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 "Lesson learned from Cyber MAR pilots: Cyber-attack scenario on the Valencia port authority's electrical grid"

INTERMEDIATE 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: Lesson learned from Cyber MAR pilots: Cyber-attack scenario on the Valencia port authority's electrical grid

DELIVERY DATE: 1st December 2021

COURSE DESCRIPTION: The training course is designed to provide a high-level overview of the Valencia Port scenario, implemented as topology in the Cyber Range and the lessons learned through this exercise, both from the viewpoint of the cyber attackers and the cyber defenders.

This course is intended to equip an understanding of how to plan for cyber range scenarios application through the insights gained by implementing an actual topology.

The intended audience is managers who want/have to use the cyber range capabilities to elaborate scenarios for risk analysis and training.
The objective is to make learners able to plan plausible scenarios in the cyber range..

This training's intended audience is IT personnel, IT managers, cybersecurity personnel.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 1 hour

PREREQUISITE: Knowledge of risk management fundamentals

CONTENTS

1. Valencia port pilot: why this scenario
2. From scenario definition to topology implementation: do and don't
3. Blue and Red team insights from the scenario
4. Risk models and impact

✓ Final Training evaluation

TRAINING STRUCTURE

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

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.