ECSF WORKSHOP 2025

AGENDA

TITLE	ENGAGING EU PROJECTS USING THE ECSF
VENUE	THON HOTEL BRUSSELS CITY CENTRE, AVENUE DU BOULEVARD 17, 1210 BRUSSELS
DATE	20-21 NOVEMBER, 2025

DAY 1: THURSDAY 20 NOV 2025		
9.00-9.30	Opening keynotes - EU perspective	**Evangelos OUZOUNIS**, Head of Capacity Building Unit, ENISA **Katarzyna PRUSAK – GÓRNIAK,** Vice-Chairman, Governing Board of the European Cybersecurity Competence Centre (ECCC) **Anne Sophie DIEHL**, Policy Officer, European Commission **Giuseppe ZUFFANTI**, Coordinator for Cyber issues and for the Cyber ETEE Platform, European Security & Defence College (ESDC) **Ruxandra GHEORGHESCU,** European Cybersecurity Competence Centre (ECCC)
9.30-10.30	Inspiring Talks (15'each)	
	ECSF & its strategic approach	**Fabio DI FRANCO,** ENISA
	Cybersecurity Educator profile: Awareness Raising in a Box	**Christina Skouloudi,** ENISA
	Cybersecurity in the Bulgarian Vocational Education System	**Yasen Tanev,** dihtrakia.org
	CyberHubs: Actionable Roadmap for Closing National Cybersecurity Skills Gaps in alignment with the ECSF	**Jutta Breyer,** Breyer Publico, member of the AHWG on the ECSF **Antonela Bardhoku**, DigitalEurope
10.30-11.00	Coffee Break	
11.00 -12.20	Inspiring Talks	
	NERO results inspired by ECSF (20')	**Kitty Kioskli & Eleni Seralidou,** trustilio **Pedro Thomas,** ONESOURCE
	Demo from NERO marketplace (5')	**Wissam Mallouli,** Montimage
	CYberSynchrony and ECSF (25')	**Violeta Vasileva,** Maggioli **Demetris Antoniou,** Ianus Technologies

	CyberSecPro: training courses aligned to ECSF (15') **ECSF & product security** (15')	**Chatzopoulou Argyro,** Apiroplus Solutions, member of the AHWG on the ECSF **Jetzabel Serna,** Cyber4People, member of the AHWG on the ECSF
12.20–12.50	**Fireside chat** Facilitator: **Christina Skouloudi,** ENISA	**Mette Svensson,** kth.se & https://cyberbridgeforum.com/ & Cybercampus, Sweden **Joanna Kulesza,** Cybersecurity and International Law, University of Lodz, Poland & ESDC member **Annalisa Andaloro,** 28DIGITAL & CYCERONE
12:50	Family picture	
12.50–14.00	Lunch Break	
14.00-15.40	Hands-on Interactive Exercise: 4 Breakout sessions - Showcase how each contributor's work contribute to closing the skills gap - Map ongoing & planned initiatives to objectives and actions - Helping identify overlaps, gaps, synergies, and future priorities **Introduction: Fabio DI FRANCO & Marianna KALENTI, ENISA** Each Breakout session will focus to a thematic area as indicated below: 1. **Designing and Delivering Training Activities for Specific Workforce Sectors** Moderated by *Jetzabel Serna & Alina Taralunga* 2. **Designing and Delivering Horizontal Training and Education Initiatives** Moderated by *Nineta Polemi, Eleni Seralidou & Antonio Nevado* 3. **Analysis of Cyber Skills Gaps in the Workforce** Moderated by *Jutta Breyer & Aleksandra Malecka* 4. **Types of Cyber Skills Certificates** Moderated by *Chatzopoulou Argyro & Paolo Atzeni*	

	Projects (alphabetically)	**Contributors** (alphabetically)
	▪ AKADIMOS ▪ Cadmus ▪ CURIUM ▪ CyberActioning ▪ CyberFort ▪ CyberGuard ▪ CyberHubs ▪ CyberMACS- Erasmus Mundus ▪ CyberSec4OT ▪ CybersecPro ▪ Cybersynchrony ▪ CYBERUS Erasmus Mundus ▪ CYCERONE	▪ Paolo Atzeni, Simon Pietro Romano, Dimitrios Serpanos, Georgios Stergiopoulos ▪ Zlatan Moric, Mark Ruijsendaal, Christos Zaroliagis ▪ Esther Garrido, Elia Giovacchini ▪ Henrique Manuel Dinis Santos ▪ Nikolaos Kekatos ▪ Marios Ioannou ▪ Antonela Bardhoku, Jutta Breyer ▪ Ebru Dilan ▪ Evren Buyer, Orçun Çetin, Esma Dilik, Valerie Mack ▪ Argyro Chatzopoulou, Nineta Polemi ▪ Demetris Antoniou, Violeta Vasileva ▪ Jean Peeters ▪ Annalisa Andaloro, Mette Svensson

	▪ Digital4Security ▪ EU-Inspire ▪ NERO	▪ Razvan Deaconescu ▪ Andreea Catalina SCARLAT, Daniela Tapi, ▪ Luis Cordeiro, Kitty Kioskli, Eleni Seralidou, Wissam Mallouli, Pedro Thomas
15.40-16.00	Coffee Break	
16.00-17.20	Hands-on Interactive exercise: Report back to plenary Moderators and selected contributors will ▪ present the outcomes of the breakout discussions ▪ summarize key findings, identified synergies and gaps ▪ reflect on future priorities and needs	
17.20 – 17:30	Closing Remarks (1st day)	

DAY 2: FRIDAY, 21 NOV 2025		
9.00- 9.40	Opening keynotes- Member States perspectives	**Miguel Ángel Cañada,** INCIBE, Spain **Paolo Atzeni**, Agenzia per la Cybersicurezza Nazionale, Italy **Andreea Catalina SCARLAT,** National Cyber Security Directorate, Romania
	Inspiring Talks (15' each)	
9.40-10.55	**The experience of Portugal: C-Academy** **CADMUS: training courses aligned to the ECSF** **Digital Identity & Trust Services roles and credentials aligned with the ECSF** **CYBERGUARD: Enhancing Maritime Cybersecurity – ECSF role alignment**	**André Filipe dos Santos Silva,** Portuguese National Cybersecurity Centre (CNCS) **Mark Ruijsendaal,** https://securitydelta.nl **Thanos Vrachnos,** Digital Trust Center of Excellence, https://dtcoe.org **Marios Ioannou,** https://columbia-shipmanagement.com
10.55-11.15	Coffee Break	
11.15-11.35	**Fireside chat with AKADIMOS project** Facilitator: **Fabio DI FRANCO,** ENISA	**George Stergiopoulos**, Athens University of Economics & Business, Greece **Paolo Atzeni**, ACN – Agenzia per la Cybersicurezza Nazionale, Italy **Simon Pietro Romano**, Università degli Studi Federico II, Naples, Italy **Dimitrios Serpanos**, CTI, Greece
11.35-12.05	**Panel Discussion: Skills & CRA** Moderator: **Tjabbe BOS**, European Commission	**Nikolaos Kekatos,** Clone-Systems & CYBERFORT **Esther Garrido,** 28DIGITAL & CURIUM **Jetzabel Serna,** Cyber4people (tdc)

12.05 -12.50	**Panel Discussion:** **The importance of aligning Master's programmes with the ECSF** Moderator: **Nineta Polemi**, UPRC	**Razvan Deaconescu,** University POLITEHNICA of Bucharest, Digital4Security Master **Henrique Manuel Dinis Santos,** Cyberactioning & uminho.pt **Jean PEETERS,** CYBERUS Erasmus Mundus **Daniela Tapi,** EU- INSPIRE Master & National Cyber Security Directorate, Romania **Ebru Dilan,** CyberMACS
12.50-13:00	Summary Closing remarks	

Workshop Sponsors

This event is powered by three DEP projects - NERO, CyberSynchrony, and CyberSecPro with support from: Infotrend Co. Ltd, Ianus Technologies Ltd, Maggioli S.p.A., trustilio B.V., and the University of Piraeus Research Center (UPRC).

Hands-on Interactive Exercise: Showcasing ECSF-led Initiatives to Close the Cybersecurity Skills Gap

The purpose of this exercise is to **showcase and discuss how EU-funded projects and initiatives contribute to closing the cybersecurity skills gap**, in alignment with the **European Cybersecurity Skills Framework (ECSF)**.

Each project will contribute to 4 thematic areas:

1. **Designing and Delivering Training Activities for Specific Workforce Sectors**
2. **Designing and Delivering Horizontal Training and Education Initiatives**
3. **Analysis of Cyber Skills Gaps in the Workforce**
4. **Types of Cyber Skills Certificates**

STRUCTURE OF THE EXERCISE

Part 1 – Breakout Discussions

Format: Four parallel breakout groups - one per thematic area

Each group will include:

- Contributors, as listed in the agenda, presenting their relevant work.
- Two moderators, responsible for guiding discussions, maintaining focus, and recording key insights.

STEP 1 – GROUP ALLOCATION

Each contributor will be representing their **entire project**, and the information s/he shares should reflect a **coordinated position agreed** prior to the workshop.

The **list of contributors** assigned to each initial thematic area is provided in the **Annex**.

Contributors will initially attend the **thematic area** they have been assigned to for 30-40 min and afterwards move on to a different thematic area.

The insights collected during the session may feed into **reports.**

Step 2 – Progress Mapping (Post-it Exercise)

A **colour-coded mapping** will be used to indicate each project's progress in meeting the objectives associated to the 4 thematic areas:

Objective 1: Upskill professionals for specific sectors.

Objective 2: Upskill individuals through horizontal and cross-sectoral training and education initiatives.

Objective 3: Measure cybersecurity skills gaps and workforce needs.

Objective 4: Promote interoperable and stackable certificates that support mobility and recognition.

Colour	Status Description
Green	Objective achieved / Deliverables completed
Orange	Objective expected to be reached within 12 months
Red	Objective expected to be reached in more than 12 months

This visual exercise will help identify **projects with similar objectives but different timelines**, encouraging the creation of **synergies and collaboration opportunities**.

STEP 3 – PROJECT CONTRIBUTION

Project information on the 4 thematic areas will be presented as follows:

THEMATIC AREA 1: DESIGNING AND DELIVERING TRAINING ACTIVITIES FOR SPECIFIC WORKFORCE SECTORS

Objective: Upskill professionals in specific sectors.

This thematic area aims to **identify projects that have already upskilled -or plan to upskill -professionals** in one or more specific sectors and to **quantify the number of individuals trained**. Projects that have achieved their objectives will also be invited to **share challenges encountered** and **propose recommendations** for improvement.

Sectors in scope:
Transport, Finance, Health, Public Administration, Energy, Defence, Other.

Information Requested:

1. Number of individuals trained to date per sector.

2. Target number of individuals to be trained by the end of 2026 per sector.

Example — Possible Questions and Short Answers
(Note: Project names and figures below are only used for demonstration purposes.)

Question:
Which projects have developed and delivered training material for the transport sector?

Possible short answers:

- *CyberSecPro* has completed its activities, having trained **500 professionals**, aiming for **700 by end of 2026**.
- *CyberGuard* developed training materials; implementation will start within **12 months** (target: **740 professionals** by 2026).
- *Cadmus* plans to begin delivery **after 12 months**.

Follow-up Questions:

1. What challenges did you encounter when upskilling professionals in this sector?
2. What has been the measurable impact of your training on the workforce?
3. Based on your experience, what **three key recommendations** would you propose to overcome the challenges?

THEMATIC AREA 2: DESIGNING AND DELIVERING HORIZONTAL TRAINING AND EDUCATION INITIATIVES

Objective: Upskill individuals through **horizontal and cross-sectoral training and education initiatives**, supporting the development of cybersecurity professional skills and roles defined in the ECSF.

This thematic area seeks to identify projects that have **trained or plan to train individuals** in one or more **ECSF professional profiles**, and to **quantify participation levels**.

Projects are invited to share:

- The **tools, methods, and approaches** used in their training activities.
- The **measures ensuring suitability, quality, and relevance** of these activities

Information Requested:

1. Which ECSF profiles are targeted by your training activities?
2. What tools and methods are used (e.g. online platforms, simulations, practical labs, testing)?
3. What quality assurance measures are in place?
4. Number of individuals trained to date
5. Target number of individuals to be trained by 2026

Follow-up Questions (for projects reached the objectives):

1. What challenges did you face in delivering cross-sectoral training?
2. What key recommendations would you propose to strengthen **horizontal training initiatives**?

THEMATIC AREA 3: CYBERSECURITY SKILLS GAP ANALYSIS IN THE WORKFORCE

Objective: Analyse cybersecurity workforce needs and skills gaps across the EU.

This thematic area focuses on **workforce demand, supply, and forecasting**, as well as the **methodologies and tools** used to collect and interpret data.

Projects are invited to share:

- Their **scope, tools, and methods** for skills gap analysis.
- **Quantitative indications on data** collected (e.g. number of job postings, survey responses, reports).
- **Challenges and solutions** encountered during the analysis.

Dimensions of Analysis

- **Workforce Demand Analysis** – Identifying skills and roles needs in the labour market.
- **Workforce Supply Analysis** – Mapping availability of skilled cybersecurity professionals.
- **Forecasting Analysis** – Anticipating future demand and supply trends.

Information Requested:

1. What is the **scope** of your workforce needs analysis?
2. Does it focus on a particular sector or professional group?
3. Which **frameworks or taxonomies** have you used (e.g. ECSF, NICE, ESCO, EN16234 e-CF)?
4. Which **methods** were applied (quantitative and qualitative), and **in which numbers**?
5. Have you performed any **supply-side** or **forecasting** analysis?
6. Was your analysis conducted at **EU level** or **country-specific**?
7. What **challenges** did you encounter in measuring the cybersecurity skills gap, and how did you address them?

SCOPE OPTIONS & EXAMPLE METHODS FOR WORKFORCE ANALYSIS

Scope Options:
• Cybersecurity core professionals (ECSF)
• Cybersecurity skills for ICT professionals (e.g Data Administrator, Developer, Systems Administrator, Enterprise Architect, Network Specialist) (e-CF & ICT Role Profiles)

• Transversal cybersecurity skills – basic cybersecurity competences
• Other (please specify)

Example Methods Used:
• Job postings analysis • Surveys / Questionnaires • Expert interviews or focus groups • Labour market reports • Desk research

Example – Illustrative Project Response expected in this thematic area

Project: *CyberHubs*
Focus: Workforce needs analysis for cybersecurity professionals.

CyberHubs conducted a **workforce demand analysis** focused exclusively on **cybersecurity core professionals**, using several frameworks to guide its work — **ECSF**, **NICE skills categories**, and **ESCO soft skills**.
The analysis did not include ICT or transversal cybersecurity skills and neither a particular sector. It covered **six EU Member States**: Belgium, Lithuania, Greece, Hungary, Slovenia, Spain, and Estonia.

Methodology and Tools:
CyberHubs applied a **mixed-method approach** combining job postings analysis, surveys, expert meetings, and desk research. A dedicated tool was developed to continuously monitor job vacancy data. Initial categorisation is performed manually, followed by **AI-supported updates** for ongoing refinement.

Data collection (2024) in numbers:

- **2,612 job postings** analysed to identify demand trends.
- **616 survey responses** from ICT and cybersecurity managers, professionals, and HR representatives.
- **193 papers selected for detailed analysis**
- **7 expert meetings** with a total of **120 participants**, representing employers, training providers, policymakers, and business associations.

Supply and Forecasting:
CyberHubs also analysed the **supply of cybersecurity professionals** by systematic research on qualification offers: 147 learning programmes analysed in total.
A **forecasting model** is currently under development to project future demand and supply dynamics.

THEMATIC AREA 4: TYPES OF CYBER SKILLS CERTIFICATES

Objective: Identify and characterise the **types of certificates** issued by EU-funded projects in cybersecurity skills development.

This thematic area aims to explore how projects design, and structure their certificates and the available information, focusing on how these align with recognised qualification frameworks and the European Cybersecurity Skills Framework (ECSF).
Projects are encouraged to share insights into the types of certificates they issue, their defining characteristics, and how these contribute to the recognition and validation of cybersecurity skills across Europe.

Dimension 1 – Type of Certificate Provided

Does your project issue or plan to issue any of the following?

a. Certificate of completion/of attendance/training
b. Micro-credential
c. Certificate of skills based on a formal assessment
d. Formal education recognized diploma
e. Other (please specify)

Dimension 2 – Key Characteristics of the Certificate

(*Note: Formal education diplomas do not need to complete this part.*)

Please indicate which of the following characteristics are included in your certification.
Consider that the information may not appear directly on the certificate itself but could be part of an associated data model.

Please indicate which of the following characteristics are included in your certification.
Consider that the information may not appear directly on the certificate itself but could be part of an associated data model.

Characteristic	Yes/No
1. Date of issuance	
2. Defined learning outcomes	
3. Workload (e.g. expressed in ECTS)	
4. Level of learning experience (e.g. EQF level)	
5. Type of assessment applied	
6. Mode of participation (e.g. online, blended, in-person)	
7. ECSF profile(s) covered	
8. Authenticity or validity check	
9. Other (please specify)	

Follow-up Questions:

1. What are the main challenges your project encountered when defining or issuing certificates?
2. How do you ensure consistency, recognition, and quality of the certificates issued?
3. Based on your experience, what recommendations would you propose to improve the interoperability and recognition of cybersecurity certificates across Europe?

Part 2: Reporting and Wrap-up

Format: Plenary sessions

- The session will conclude with a **summary of key findings**, **challenges encountered in achieving the objectives**, and **recommendations for future action**.
- **Moderators** will present the main outcomes and insights from each breakout discussion.
- They may also **invite contributors** to complement specific points.

Annex: List of contributors assigned to the initial thematic area

Project	Full Name	ASSIGNED THEMATIC AREA
AKADIMOS	Dimitrios Serpanos	2
AKADIMOS	GEORGIOS STERGIOPOULOS	3
AKADIMOS	Simon Pietro Romano	4
Cadmus	Christos Zaroliagis	1
Cadmus	Mark Ruijsendaal	3
Cadmus	Zlatan Moric	4
CURIUM	Esther Garrido	1
CURIUM	Elia Giovacchini	3
CyberActioning	Henrique Manuel Dinis Santos	2
CyberFort	Nikolaos Kekatos	1
CyberGuard	Marios Ioannou	1
CyberHubs	Antonela Bardhoku	3
CyberMACS - Erasmus Mundu	Ebru Dilan	2
Cybersynchrony	Demetris Antoniou	1
Cybersynchrony	Violeta Vasileva	3
CYBERUS Erasmus Mundus	Jean PEETERS	2
CYCERONE	Mette Svensson	2

CYCERONE	Annalisa Andaloro	4
Digital4Security	Razvan Deaconescu	2
Eu-Inspire	Daniela Tapi	2
Eu-Inspire	Andreea Catalina SCARLAT	4
Nero	Kitty Kioskli	1
Nero	Luis Cordeiro	2
Nero	Wissam Mallouli	3
Nero	Pedro Thomas	4
CyberSec4OT	Evren Buyer	1
CyberSec4OT	Valerie Mack	3
CyberSec4OT	Orçun Çetin	4