



Cyber-MAR: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Building cyber-resilience within maritime

FACTS

Call Identifier: SU-DS01-2018

Duration: From 2019-09-01 to 2022-08-31, on-going project

Total Cost: EUR 7.154.505

EU contribution: EUR 6.018.367

Coordinator: Institute of Communication and Computer Systems (ICCS), Greece



cyber-mar.eu

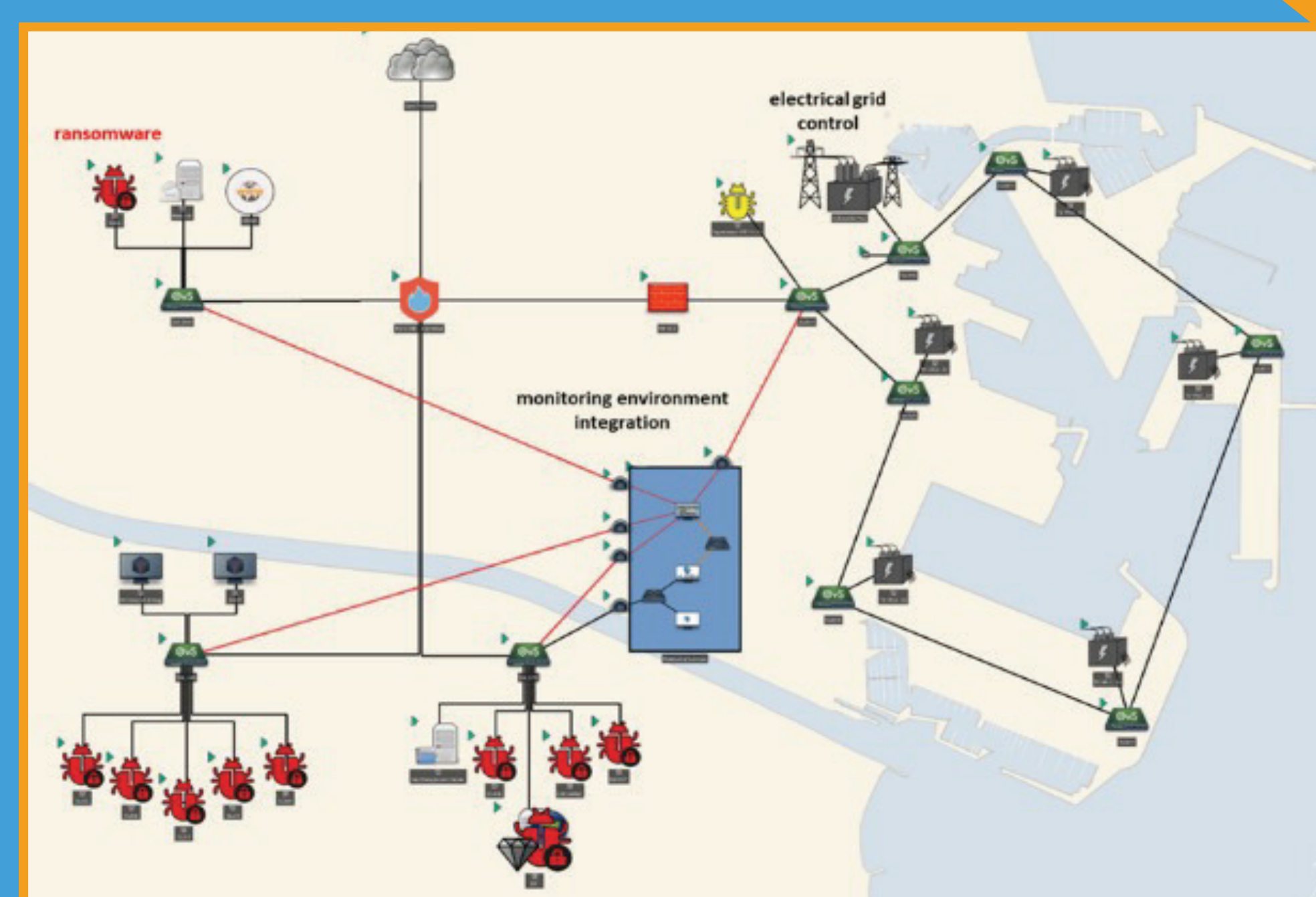
Cyber-MAR pilots

Pilot 1: Energy sources in the port of Valencia

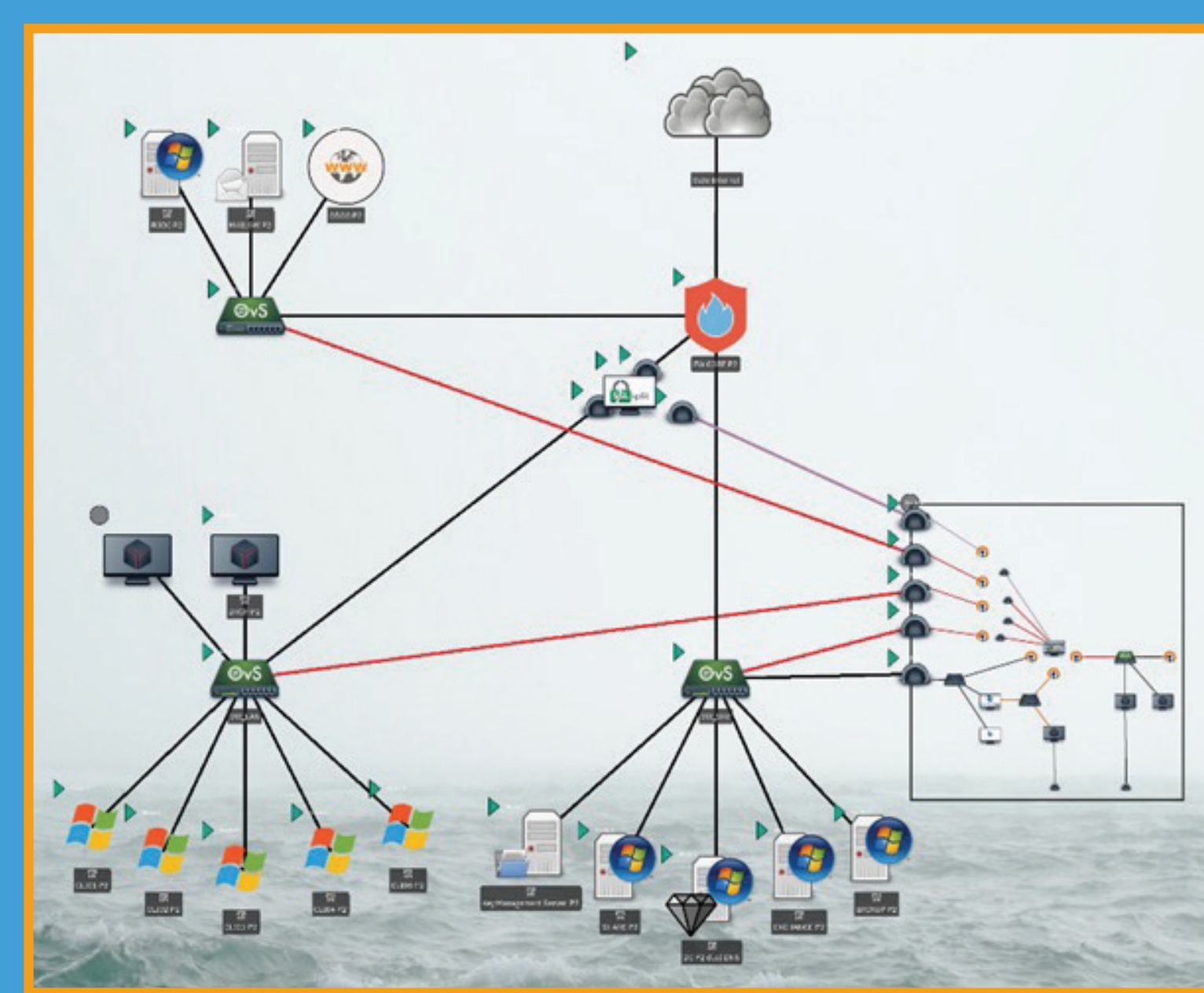
The first pilot scenario was about testing and validating an initial version of the Cyber-MAR system in the scope of a cyber-attack scenario on the port authority's electrical grid, in the Port of Valencia. The scenario was focused on the simulation of a remote access attack on the IT and OT infrastructure, and energy grid of the Port of Valencia. The primary aim of this attack was to cut off the power supply to the port, by shutting down the grid management OT system, with the OT manager's computer as the original infection point. The secondary aim was to simulate a Ransomware attack triggered by the Command & Control server, that would cryptolock all workstations within the infrastructure of the port. During the demo, the Cyber-MAR Cyber Range provided insights of the scenario through different points of view: from an attacker's perspective and from a defender's perspective using Intrusion Detection System (IDS) and SIEM.

Objectives

- Adapt the systems to avoid of cyber-attacks on the port smart grid.
- Mitigate consequences in the case of having an attack.
- Restore the system in the case of having an attack.
- Increase the port personnel awareness of these situations.
- Provide training for the necessary skills in cyber threats.
- Provide training for quick response in case of emergency.
- Possibility to adapt the knowledge provided by this scenario in other medium and low voltage networks.



Valencia pilot topology: Integration of IDS, XL-SIEM and MISP



Main topology deployed in the Cyber-MAR Cyber Range

Pilot 2: Vessel navigation and automation systems

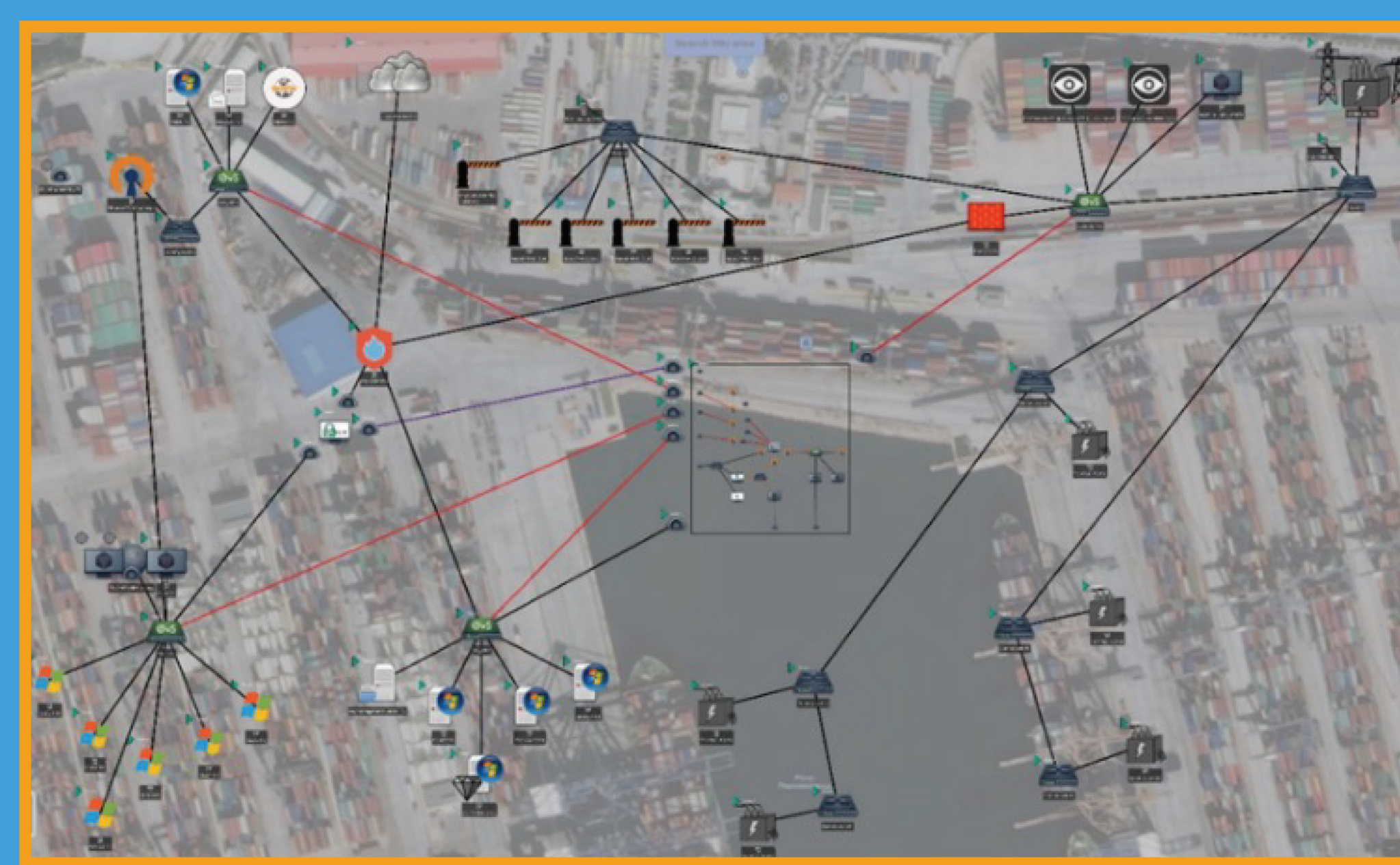
The vessel scenario constituted a scenario where an attacker launched an attack that allowed him to temporarily alter the course of a large container vessel and in so doing cause a blockage on the approach channel.

Progression of Attack was broken down into a number of stages:

- Downloading and Propagation of Attack (Within IT Infrastructure)
- Installing and Initiating the Attack on Vessel Control Systems
- Attack realisation and crew response.

Objectives

The objective of the second pilot scenario was to conduct a vulnerability assessment of the vessel's navigational capabilities (e.g., navigation systems, navigation aids) to mitigate malicious attacks, to train crews to identify and mitigate such cyber-attacks, and to identify restoration and reporting procedures in case the vessel is compromised at sea.



Piraeus Pilot topology in Cyber-MAR Cyber Range

Pilot 3: SCADA system in Port Container terminal

This scenario presented and tested a combined attack targeting initially the SCADA system that controls the traffic around the train yard, aiming for a collision between heavy trucks and incoming trains, followed by the main attack to the port's network, wiping out the entire network's IT and OT infrastructure.

Objectives

- Assess cyber-risk for port's IT and OT infrastructure.
- Highlight the consequences and the economic impact of such cyber-attacks to the port terminal's operations.
- Increase stakeholders' cybersecurity awareness.
- Prepare port personnel to mitigate and restore systems in case of a cyber-attack.
- Underline the necessity of keeping offline back-ups and spare machines for quick restoring operations.
- Test and demonstrate the capabilities of the Cyber-MAR platform and components.

Cyber_MAR Cyber-MAR Cyber-MAR EU Project info@lists.Cyber-MAR.eu

THE CONSORTIUM



This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.



FUNDACIÓN VALENCIAPORT



UNIVERSITY OF PLYMOUTH

