Cyber-MAR Overview

About | Project Facts

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

Topic: SU-DS-2018: Cybersecurity preparedness-cyber range, simulation and economics

Contracting Authority: European Commission H2020

Project ID: 833389

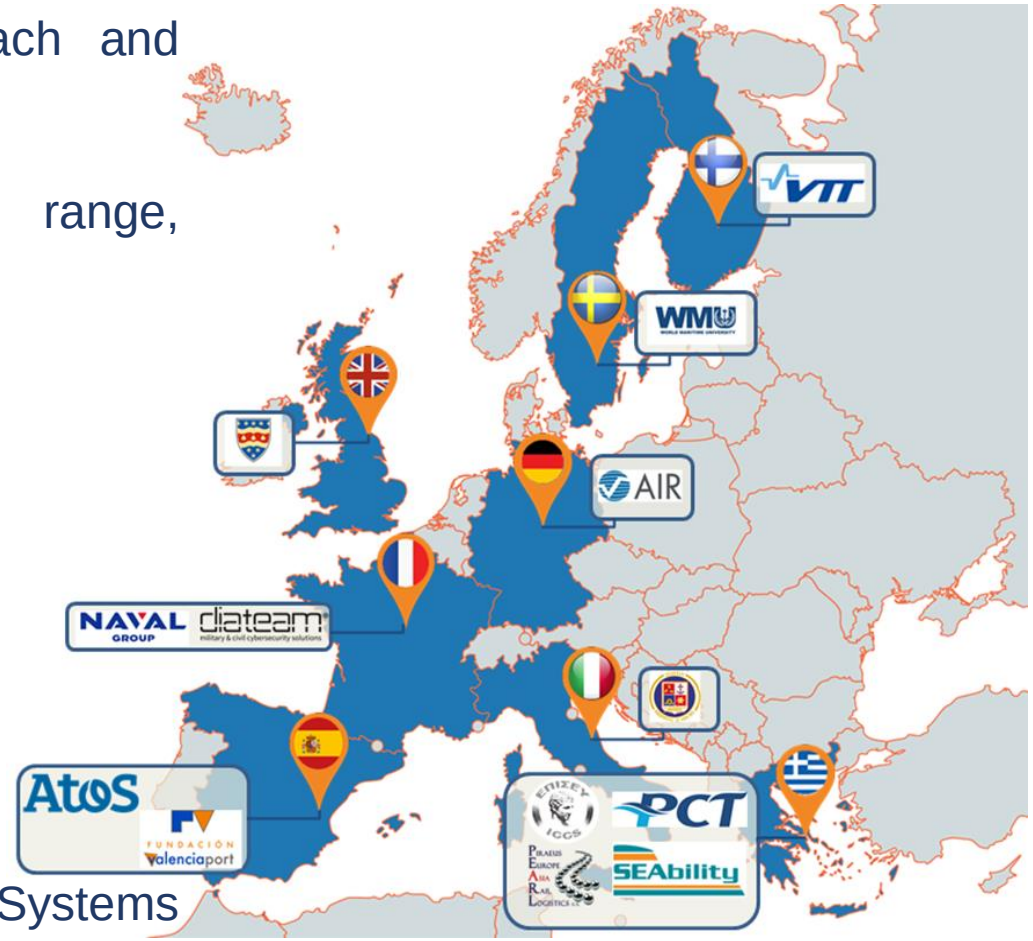
Funded scheme: IA – Innovation Action

Duration: From 2019-09-01 to 2022-08-31

Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

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



Challenges & Goal

- **Maritime information systems** in many cases designed without accounting for the **cyber risk**
- **Digital infrastructure** has become essential & critical to the **safety** and **security** of shipping and ports
- Importance of **handling cyber preparedness** as a highly prioritized aspect is paramount
- Estimation of accurately cybersecurity investments based on valid risk and econometric models

Cyber-MAR ultimate goal unfolds in **two main directions**:

Establishing a "**cyber ecosystem for preparing of cyber attacks**"

Estimating the **impact of cyber-attack** from a financial perspective and supporting the **undertaking of prompt decisions**

Cyber-MAR Key Objectives (1/2)

O1. Enhance the **capabilities** of cybersecurity professionals and **raise awareness** on cyber-risks

Deploy Cyber-MAR Range, training modules through LMS, improvement in response times in specific resilience metrics

O2. Assess cyber-risks for operational technologies (OT)

Maritime Cyber-Risk Assessment deployment and integration in Cyber-MAR platform

O3. Quantify the **economic impact** of cyber-attacks across different industries with focus on **port disruption**

Quantify economic risk in terms of Time-to-Recover or Product Value at Risk, integration in Cyber-MAR platform

Cyber-MAR Key Objectives (2/2)

O4. Promote **cyber-insurance market maturity** in the maritime logistics sector (adaptable to other transport sectors as well)

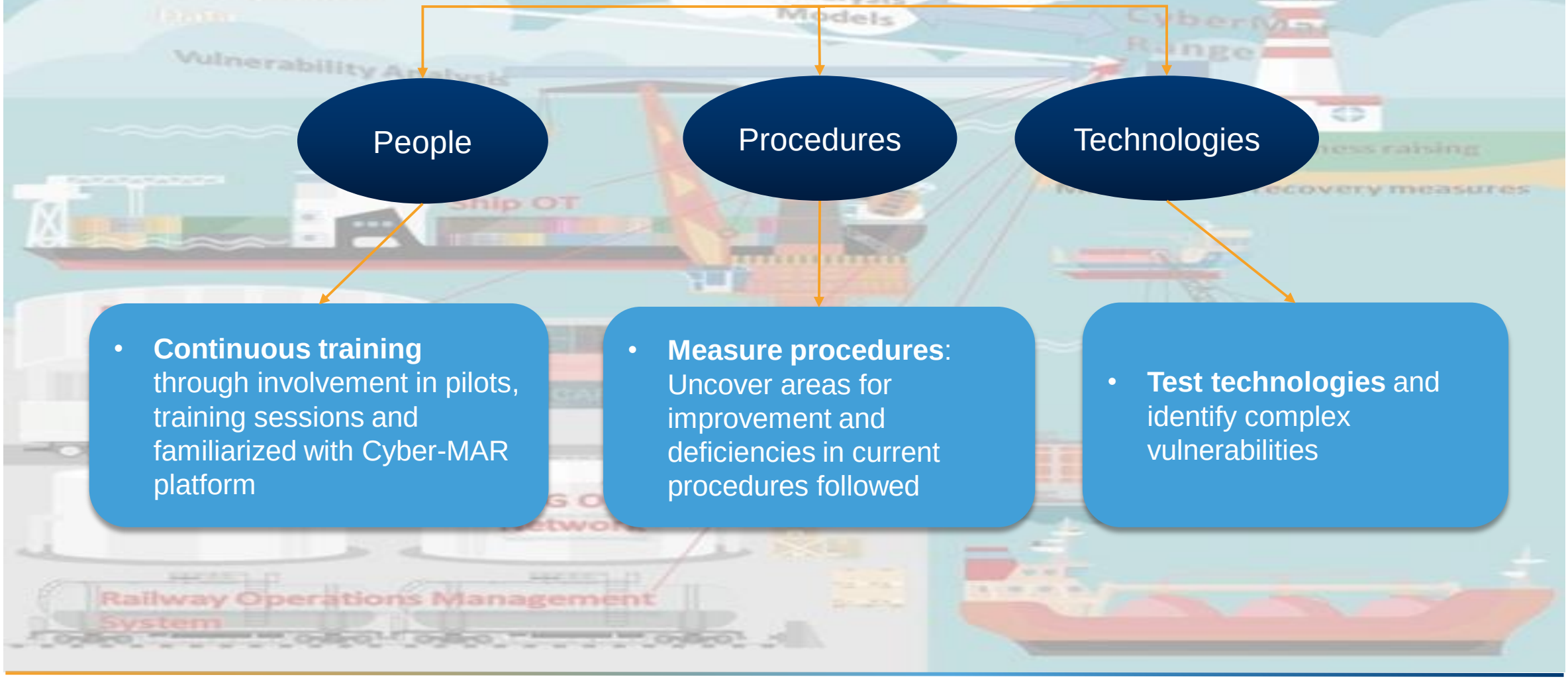
Develop recommendations based on findings and outcomes from Cyber-MAR pilots and simulations

O5. Establish and **extend** CERT/CSIRTs, competent authorities and relevant actors **collaboration** and **engagement**

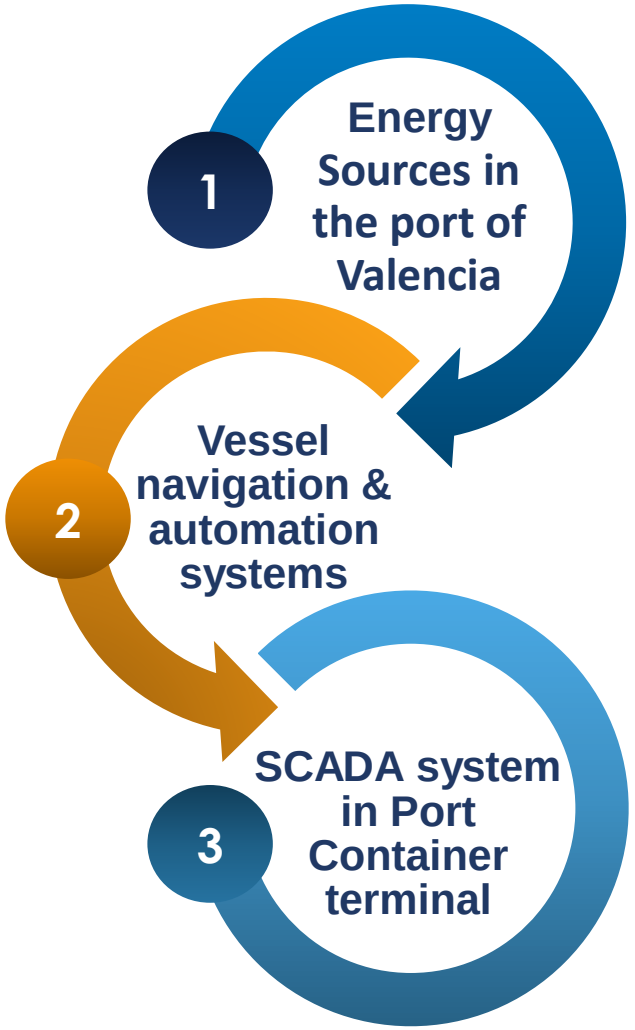
Create a maritime Malware Information Sharing Platform (MISP) community, engage at least 2 CERT/CSIRTs in pilot activities

Cyber-MAR Concept & Methodology

Cyber-MAR takes advantage of cyber range environment and adopts a three-tiered approach in:



Pilot Scenarios



The Cyber-MAR platform will be applied to simulate **the port electrical grid of the port of Valencia**, including protocols for protecting the grid and crisis management after attack.

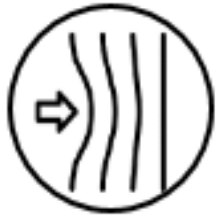
The Cyber-MAR platform will be applied to simulate **a ship bridge cyber-attack**, including potential attacks to navigation, communication and control systems.

The Cyber-MAR platform will be applied to simulate **a SCADA attack to the Port Container Terminal of Piraeus Port**. In particular, the consequences of a cascade effect extending the attack to the railway operator network.

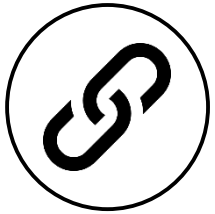
Expected Impacts

Impact on Resilience to Cyber-Threats & Data Privacy Breaches

Enhancement of the **resilience of target organizations** to new and emerging threats through the **identification of recurring or emerging patterns of cyber-attacks** and **privacy breaches** with a decent degree of accuracy.



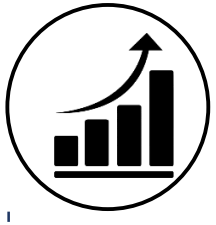
Impact on Supply Chain Efficiency



Cyber-MAR aims to offer the potential to **big players of logistics domain** to **join forces on estimating cyber-risk** and **mitigate** such **threats**, while **fostering open tools** that will improve the internal processes within each organization.

Impact on Appropriate Investments for Cyber-Security

Cyber-MAR focuses on the provision of a fully customizable and tailored view on the trade-offs, aims to **increase the available open tools** in number and variety, while offering an **intuitive integration to all** (physical and virtual) **IT components**.



Societal Impact

Cyber-MAR overemphasizes the importance of **accessible training infrastructures for cyber-defense**, in OT, transport and logistics domains and at the same time aims to contribute to the **standardization efforts** to make such issues prominent in the society.

Cyber-MAR Target Audience

- Decision Makers, Public Authorities and International Organizations
- Academia
- Port authorities, operators and associations
- Freight transport and Logistics actors
- CERT/CSIRTs network
- Insurance, Shipping and Cybersecurity companies/enterprises
- European and International organizations & networks for cybersecurity

Cyber-MAR User Requirements

User Requirements extraction methodology

User requirements classified in categories:

- Cyber-security
- Visualization
- Notification
- Audit
- Architecture
- Data security
- Training
- Legal

Co-design of the requirements with the Cyber-MAR stakeholders community:

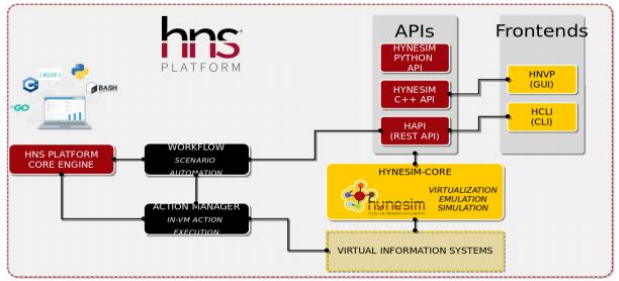
- dedicated workshop in Piraeus
- relative interviews for each pilot area

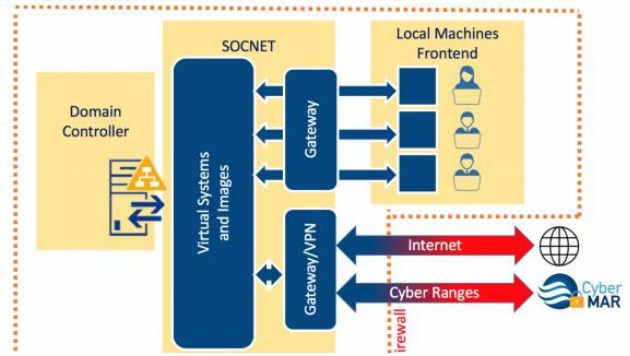
Cyber-MAR System Requirements

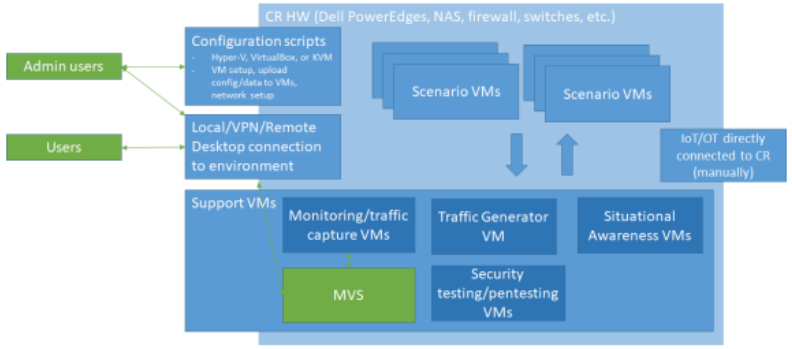
- **The categories of the system requirements created are:**
  - **Common**: Horizontal requirements related to most or all components of the Cyber-MAR system
  - **Simulation building**: related to setting up a new simulation instance
  - **Simulation execution**: related to the realization of a simulation
  - **Simulation monitoring**: related to the monitoring of simulation and scenarios during their execution
  - **Risk Analysis & insurance Model**: related to the cybersecurity risk analysis and the econometric model components
  - **Evaluation**: related to the evaluation of trainees
  - **Training**: related to features dedicated to training use cases

Cyber-MAR Components

- **HNS**
  - Cyber Range with virtualization and task automation capabilities creating a realistic environment used for training or prototyping computer networks.
- **Ship Simulator**
  - The ship simulator provides the capability to simulate a complete ships bridge (i.e. ECDIS, Radar etc). The simulator can be used to simulate a fully operational ship and traffic flowing between different components can be captured and used for off-line analysis.
- **IDS**
  - Intrusion Detection / Prevention functionality suitable for the maritime scenario. It analyses all relevant network traffic in the scenario and alerts when an attack or other suspicious behavior is detected.
- **Expert SA - High Level SA**
  - Expert Situational Awareness (SA) producing situational awareness visualization of the outputs of network monitoring tools. This view displays detailed technical views with the possibility to dig in to details.
  - The Metric Visualization System (MVS) is a tool for designing and monitoring the security of information systems and increasing the meaningfulness of security metrics by visualizing their full range.

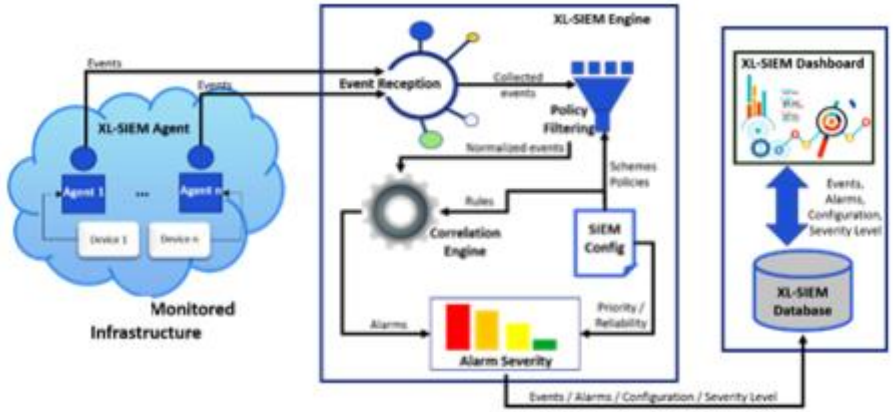




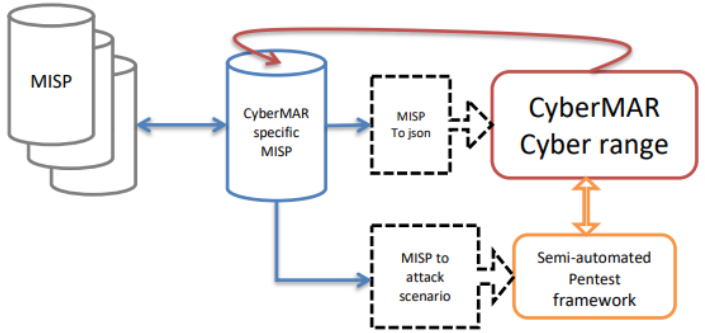


Cyber-MAR Components

- **XL-SIEM and L-ADS**
  - **XL-SIEM:** Real-time collection and analysis of security events. Prioritization, filtering and normalization of the data gathered from different sources. Consolidation and correlation of the security events and generation of alarms and reports Execution of countermeasures (scripts) or creation of tickets for further investigating the incident
  - **L-ADS**: live anomaly detection system based on unsupervised machine learning algorithms that analyses the network traffic using NetFlow to identify anomalous behaviors in device communications

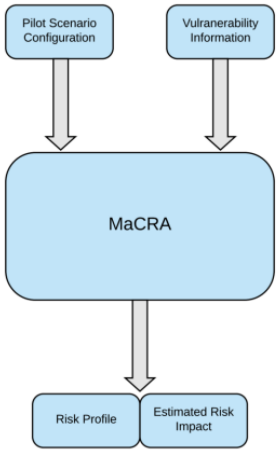


- **CERT**
  - The CERT component is mainly based on technical and operational datas produced by inter-CERT cooperation. Main function is to upgrade the cyber security cooperation MISP platform by setting up and taking part in a MISP community dedicated to the maritime sector stakeholders. This community will allow to share and communicate IOCs and specific maritime consequences of vulnerabilities to improve cybersecurity early warning.

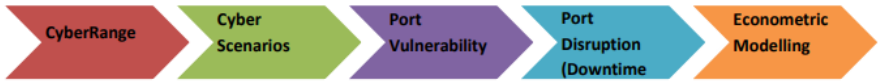


Cyber-MAR Components

- **Macra**
  - measures the level cyber-risk exposure of the pilot systems under consideration. A risk model is then be applied to a discrete event simulation model of the port operations so that an estimate of the expected effect of cyber-attacks on maritime operations can be calculated.
    - e.g. the effect of the attack will be quantified in terms of the expected reduction in operational capacity of the maritime port and the consequential estimated delay in processing containers that will be caused by that drop in operational capacity.

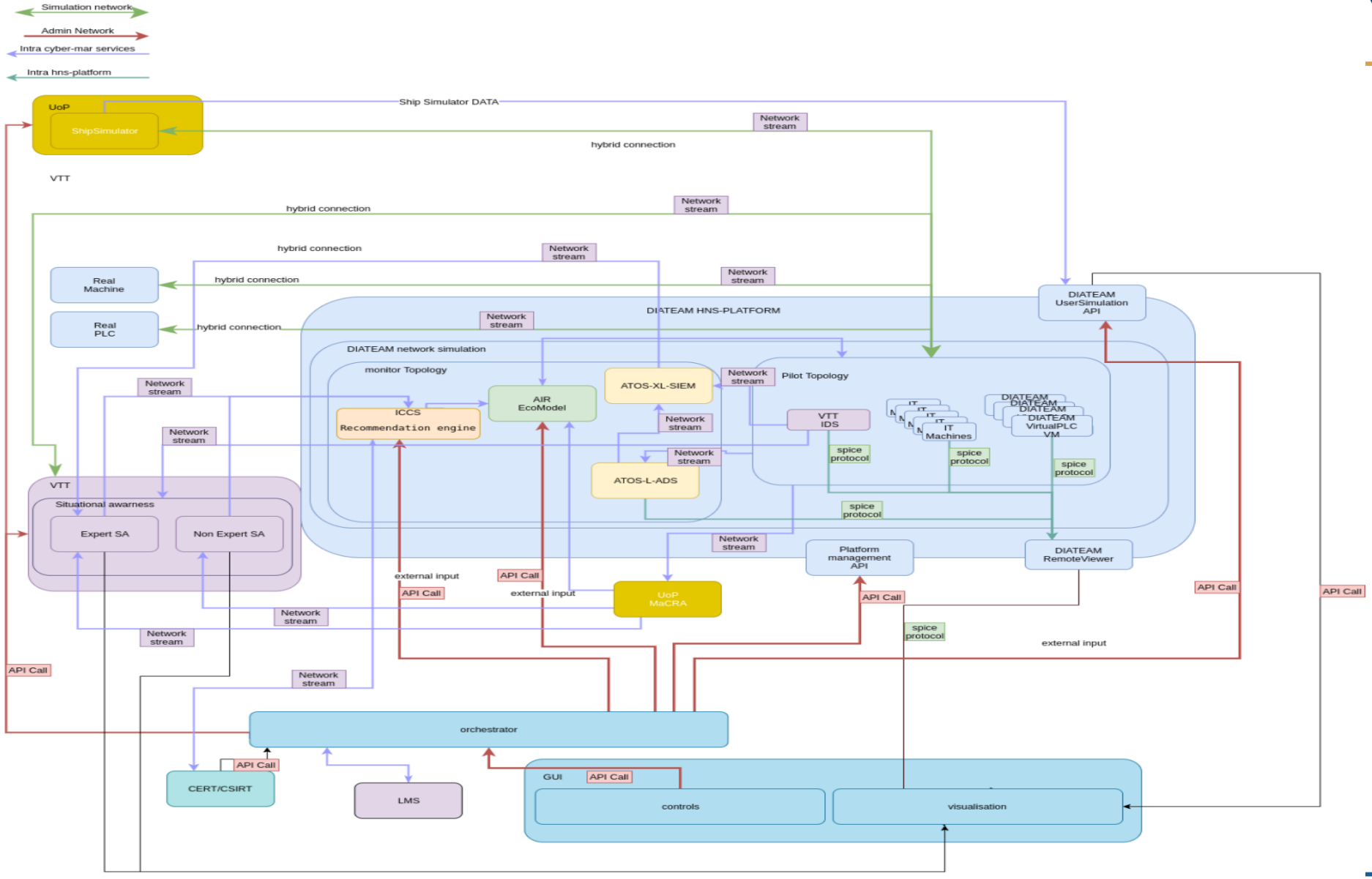


- **Econometric Model (AIR)**
  - outputs the economic losses for different nodes in the value chain. Either in-terms of business disruption days or monetary losses



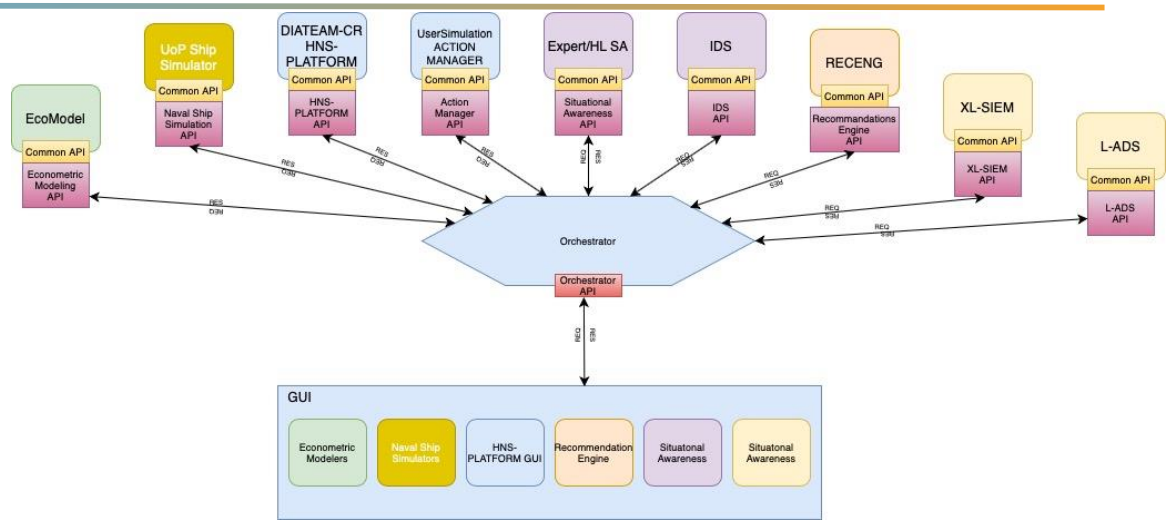
- **Recommendation Engine**
  - receives input from the IDS in terms of the up-to-the-moment sequence of an attacker's actions and overall state of the network. Provides a probabilistic prediction of the next/future actions of the attacker and/or the next/future state of the network. Fused with information from econometric models, aiming to help the defenders prioritize their responses.
- **LMS**
  - Platform to improve performance, skills and retain the best talent in the teams and allows to manage the transformation in e-learning and the distribution of courses

Cyber-MAR High Level Architecture (Physical View)



Cyber-MAR Orchestrator

- The Orchestrator is the main controller component of the Cyber-MAR CR system.
- The Orchestrator controls all other modular components and communicates with them, via an API designed with the principle of functionality inheritance:
  - “all components that wish to integrate with the CR, need to properly implement an API for common, type specific and component specific functions.”
- on-going work is started on the specific definitions of the component’s API



API Level	Required	Stability
Level 0 - Common API	Yes, without it a component cannot be integrated inside Cyber-MAR	Designed by system architects, changes only between system version changes
Level 1 - Component Type API	Yes for components that provide specific type of service (e.g. SIEM)	Designed by system architects, changes only between system version changes
Level 2 - Component Specific API	No	Designed by developers of components, can change between releases without keeping the same design

Cyber-MAR 1st Pilot

Valencia Pilot Event (conducted **online),** on **16.12.2020**, at **10.00-13.00 CET**, via an online conference platform.

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**.

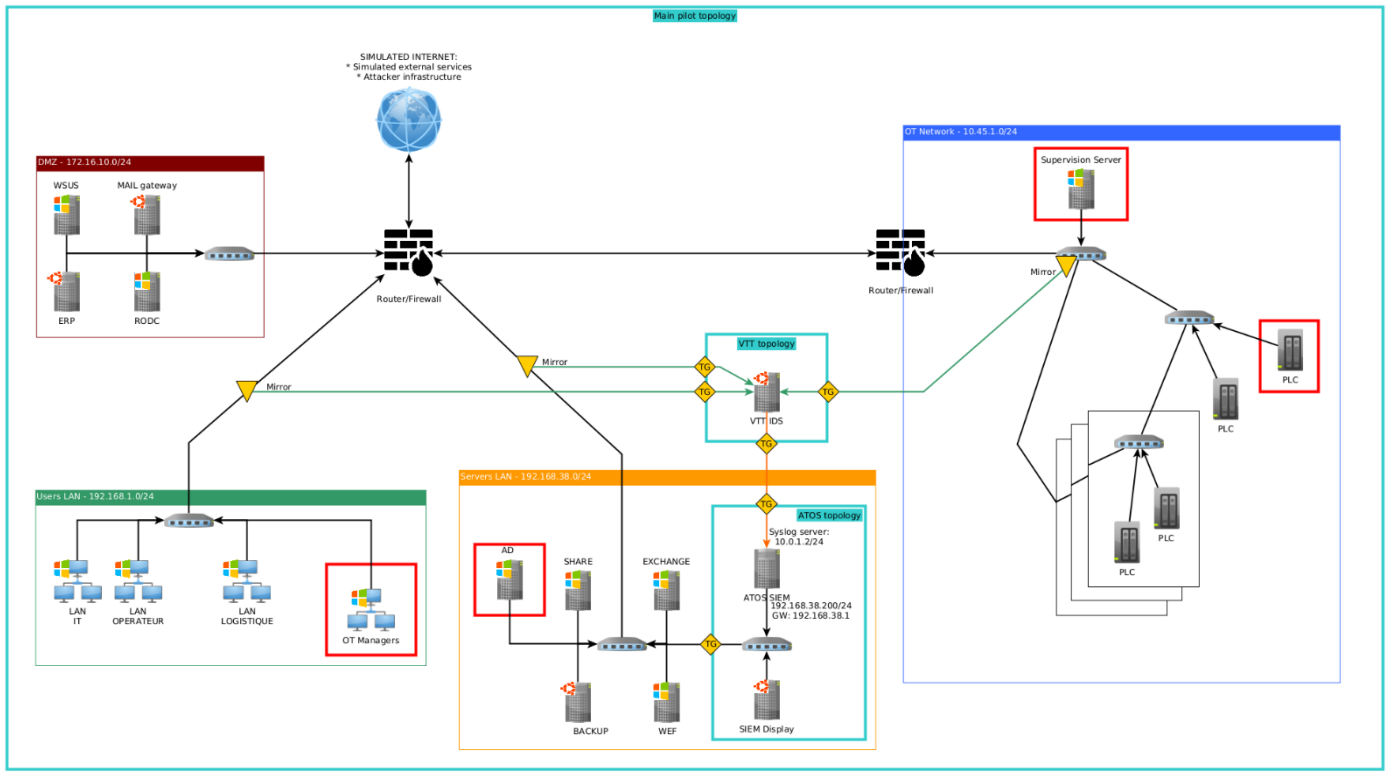
Simulation of a remote access attack on the IT and OT infrastructure, and energy grid.

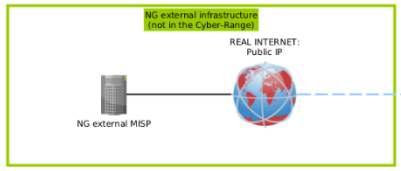
- cut off the power supply to the port, by shutting down the grid management OT system.
- simulate a Ransomware attack triggered by the Command & Control server, that will cryptolock all workstations within the infrastructure of the port

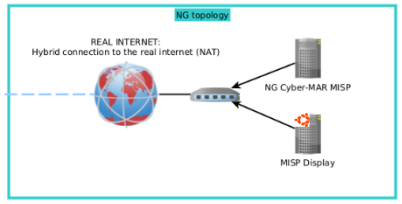
Registration is free of charge but required.
Please use the link to register and receive the conn details!

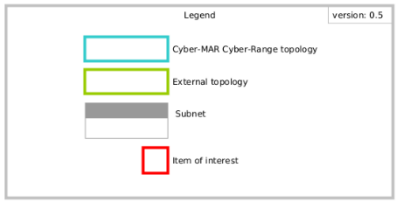
https://www.eventbrite.com/e/cyber-mar-valencia-pilot-event-tickets-127998062651

Cyber-MAR 1st Pilot









Scenario Steps:

1. Spear phishing email sent to the OT operator containing malicious document with embedded malicious code (macro)
2. Exploit the Zerologon vulnerability (CVE 2020-1472) to gain access to the Domain Controller (Active Directory) – privilege escalation.
3. Threat actor objectives:
    1. Attacking modbus PLC: Change state from RUN to STOP without authentication
    2. Cryptolock: encrypt files on the machines and network shares and hold them for ransom

Registration is free of charge but required.
Please use the link to register and receive the co details!

https://www.eventbrite.com/e/cyber-mar-valencia-pilot-event-tickets-127998062651

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Eleftherios Ouzounoglou, ICCS

eleftherios.Ouzounoglou@iccs.gr

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389