**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 "Using a Cyber Range to Understand risk (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:** Using a Cyber Range to Understand risk (Theory)

**DELIVERY DATE**: 15th June 2021 – 16:00 -18:00 (CET)

**COURSE DESCRIPTION**: The training course is designed to provide a high-level overview of the Cyber Range as a tool to understand cyber risk through the exploration of the insights that can be gained by running scenarios on cyber range: Econometric models and Remediation Plans

This course is intended to equip an understanding of how to plan for cyber range scenarios application to cyber risk management.

The intended audience are managers who want/have to make use of the cyber range capabilities to elaborate scenarios for risk analysis and for trainings.

The objective is to make learners able to plan scenarios for risk analysis and insights on cyber range.

**DELIVERY MODALITY**: E-LEARNING CLASS

**DURATION**: 2 hours

**PREREQUISITE:** Knowledge on risk management fundamentals

**CONTENTS**

1. Cyber Range inputs and outputs
2. Selection of the scenarios to replicate on the cyber range
3. Econometric models
4. Remediation plans

✓ 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:*

- Remaining aware of evolving technical infrastructures
- Using 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
- Packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Network mapping and recreating network topologies
- Organization's risk tolerance and/or risk management approach
- Information security program management and project management principles and techniques
- Risk Management Framework (RMF) requirements
- Cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data
- Specific operational impacts of cybersecurity lapses
- Risk management processes (e.g., methods for assessing and mitigating risk)