials and Management **2.** Human Factors and Cybersecurity **3.** Cybersecuri **4.** Network Se **5.** Data Protec **6.** Cyber Threa **7.** Cybersecuri **8.** Critical Infr **9.** Software Se **10.** Penetration **11.** Cyber Rang **12.** Digital Fore

Description of Training Module-1: Cybersecurity Essentials and Management in <sector name>

cyber security in an <sector name> orga

Module description *Indicates the main purpose and description of the module*	The Cybersecurity Essential and Mar *<sector-name>* training module provides and trainees with the knowledge and skil to manage the security of information organisation. The module covers a wi topics as described on the main topics. Th designed to be more practical and ha participants will gain experience in a concepts they learn through a variety of e activities
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a module*	By the end of the training, participants wi • Demonstrate ethical and professiona all aspects of information and c management • Comprehend and articulate the key c principles of information and cyber s • Understand the evolving cyber threa and the diverse range of cyber attacks • Identifies the cybersecurity vulnerabilities, and risks to an organi • Recognises the human factor's cybersecurity breaches and risk strategies • Strategically aims to design and deve information security governance fra risk management aligned with or goals

Syllabus of the Training Module-1: Cybersecurity Essentials and Management for <sector name>

Main topics	Suggested Content
Ethical Conduct and Professionalism in *<sector-name>*	**Introduction to ethics and professional conduct in cyber security**: This section will introduce the concept of ethics and professional conduct in cyber security, and discuss the importance of these principles in the field in *<sector-name>*. **Code of ethics:** This section will discuss the different codes of ethics that are relevant to cyber security in *<sector-name>*, its business activities, and how these codes can be used to guide ethical decision-making. **Professional responsibilities:** This section will discuss the professional responsibilities of cyber security professionals in *<sector-name>*, such as confidentiality, integrity, and availability. **Introduction to legal and ethical aspects of information security:** This section will discuss the laws and regulations that govern information security in *<sector-name>*. It will also discuss the ethical considerations that need to be considered when managing information security. **Legal and regulatory requirements:** This section will discuss the legal and regulatory requirements that apply to cyber security, such as the General Data Protection Regulation (GDPR). **Resolving ethical dilemmas:** This section will discuss how to resolve ethical dilemmas in cyber security, such as when to disclose

CYBERSECPRO

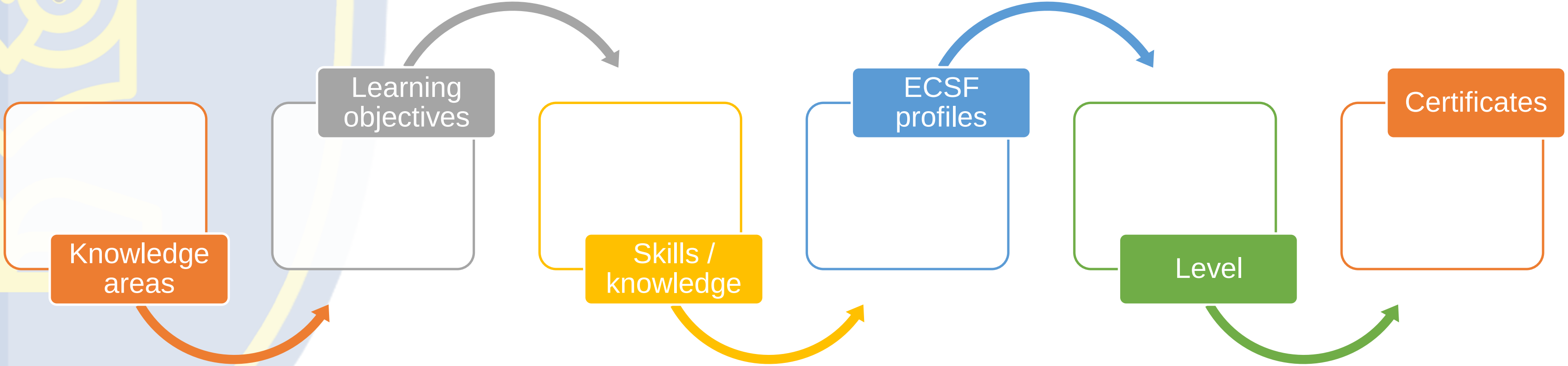
Certificates

Built on the concept of micro-credentials, they include:

- Identification of the learner
- Title of the micro-credential
- Country/Region of the issuer
- Awarding body
- Date of issuing

- Learning outcomes
- Notional workload needed to achieve the learning outcomes
- Level of the learning experience leading to the micro credential (EQF)
- Type of assessment
- CyberSecPro knowledge areas
- Level of training (Basic / Advanced)

Certificates


Knowledge areas
Learning objectives
Skills / knowledge
ECSF profiles
Level
Certificates