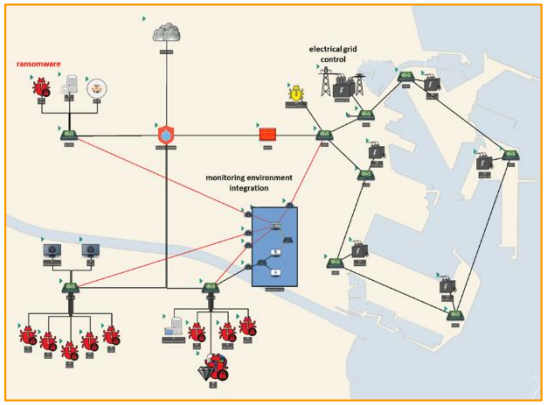
Pilot 1: Energy sources in the port of Valencia

Description

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

Realisation

The Valencia Pilot Event took place on 16.12.2020, virtually at 10.00-13.00 CET, via zoom meeting.

Material

Cyber-MAR pilot 1 material is available is the following URL: https://www.cyber-mar.eu/event/cyber-mar-valencia-pilot-event-material-access/

Cyber-MAR At a glance

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

Project ID: 833389

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

www. cyber-mar.eu

Cyber_MAR

Cyber-MAR

info@lists.cyber-mar.eu

Consortium

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 material reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.