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

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: **Basic Tools for a Cyber Range**

DELIVERY DATE: 29th November 2021

COURSE DESCRIPTION: The training course is designed to deepen the knowledge of some software tools useful in cyber incident handling.
An overview of the Cyber Range and the Valencia Port scenario is the introduction to the OODA (Observe Orient Decide Act) loop in approaching cyber security incidents; a range of software tools is presented. Network analyzers and their primary usage, SIEM, forensics tools are illustrated to the learners also using videos reproducing typical usage situations. This course is intended to involve the learners in a cyber security incident handling setting.

This training's intended audience is IT, cyber security, and OT personnel.

The objective is to increase basic knowledge of Incident response tools and their use.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 4 hours

Syllabus

Online Training "Basic Tools for a Cyber Range"

INTERMEDIATE LEVEL

PREREQUISITE: good knowledge of TCP/IP networking protocol, routing, proficiency with IT systems and networks administration.

CONTENTS

1. General introduction about Cyber Range
2. Basic topology of how to
3. Valencia port case topology
4. The OODA (Observe Orient Decide Act) loop
5. Software tools useful in incident response with examples

✓ 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:

- Application of techniques for detecting host and network-based intrusions using intrusion detection technologies
- System and application security threats and vulnerabilities
- Security system design tools, methods, and techniques
- What constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- Perform analysis of log files from various sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.

- Network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth)
- The infrastructure supporting information technology (IT) for safety, performance, and reliability
- Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such warnings.
- An organization’s threat environment