



CyberSec4OT

Cybersecurity for
Industry 4.0 and Operational Technology

NEWSLETTER

March 2025

The rapid evolution of Industry 4.0 has transformed manufacturing and industrial processes, but it has also introduced unprecedented cybersecurity challenges. The increasing reliance on interconnected systems, including Information Technologies (IT), Industrial Internet of Things (IIoT), Industrial Control Systems (ICS), and Operational technology (OT) has created new vulnerabilities, making industries more susceptible to cyber threats. The **CyberSec4OT** project was initiated to tackle these pressing concerns by equipping professionals with the expertise needed to protect critical infrastructure.

CyberSec4OT aims to close the cybersecurity skills gap, enhance industry resilience, and contribute to the EU's broader digital security goals.

As digital transformation accelerates, the integration of IT, IIoT, ICS, and OT has led to new vulnerabilities. **CyberSec4OT** is designed to combat these threats by developing tailored training programs and hands-on workshops that bridge the cybersecurity skills gap across Europe.



What to Expect?

- ✓ Customized Cybersecurity Training: Online and in-person courses tailored to industry needs.
- ✓ Engaging Workshops: Practical, job-training sessions addressing real-world cybersecurity challenges in OT.
- ✓ Certification & Career Development: Participants will receive recognized certifications to boost employability and expertise.

Key Objectives

- ✓ Train and upskill professionals in cybersecurity for OT, catering to both technical and non-technical backgrounds.
- ✓ Develop industry-aligned curricula, including topics such as Network Security, Risk Management, Penetration Testing, and Secure Coding for OT.
- ✓ Deliver practical learning experiences through workshops and real-world case studies to prepare individuals for emerging cybersecurity challenges.
- ✓ Address gender disparity in cybersecurity by encouraging female participation and leadership in OT security roles.



Co-funded by
the European Union



This project has received funding from the European Union under the Digital Europe Programme.