



advan**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

NERO contributes to ECSF implementation

November 20th, 2025, ENISA European Cybersecurity Skills Workshop

Dr Kitty Kioskli, kitty.kioskli@trustilio.com (trustilio)

Dr Eleni Seralidou, eleni.seralidou@trustilio.com (trustilio)

Wissam Mallouli, wissam.mallouli@montimage.eu (Montimage)

Pedro Tomas, pedro.tomas@onesource.pt (OneSource)



Aim of Presentation

To showcase **implementation** aspects of ECSF within NERO Project's training and tool integration workflows.



NERO project



advanced cybersecurity
awareness ecosystem for SMEs

Call: DIGITAL-ECCC-2022-CYBER-03

Topic: DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS

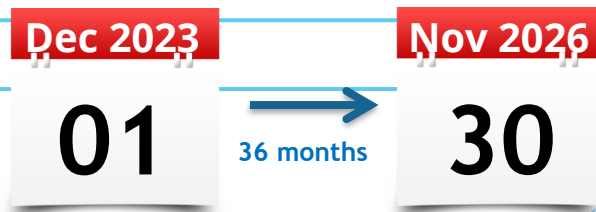
Grant Agreement No: 101127411

Type of Action: DIGITAL JU SME Support Actions

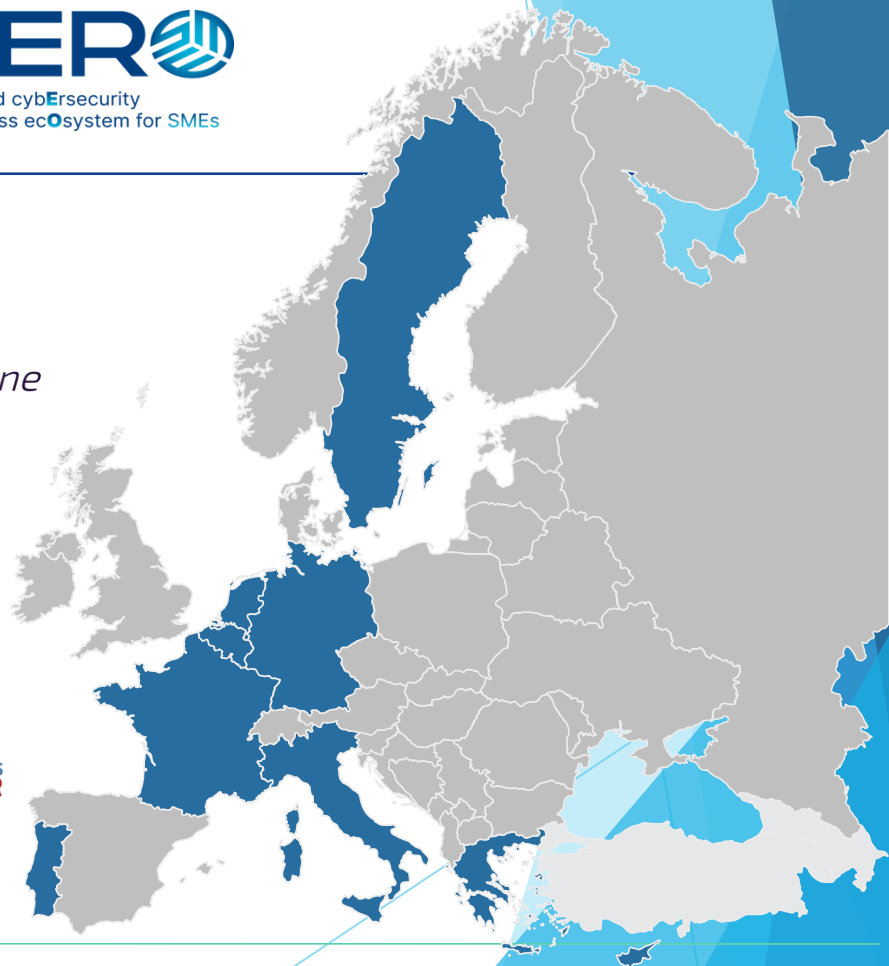
Funding 75%

Requested from the EU: 4,284,604.45 €

Total Cost: 5,955,697.47 €



Consortium



Objectives

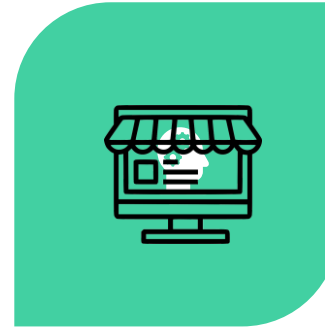


- Strengthen market-driven cybersecurity capabilities by providing the **NERO marketplace** that offers tools, **training**, and hands-on **testing experiences**.
- Enable cybersecurity professionals to acquire the **ECSF-aligned competencies** required to perform effectively in their roles.

NERO main outcomes



**CYBERSECURITY AWARENESS
ECOSYSTEM**



**USER FRIENDLY
MARKETPLACE – TRAININGS
PLATFORM**

ECSF and NERO

- **ECSF by design:** NERO's training modules offer practical skills required by ECSF. The curricula are developed to equip diverse cybersecurity professional profiles with ECSF-defined skills and competencies.
- **ECSF Integration Points:** We use ECSF as a tool to map:
 - **Curriculum Design:** Ensuring modules cover technical and soft skills required by industry.
 - **Competence Gap Assessment:** Measuring pre- and post-training knowledge acquisition.
 - **Solution Development:** Defining tool requirements based on the needs of ECSF roles.



Policy Relevance to ECSF and Ecosystem Fit

- NERO reinforces EU objectives by contributing to the capacity building efforts of the **ECSF**.
- NERO partners actively support the goals of the **Cybersecurity Skills Academy** and **ENISA** ECSF activities (ad-hoc working group, workshops).
- NERO's focus on Auditing and Vulnerability Management helps SMEs comply with **NIS2** and the **Cyber Resilience Act (CRA)**.



NERO skills for ECSF professionals

NERO Training Modules

- 🧩 **Module 1:** Fundamentals of Cybersecurity
- 🚒 **Module 2:** Cyber Threats
- 🎭 **Module 3:** Social Engineering
- 🌐 **Module 4:** Network Security & Pen Testing for SMEs
- 💻 **Module 5:** Software Security
- 🕵️ **Module 6:** Intrusion Detection Systems
- 🛡️ **Module 7:** Privacy & Protection Enhancing Techniques
- 🎯 **Module 8:** Cyber Ranges
- 🎮 **Module 9:** Gamification

Support ECSF Profiles

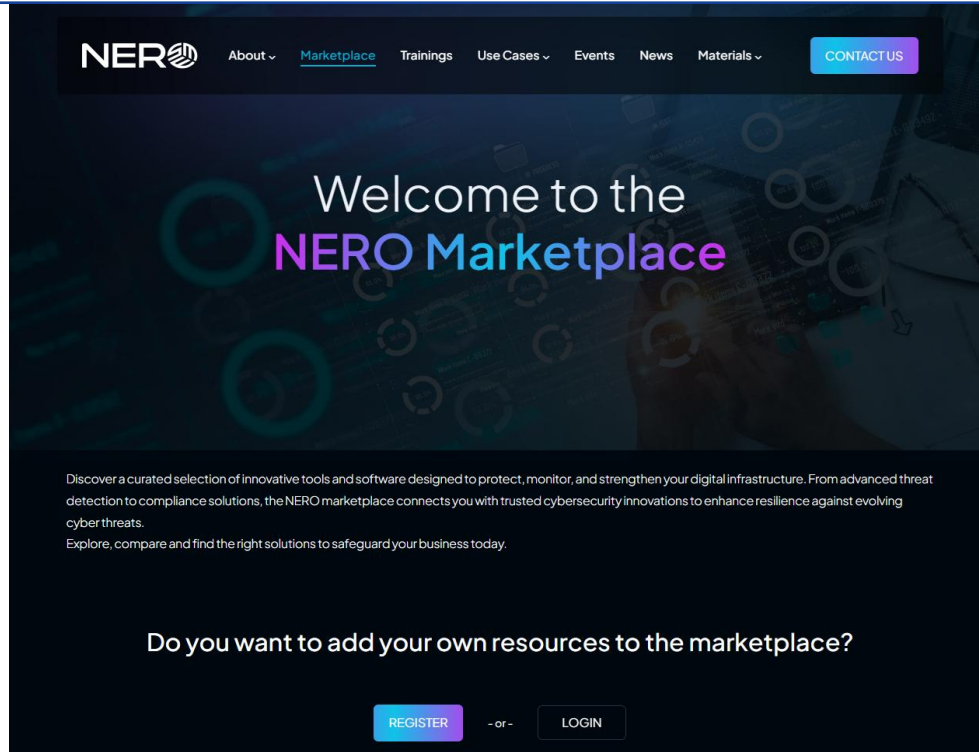
- 🎓 **Cybersecurity Educator** • Cybersecurity Implementer
- 🔍 **Cyber Incident Responder** • Digital Forensics Investigator
- 🧪 **Cybersecurity researcher** • Cybersecurity Educator
- 🔪 **Penetration Tester** • Cybersecurity Architect • Cyber Threat Intelligence Specialist
- ⚙️ **Cybersecurity Implementer** • Cybersecurity Auditor
- 🔍 **Cyber Threat Intelligence Specialist** • Cyber Incident Responder
- ⚖️ **Cyber Legal, Policy & Compliance Officer** • Cybersecurity Architect
- 🏢 **Chief Information security officer** • Cybersecurity Educator
- ⚠️ **Cybersecurity Risk Manager** • Cybersecurity Implementer



More info from Pedro
Tomas!

<https://lms.nerocybersecurity.eu/>

ECSF Mapping to NERO Marketplace



Live Demonstration
from Wissam Mallouli!

<https://nerocybersecurity.eu/marketplace>

ECSF Impact

- **Clustering:** NERO successfully clustered and collaborated with **over 20 distinct EU-funded projects** (e.g., CyberSecPro, CyberSynchrony).
- **ECSF as a Blueprint:** NERO can be positioned as a "**blueprint for ECSF operationalization**", aiding peer institutions in creating comparable skills programs.



NERO demonstrates the ECSF in real deployment



Strategic
design

Integrated
training

Quantifiable
skill
measurement

*We reinforce ENISA's goal of skills alignment
and workforce transparency*

Our Published Research

Rathod P, Rajamäki J, **Kioskli K**. Implementing the European Cybersecurity Skills Framework (**ECSF**): A Case Study of EU Innovation Projects. (2024) ECCWS, 24(1). <http://bit.ly/4l6ym1J>

Rathod P, **Polemi N**, Letho M, **Kioskli K**, Wessels J, Lugo R. (2024). Leveraging the European Cybersecurity Skills Framework (**ECSF**) in EU Innovation Projects: Workforce Development through Skilling, Upskilling and Reskilling. IEEE Global Engineering Education Conference (EDUCON 2024). Kos Island Greece, pp. 1-9. DOI: 10.1109/EDUCON60312.2024.10578846.

Polemi N, **Kioskli K**. Enhancing practical cybersecurity skills: The **ECSF** and the CyberSecPro European Efforts. In proceedings of the 14th International Conference on Applied Human Factors and Ergonomics (AHFE2023)/Track: 'Human Factors in Cybersecurity', July 20-July 24, 2023, San Francisco, California, USA.

Thank you!



advanCed cybERsecurity
awaReness ecOSystem for SMEs

VISIT US

VISIT US

NERO: <https://nerocybersecurity.eu/>



Dr Kitty Kioskli

Project Manager at trustilio B.V.
kitty.kioskli@trustilio.com

Dr Eleni Seralidou

Co-Project Manager at trustilio B.V.
eleni.seralidou@trustilio.com

NERO Training Methodology

Pedro Tomás, OneSource

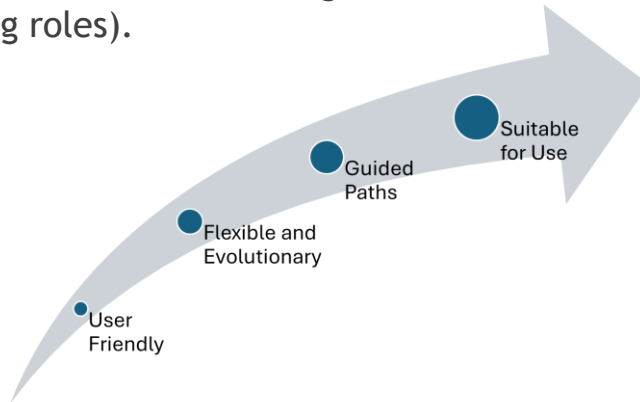
NERO Training methodology & details

Outline:

- ▶ Training methodology
 - ▶ Training strategy
 - ▶ Course Management
 - ▶ Modules and Syllabus
 - ▶ Training Evaluation
-

Training Methodology

- ▶ **User Friendly:** Clear syllabus and well-structured training materials.
- ▶ **Flexible:** Modular design with adaptable content and ongoing updates.
- ▶ **Guided Paths:** Tailored modules to meet specific industry needs.
- ▶ **Suitable for Use:** Practical content aligned with current enterprise demands (i.e., ECSF profiling roles).



Training Strategy



Relevance

Focusing on the most pertinent cybersecurity issues that SMEs face, ensuring that the training content is directly applicable to their operational context



Practicality

Emphasizing hands-on learning and real-world application to ensure that trainees can effectively implement cybersecurity measures



Accessibility

Designing the training to be easily accessible, both in terms of cost and delivery methods, to accommodate the limited resources of SMEs



Scalability

Providing flexible training solutions that can grow with the organisation as its cybersecurity needs evolve

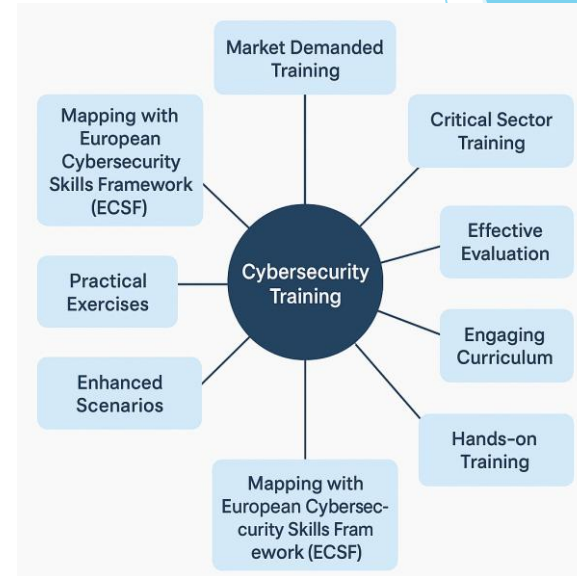


Alignment

NERO Trainings were designed considering ENISA ECSF role profiles

Training Objectives

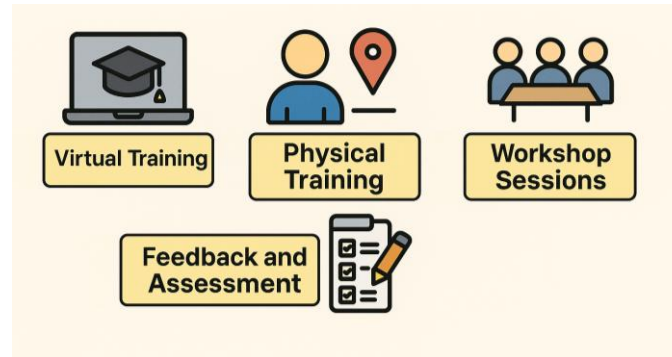
- ▶ Cybersecurity Training
- ▶ Market Demanded Training
- ▶ Critical Sector Training
- ▶ Effective Evaluation
- ▶ Engaging Curriculum
- ▶ Hands-on Training
- ▶ Gamified Learning
- ▶ Enhanced Scenarios
- ▶ Practical Exercises
- ▶ Mapping with European Cybersecurity Skills Framework (ECSF)



Course Management

NERO provides the training through a hybrid training approach:

- ▶ Virtual Training
 - ▶ Moodle Platform
 - ▶ Interactive Training Sessions
- ▶ Physical Training
 - ▶ Target Audience
 - ▶ Venue/Location
 - ▶ Schedule
 - ▶ Invitations/Registrations
- ▶ Workshop Sessions
- ▶ Feedback and Assessment



Modules and Syllabus

- ▶ Independent modules
- ▶ Tailored to broad audiences (experts and non-experts)
- ▶ Each module includes hands-on training supported with different NERO's tools

#	Title	Syllabus Overview	ECSF Profiles
1	Fundamentals of Cybersecurity	Cybersecurity basics, history, CIA triad, frameworks (NIST, ISO), threat types	Cybersecurity Implementer, Cybersecurity Risk Manager, Cyber Legal, Policy and Compliance Officer
2	Cyber Incidents and Incident Handling	Incident types, handling procedures, roles, detection and response techniques	Cyber Incident Responder, Digital Forensics Investigator, Cyber Threat Intelligence Specialist
3	Social Engineering	Psychological tactics, phishing, spear phishing, awareness strategies	Cyberthreat Intelligence Specialist, Cybersecurity Risk Manager
4	Network Security & Penetration Testing for SMEs	Firewall config, secure protocols, network scanning, basic pen-testing	Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cybersecurity Architect, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Risk Manager, Penetration Tester.
5	Software Security	Secure coding, common vulnerabilities (OWASP), patching, lifecycle management	Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cybersecurity Architect, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Risk Manager, Penetration Tester, Cybersecurity Auditor.
6	Intrusion Detection Systems (IDS)	IDS/IPS fundamentals, deployment, alert handling, tuning	Cyber Incident Responder, Cybersecurity Architect, Cybersecurity Implementer, Digital Forensics Investigator, Cyber Threat Intelligence Specialist
7	Privacy & Protection Enhancing Techniques	GDPR basics, anonymization, pseudonymization, privacy by design	Cybersecurity Architect, Cybersecurity Implementer, Chief Information Security Officer (CISO), Cyber Legal, Policy and Compliance Officer
8	Cyber Ranges Training and Exercises	Simulated attack/defense scenarios, team-based challenges	Cyber Incident Responder, Penetration Tester, Cyber Threat Intelligence Specialist, Cybersecurity educator, Digital Forensics Investigator
9	Gamification-Based Cybersecurity	Scenario-based learning, badge/score system, interactive feedback loops	Cybersecurity Implementer, Cybersecurity Risk Manager, Cyber Legal, Policy and Compliance Officer

Training Evaluation

- ▶ Pre and post-training evaluation questionnaires
- ▶ Questionnaires analysis to assess training performance
- ▶ Continuous evolution assessment
- ▶ Example of training sessions
 - ▶ CyberHot 2024
 - ▶ Train-the-trainers
 - ▶ Training Round I
 - ▶ CyberHot 2025

Cyber-security Awareness & Hygiene

What is a good example of cyber-hygiene practices? *

- ☐ Keep a clean desk, without sensitive information visible
- ☐ Use a password manager
- ☐ Being alert for suspicious emails, attachments, and hyperlinks
- ☐ Don't use the personal mobile to handle professional information
- ☐ All of the above

What kind of password do you think is the most secure for accounts and devices? *

- ☐ One word that is meaningful to the user
- ☐ A long list of random words combined with numbers and symbols
- ☐ A series of numbers, such as a telephone number, that is meaningful to the user
- ☐ A short, easy to remember combination of random words and symbols

Which is the best way to protect against viruses or other security threats? *

- ☐ Hire a new company that has made the effort to alert you to viruses on your system and offers to help you fix them.
- ☐ Install new virus protection software that you find online.
- ☐ Change the network password.
- ☐ Call your security software company to review the steps it has taken to set up virus protection and what else it has done or can do to protect your business.



advan**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

ONE SOURCE

Consultoria Informática Lda.

Thank you!

Pedro Tomás, OneSource
pedro.tomas@onesource.pt



NERO Website

<https://nerocybersecurity.eu/>

NERO Socials:



YouTube



LinkedIn



X