Cyber Security Training on Operational Technology Resilience
2022-1-AT01-KA220-VET-000087608

Co-funded by the European Union

Newsletter No. 3

CSecTOR – PROTECTING OUR INDUSTRIAL SMEs

CSecTOR (Cyber Security Training on Operational Technologies Resilience) is an innovative project financed by the Erasmus+ program of the European Union which addresses a topic, that of the cybersecurity of operational technologies (OT) often overlooked by both sector experts and political decision-makers.

Plans, projects, training or awareness-raising actions, etc. they focus on the IT security of networks, or, better said, on preventing cyber-attacks, theft or misuse of data while using the internet for work or entertainment purposes.

Yet in an increasingly interconnected and digitalized world, even operational technologies can be the subject of cyber-attacks capable of compromising critical infrastructures and interrupting production operations.

The CSecTOR project addresses this important challenge with a set of actions and tools that we briefly describe below

ATTACKS ON OT AND IT SYSTEMS

KonBriefing (Cyber-attacks worldwide 2022 | KonBriefing.com) carries out an annual survey into cyber attacks that have affected all sectors in all countries around the world, from the USA to China to Europe.

Even just by taking a look at the survey you would immediately understand the importance of cybersecurity of OT systems

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

THE OBJECTIVES OF THE PROJECT

The CSecTOR project addresses digital transformation through developing digital readiness, resilience and capacity of European SMEs, helping them achieve industrial cybersecurity in an easy, understandable and approachable way.

The main expected results are:

1. The creation of **OT Cybersecurity Methodology** to support industrial SMEs in securing their industrial assets and operations
2. Development of the **OT Cybersecurity Training Course** to help companies assess their current level of operational cybersecurity and potential gaps in their security measures, provide training to employees to improve their skills in operational cybersecurity etc.
3. Design and programming of **OT Cybersecurity e-training Platform**
4. **Dissemination** & Exploitation

The primary goal of the project is to help organizations maintain the resilience of their operational technology systems, ensuring that they can continue to function properly in the face of potential cyber threats.

OT security focuses on safeguarding networks and computer systems used in operational environments

FOR MORE INFORMATION

https://csector.eu/project/

FOLLOW US!

Csectorerasmusplusproject

csector

THE PARTNERS OF THE PROJECT

FH Joanneum – University of Applied Sciences, is one of Austria's leading universities of applied sciences

Tournis Symvouleftiky EE is a Greek consulting firm in the areas of Business Resilience, Governance, Risk & Compliance Management, Incident & Crisis Management, Business Continuity Management, Information Security and Privacy Management.

PCX Computers & Information Systems Ltd is a Cypriot SME, with high expertise in applying innovative technology solutions to education

ASSET is an Agency of the Chamber of Commerce of Basilicata

Latvian Chamber of Commerce and Industry (LCCI) is the biggest association of entrepreneurs in Latvia uniting 6000 members – micro, small, medium and large enterprises

Stay in touch with us: in the next newsletter, we will update you on the Methodology Framework!