

CONNEXUS

black sea tech forum

Cybersecurity
for Industry
4.0
Technologies
in Operational
Technology

CyberSec4OT
DEP project



Под патронажа на президента на
Република България г-жа Илияна Йотова

ЧЕРНОМОРСКИ ТЕХНОЛОГИЧЕН ФОРУМ

Hristian Daskalov, PhD



5 - 7 Октомври 2026

Варна



ARCFUND

Reason for the cross-border partnership

The CyberSec4OT project at cysec4ot.com addresses the growing challenges posed by the convergence of Information Technology (IT) and Operational Technology (OT) in the context of Industry 4.0. **The rapid integration of digital technologies into production systems has exposed OT systems to increased cybersecurity risks**, including cyberattacks, data breaches, and operational disruptions.

Europe faces a severe shortage of trained cybersecurity professionals—approximately 200,000 experts are needed to safeguard OT environments. These challenges necessitate a robust initiative to upskill and reskill individuals in OT cybersecurity to support industries in adapting to the digital transformation and improving resilience against cyber threats



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

Arçelik



National Technical
University of Athens



POLITÉCNICA

Purpose of the joint project

- Train individuals with technical and non-technical backgrounds to address OT cybersecurity challenges.
- Close the workforce shortage in cybersecurity, particularly in OT systems.
- Strengthen companies' capabilities to combat cyberattacks in Industry 4.0 environments.
- Develop a sustainable training ecosystem for cybersecurity awareness and skills enhancement.
- Align with the European Commission's **Cybersecurity Skills Academy** and Digital Decade Policy Program 2030.
- Increase **compliance with EU cybersecurity regulations such as the NIS2 Directive and Cyber Resilience Act**



Summary of activities (1)

Dissemination and Communication:

- Develop a communication strategy
- 6 Webinars on OT cybersecurity
- Organize a hybrid conference on the subject

Needs Assessment:

- Surveys with 100+ companies (per partner!) and focus group meetings to identify cybersecurity needs.
- Gap analysis of existing frameworks and training programs.

Curriculum Development:

- Design modular training programs for both online and in-person delivery.
- Create specialized modules such as Malware analysis, Secure Coding, and Penetration Testing for OT systems.



1,160

Participants reached

▼ **815**

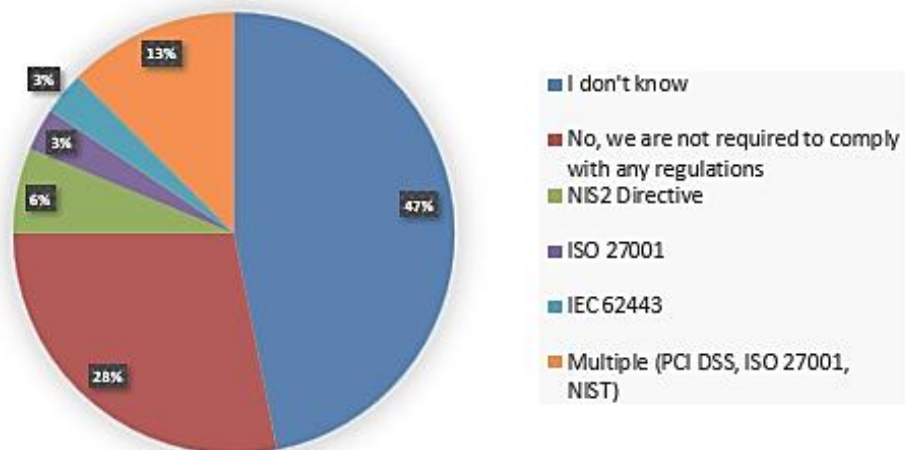
Completed responses

720

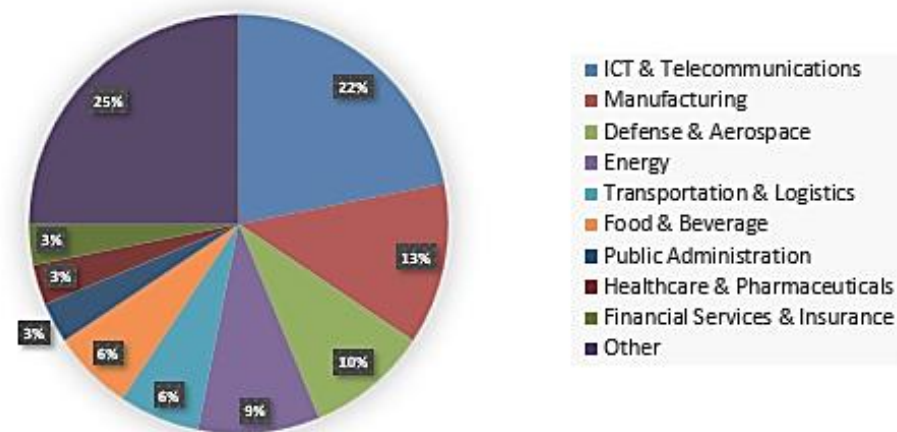
Final validated dataset

General information

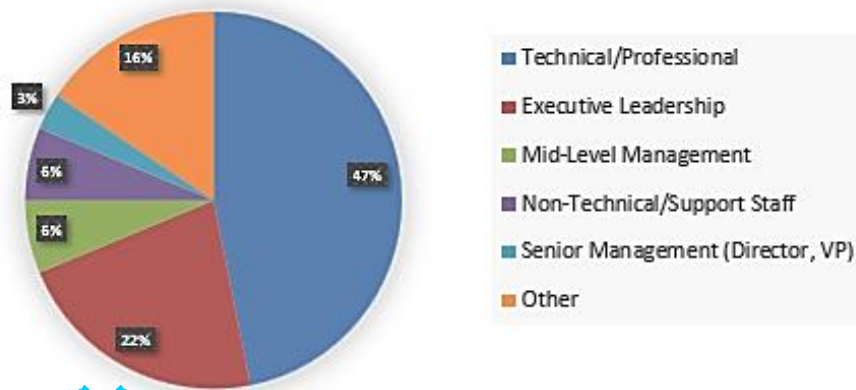
OT Cybersecurity Regulation Compliance



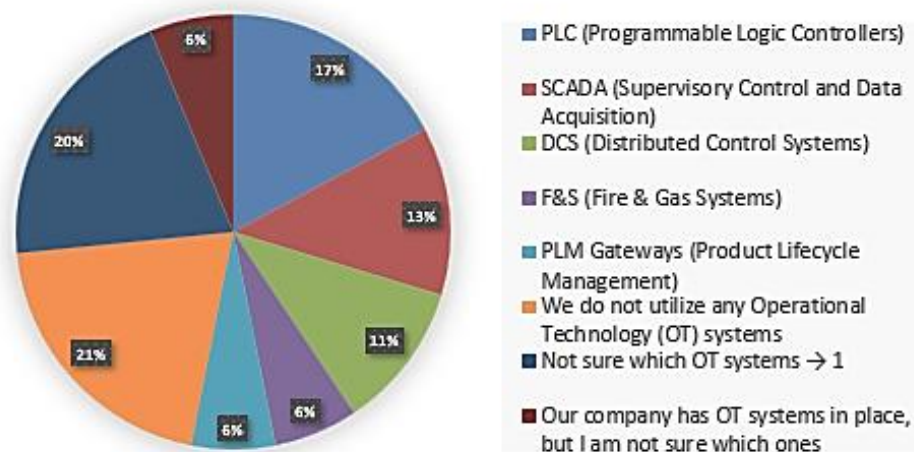
Industry Categories



Respondent Roles in the Organization

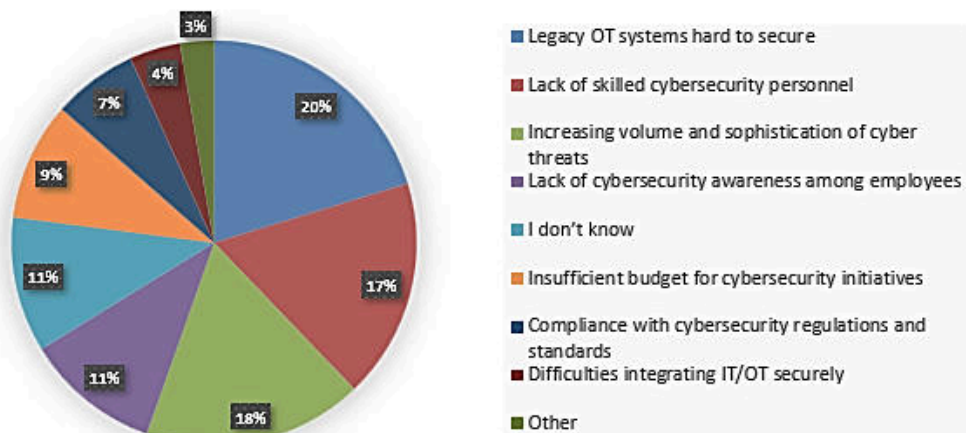


Types of OT Systems in Use

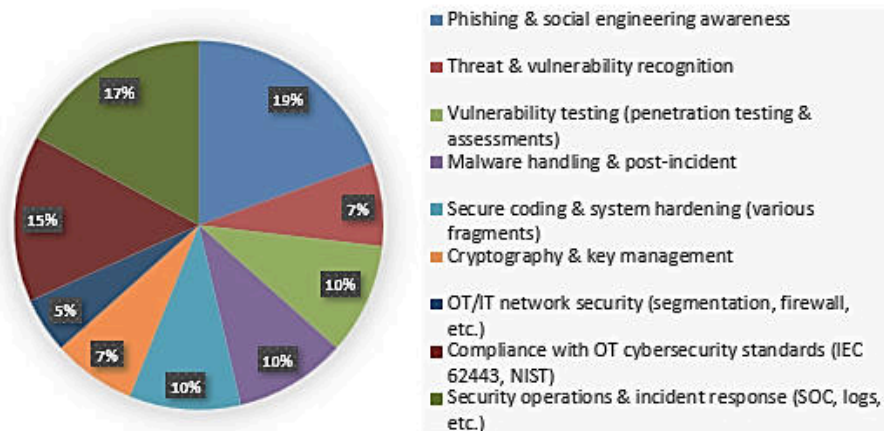


General observations

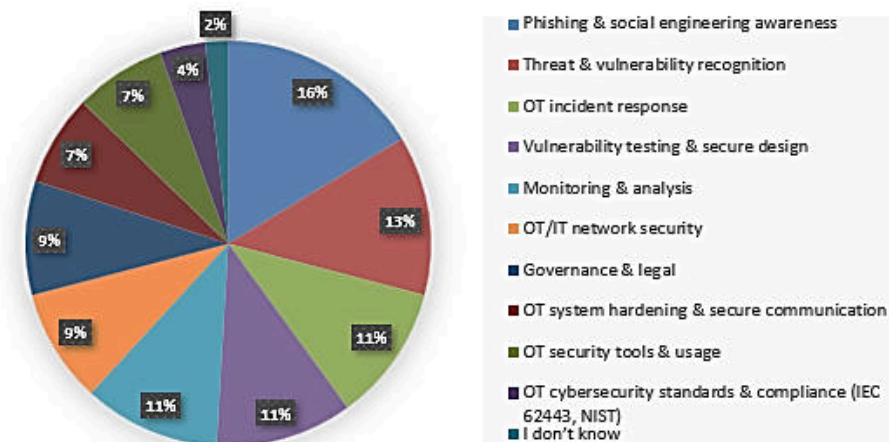
Cybersecurity Challenges in OT Environments



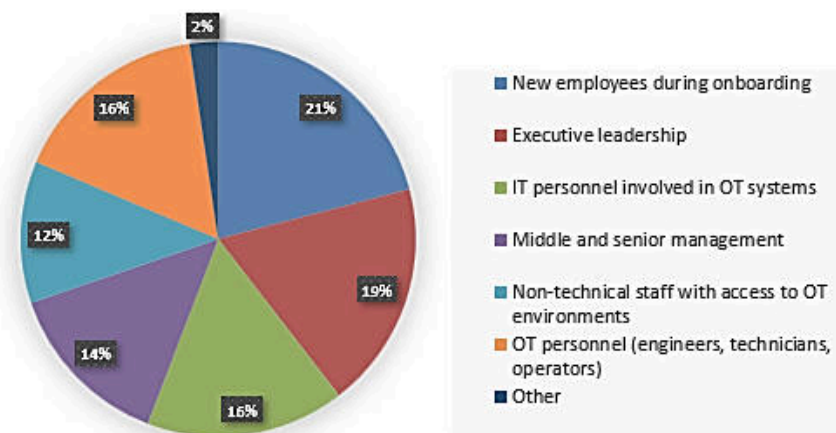
Future Training Needs in OT Cybersecurity



Gaps in OT Cybersecurity Training



Target Groups for Future OT Cybersecurity Training



Summary of activities (2)

Training Implementation:

- At least 200 people, including at least 50 women, will participate in online training.
- At least 100 people, of which at least 25 women in face-to-face training
- Conduct "train-the-trainer" programs for 30 individuals.
- Five online training programs in EU languages in the Digital Skills & Jobs Platform and/or ENISA's CyberHEAD database.

Workshop Series:

- Organize 15 workshops addressing specific OT cybersecurity challenges.
- At least 150 people will participate in the workshops; 30 of these will be women

Evaluation and Certification:

- At least 70 trainers get certificate
- Assess learning impacts and facilitate international certifications for successful participants.

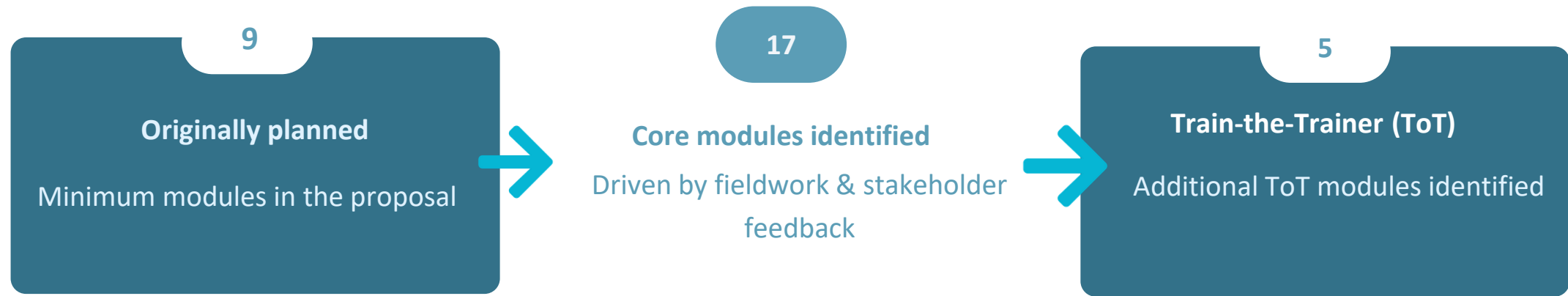


Training Contents

- Cyber forensics
- Cyber ranges
- Malware analysis
- AI for cybersecurity
- Fundamentals of Computing and Operational technologies
- Network Security and Cryptography
- Risk Management and Cybersecurity
- Penetration Testing for Operational Technology
- Malware analysis and incident response
- Secure Coding, and Software Security for OT training



STAKEHOLDER FEEDBACK ON CURRICULUM DEVELOPMENT



Why the structure expanded

Fieldwork findings demonstrated the need for a broader, differentiated structure. Seventeen technical and professional modules and a five-module Train-the-Trainer track were identified — an expansion driven directly by stakeholder feedback and survey evidence rather than assumption.

The Stakeholder Feedback Report on Curriculum Development is based on the initial stakeholder feedback collected in the early engagement phase. The WP3 and WP4 feedback cycles were later rescheduled and differed slightly in content, and are therefore reported separately as a complement to — not a replacement for — the findings presented here.

PART I — FOUNDATIONAL & INTRODUCTORY MODULES

Entry-level to intermediate modules supporting non-technical staff, managers and OT-transitioning roles.

Module	Duration	Target Audience	Sequence	ENISA Profile	Delivery
Introduction to Cybersecurity in OT	1 day	All participants	Day 1	Awareness Level	In-person / Online
Fundamentals of Computing & OT Technologies	1 day	Technical staff, engineers, IT	Day 2	Security Architect / Engineer	In-person
Introduction to Cyber-Forensics	1.5 days	SOC analysts, security teams	Wk 1–2	Cyber Incident Responder	In-person
AI for Cybersecurity (Introduction)	1 day	Analysts, SOC, technical	Wk 2–3	Emerging Tech & Threat Intel	In-person / Online
Standards & Frameworks Implementation	1 day	Compliance officers, managers	Wk 2–3	GRC Specialist	In-person / Online
Policy & Compliance for Decision-Makers	1 day	Executives, managers	Wk 2–3	Governance, Risk & Compliance	In-person / Online
Risk Management & Cybersecurity (Intro)	1.5 days	Risk officers, security managers	Wk 3–4	GRC Specialist	Hybrid / In-person
Human Factors & Cybersecurity Awareness	0.5 day	All profiles	Flexible	All profiles	In-person / Online
Data Protection & Privacy in OT Systems	1 day	Legal, compliance, management	Wk 3–4	Data Protection / Legal	In-person / Online
Cyber Hygiene & Best Practices	0.5 day	All profiles	Annual	Awareness Level	In-person / Online

PART II — ADVANCED & SPECIALIZED MODULES

Specialist tracks for cybersecurity professionals, engineers and technical experts.

Module	Duration	Target Audience	Sequence	ENISA Profile	Delivery
Advanced Computing & OT Systems	2–3 days	OT engineers, system integrators	Wk 1	Security Architect / Engineer	In-person (labs)
Network Security & Cryptography	3 days	Network engineers, specialists	Wk 2–3	InfoSec Analyst / Security Eng.	In-person (labs)
Cyber Range Simulation	3–5 days	SOC analysts, responders	Wk 4–6	Incident Responder	In-person only
Risk Management (Advanced)	2–3 days	CISOs, risk managers	Wk 2–4	Risk Manager / InfoSec Manager	Hybrid / In-person
Penetration Testing for OT	4–5 days	Pen testers, red teams	Wk 5–8	Vulnerability Assessor	In-person (sandbox)
Malware Analysis & Incident Response	4–5 days	Analysts, responders	Wk 6–10	Incident Responder / Forensics	In-person (labs)
Secure Coding & Software Security for OT	3–4 days	Developers, DevSecOps, AppSec	Wk 3–8	Secure Software Developer	Online / In-person

TRAIN-THE-TRAINER (TOT) PROGRAMME

Five additional ToT modules identified to build sustainable in-house training capacity.

ToT Module	Duration	Dependency	Target Audience	Timing	Delivery
Designing & Delivering Cybersecurity Awareness Programs	2–3 days	Strong	HR trainers, awareness leads	Month 21–30+	In-person (workshop)
Advanced Incident Response Leadership	3–4 days	Critical	SOC leads, security managers	Month 32–36	In-person (tabletop)
Cybersecurity Risk Culture & Communication	2–3 days	Strong	Risk managers, compliance leads	Month 30–36	Hybrid / In-person
Tailoring Standards & Frameworks into Training	2–3 days	Strong	Compliance trainers, auditors	Month 32–36	Online
Curriculum & Pedagogy for OT Cybersecurity	2–3 days	Strong	Lead trainers, course designers	Month 30–36	Hybrid

Thanks for the attention!

[linkedin.com/in/Hristian](https://www.linkedin.com/in/Hristian)



Funded by
the European Union

This project has received funding from the European Union under the Digital Europe Programme (GA 101083531) managed by the European Health and Digital Executive Agency (HADEA) of the European Commission. 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.



Под патронажа на президента на
Република България г-жа Илияна Йотова

ЧЕРНОМОРСКИ ТЕХНОЛОГИЧЕН ФОРУМ
Hristian Daskalov, PhD

