Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Syllabus

Online Training A004"Lesson learned from Cyber MAR pilots: SCADA system in Port Container terminal"

ADVANCED LEVEL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

COURSE: A004: Lesson learned from Cyber MAR pilots - SCADA system in Port Container terminal

DELIVERY DATE: 08th February 2023

COURSE DESCRIPTION: The training course is designed to provide a high-level overview of the Piraeus Pilot implementation, illustrating how different components of the Cyber-MAR solution are integrated allowing the platform to simulate a complex cyber-attack to the Port Container Terminal, and its impact to the port operations.

The objective is to make learners able to evaluate and plan plausible scenarios in the cyber range.

This training's intended audience is IT personnel, IT managers, cybersecurity personnel, Security Science scientific personnel from Academy.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 30 minutes

PREREQUISITE: OT and SCADA generic skills and knowledge

CONTENTS

1. Piraeus Port Pilot Objectives
2. Targeted Topology Implementation
3. Cyber Kill Chain
4. Cyber-attack execution
5. Impacts and lessons learnt

TRAINING STRUCTURE

The training will be delivered online through zoom.
The attendees will receive an invitation zoom link to join the training once enrolled.

LEARNING OUTCOMES

The participants will develop knowledge and skills necessary to apply the principles of:

- Remain aware of evolving technical infrastructures
- Use critical thinking to analyze organizational patterns and relationships
- How to use network analysis tools to identify vulnerabilities
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications
- Network mapping and recreating network topologies
- Cybersecurity and privacy principles are used to manage risks related to the use, processing, storage, and transmission of information or data
- Specific operational impacts of cybersecurity lapses
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.