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 A002 “Introduction to computer and network forensics”

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: A002 - Introduction to computer and network forensics

DELIVERY DATE: FEBRUARY 1st 2022, AM

COURSE DESCRIPTION: The training course is designed to provide learners with an understanding of the importance of computer and network forensics in cyber security (why, how, where, when, what, who), discover some of the tools, procedures and best practices for computer & network forensics.

This training's intended audience is IT or cyber security interested people, with a good first knowledge or experience of the IT and networks fundamentals.

The objective is to increase knowledge of the cyber forensics discipline

DELIVERY MODALITY: E-LEARNING CLASS - Webinar

DURATION: 2.5 hours

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

Only trainees that have successfully passed an online pre-enrollment quiz will be admitted to the training. Further details on this quiz will be given to prospective students.

CONTENTS

1. Cyber-MAR H2020 project overview
2. Understanding cyber-attack artifacts
3. Introduction to network and computer forensics operations, best practices, procedures, tools

✓ Initial and Final quizzes for training efficacy evaluation

TRAINING STRUCTURE

The training will be delivered online through Zoom Webinar and Cyber-MAR Learning Management System.
The attendees will receive individual credentials and links to join the training.

LEARNING OUTCOMES

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

- Understanding of the techniques used for detecting host and network-based intrusions using intrusion detection technologies
- Discovery of incident response and handling methodologies
- Collect intrusion artifacts and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise
- Preserve evidence integrity according to standard operating procedures or national standards
- What constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- An organization's threat environment