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 "Introduction to the Cyber Range (Theory)"

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: Introduction to the Cyber Range (Theory)

DELIVERY DATE: 15th June 2021 – 14:00-16:00 (CET)

COURSE DESCRIPTION: The training course is designed to develop understanding of what a cyber range is, how it works, which are its usages. Also, peculiarities of Cyber-MAR cyber range will be illustrated.

This course is intended to introduce the cyber range concept and components. The specific application in the Cyber-MAR project will be analyzed. An overview of the usages and potentialities of cyber range application to improve cybersecurity knowledge, to train personnel, to create scenarios for risk analysis will be provided.

This training's intended audience is IT and OT personnel as well as IT managers are also part of the intended audience.

The objective is to increase basic knowledge and create solid background of cyber range and its usages.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 2 hours

PREREQUISITE: Proficiency with IT systems and networks administration, knowledge of OT infrastructures pertinent to shipping and ports activities

CONTENTS

1. Cyber Range concept and fundamentals
2. Cyber-MAR components
3. Cyber Range usages overview

   3.1 Risk management through scenarios training

      3.1.1 Offensive security training

3.1.2 Defensive security training

✓ Final Training evaluation

TRAINING STRUCTURE

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

LEARNING OUTCOMES

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

- Application techniques for detecting host and network-based intrusions using intrusion detection technologies Risk management processes
- System and application security threats and vulnerabilities
- Security system design tools, methods and techniques
- Systems diagnostic tools and fault identification techniques
- What constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- Different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)
- Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth)
- Infrastructure supporting information technology (IT) for safety, performance, and reliability
- Penetration testing principles, tools, and techniques
- An organization's threat environment