Cyber-MAR Final and Piraeus Pilot Event

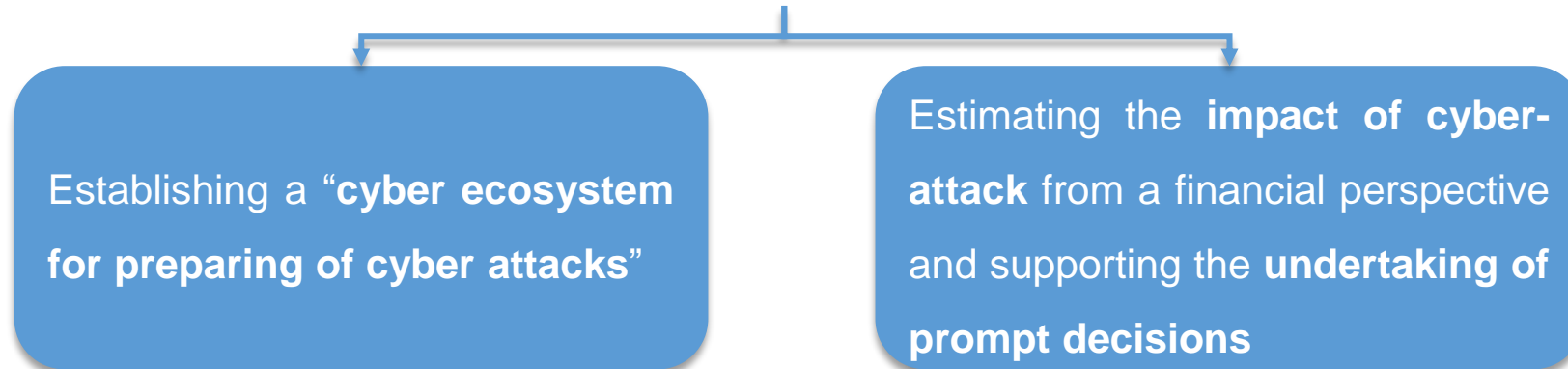# Cyber-MAR Overview and Benefits

Giorgos Papavassiliou, ICCS

16th December 2022

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 cyber range, training modules through LMS, validation in three demonstrations in real-life conditions

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 CERT/CSIRTs in pilot activities

Cyber-MAR Concept & Methodology

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

People

Procedures

Technologies

- **Continuous training** through involvement in pilots, training sessions and familiarized with Cyber-MAR platform

- **Measure procedures**: Uncover areas for improvement and deficiencies in current procedures followed

- **Test technologies** and identify complex vulnerabilities

Pilot Scenarios

1 **Energy Sources in the port of Valencia**
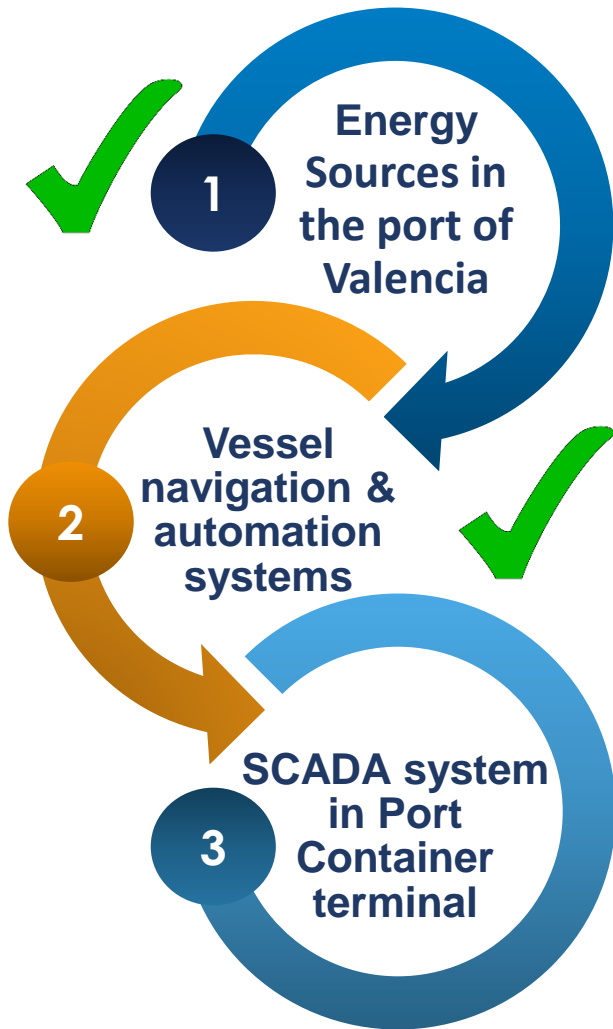
The Cyber-MAR platform was applied to simulate **the electrical grid of the port of Valencia**, including protocols for protecting the grid and crisis management after attack.

2 **Vessel navigation & automation systems**

The Cyber-MAR platform was applied to simulate **a ship bridge cyber-attack**, including attack to control systems and calculating the impact on the port operations and wider econometric impacts

3 **SCADA system in Port Container terminal**

The Cyber-MAR platform will be applied to simulate **a combined SCADA attack to the Port Container Terminal of Piraeus Port,** taking also into consideration the consequences of the attack to the railway operator network.

# Cyber-MAR Components

Cyber-MAR Components

Cyber Range

Virtual environment with task automation capabilities to realistically simulate cyber systems for cyber combat training, system/network development, testing and benchmarking. Provides full graphical interface for building and interacting with simulated network topologies. Hybrid connections allow to connect simulations to real-world equipment and other ranges via VPN
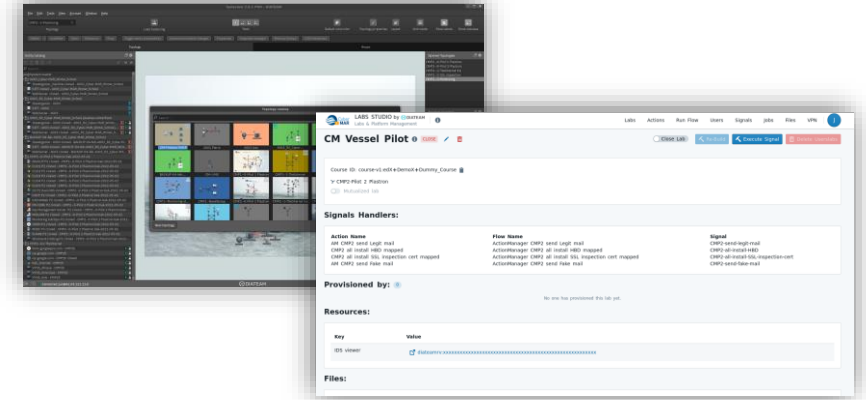
Ship Simulator

The ship simulator provides the capability to simulate a complete ship bridge (i.e. ECDIS, Radar etc). It can be used to simulate a fully operational ship and the traffic flowing between different components can be captured and used for off-line analysis. This can allow for investigations to be made on how failures in one part of the system can propagate to affect other systems within the ships bridge
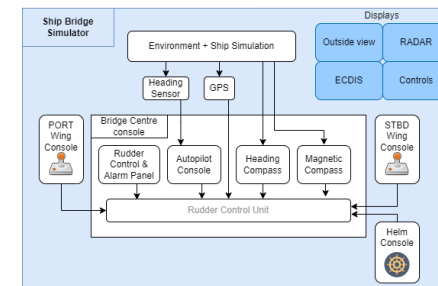
IDS

Security Onion based Intrusion Detection System providing signature-based detection and network security monitoring suitable for the maritime scenarios. It analyses all relevant network traffic in the scenario and alerts when an attack or other suspicious behavior is detected

Cyber-MAR Components
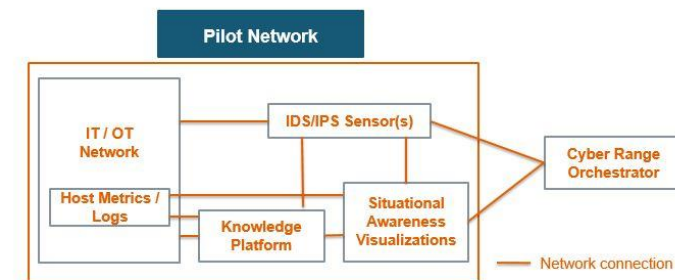
XL-SIEM and L-ADS

XL-SIEM: Real-time collection and analysis of sequences of events from different sensors. Correlation of the security events and generation of high-level alarms and reports

L-ADS: live anomaly detection system based on unsupervised machine learning algorithms that analyses the network traffic to identify anomalous behaviors in device communications
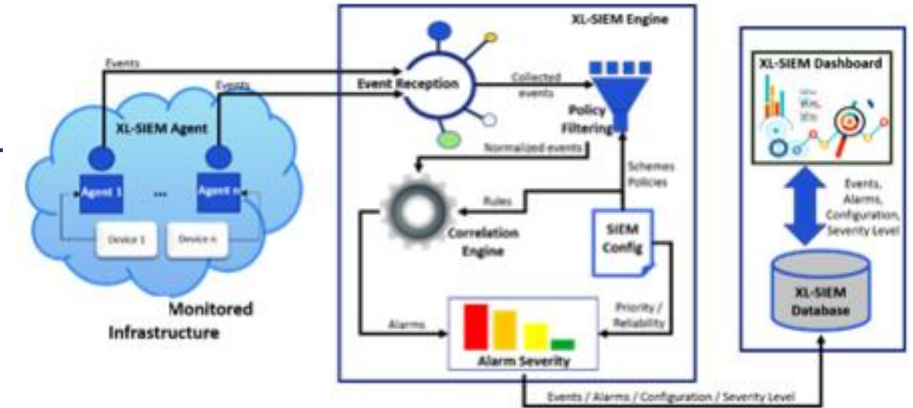
Expert SA & High-Level SA

Expert Situational Awareness produces situational awareness visualization of the current situation and history of events that have taken place in the scenario by using the outputs of the network monitoring tools. It displays detailed technical views, with the possibility to dig into details

High-Level Situational Awareness provides views of the current risk level in the target environment. The Metric Visualization System (MVS) used 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
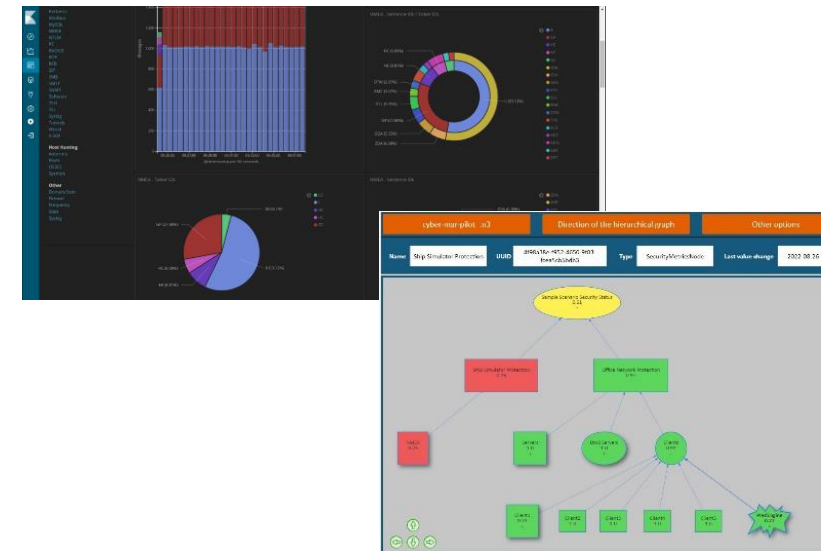
MaCRA framework

Measures the level of cyber-risk exposure of the pilot systems under consideration. The risk model is then 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

Econometric Model

Outputs the economic losses for different nodes in the value chain, as a function of the business disruption days and daily revenue for the product group / country of interest.

Prediction Engine

Receives input from the IDS & XL-SIEM 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 MaCRA and the Econometric model, aiming to help the defenders prioritize their responses.

Cyber-MAR Components
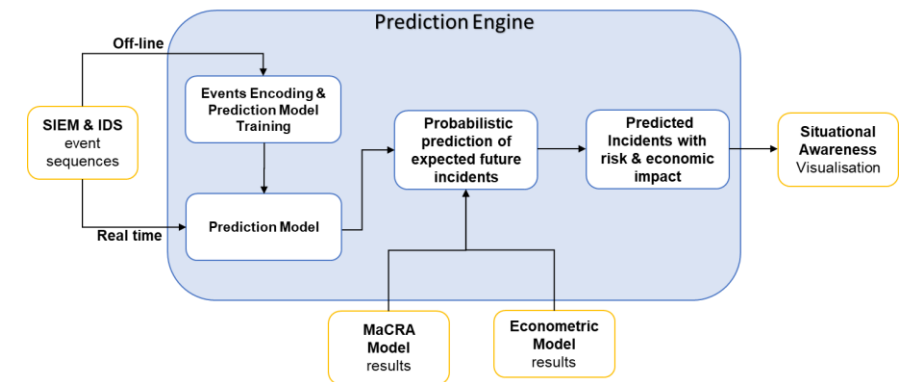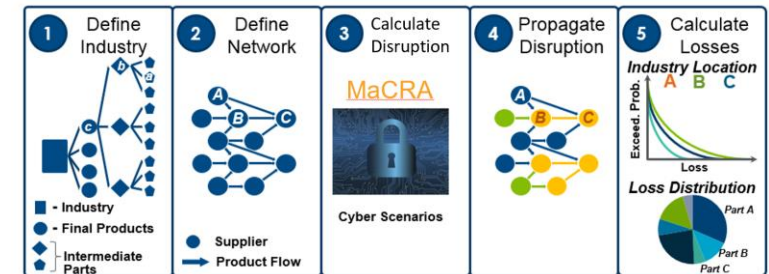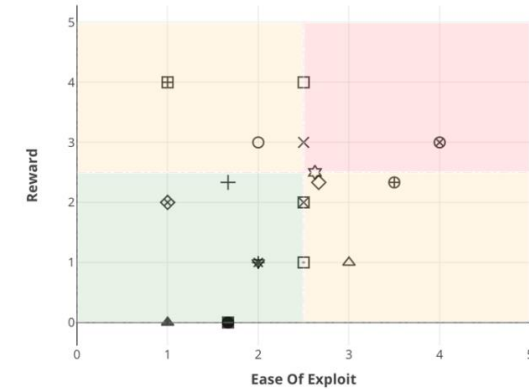
CERT tool (MISP)

The CERT component is mainly based on technical and operational data 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.
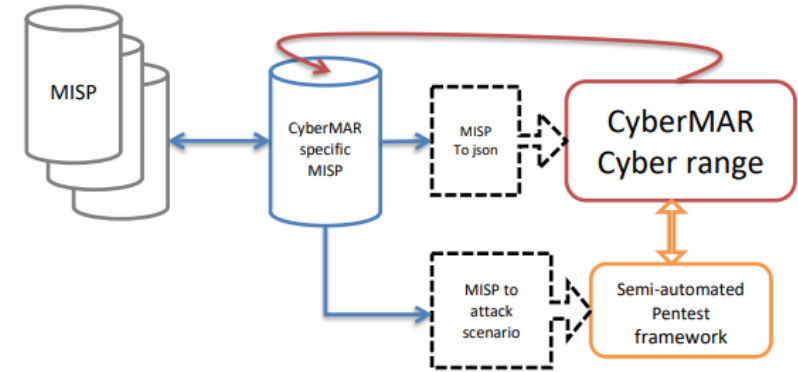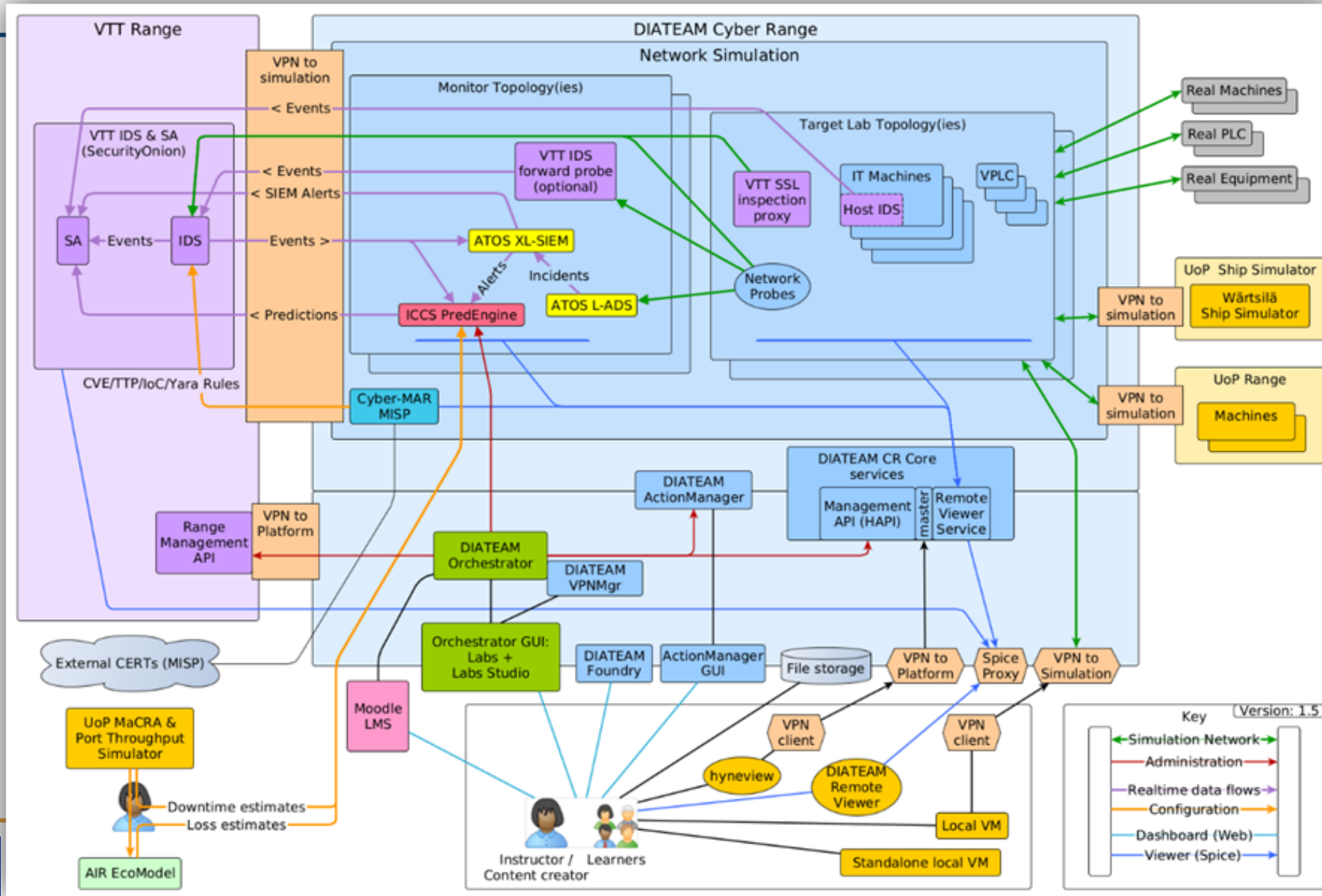
LMS

Training platform implemented and integrated into the Cyber Range aiming to improve the performance and skills and retain the best talent in teams. Allows the management and distribution of e-learning courses developed but also the monitoring and measurement of the training programs impact on the business
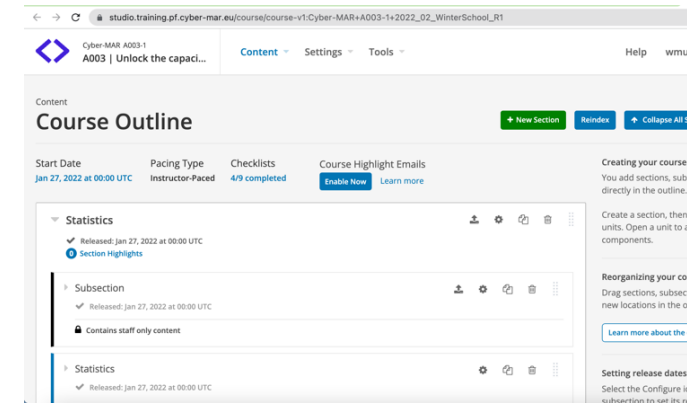
Architecture

Cyber-MAR Pilots

Cyber-MAR 1st Pilot

Testing and validating an initial version of the Cyber-MAR platform 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.

- simulated a Ransomware attack triggered by the Command & Control server, that cryptolocked all workstations within the infrastructure of the port

Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833389.

Cyber-MAR Valencia Pilot Event

Date: 16 December 2020   Time: 10.00-13.00 CET

Recording available on YouTube:
http://youtu.be/7dUEBOc_Gik

Cyber-MAR 1ˢᵗ Pilot

Pilot Conclusions:

1. Importance of cyber-security

2. Big economic impact on a port infrastructure

3. Severe incident could need from hours to days to recover

4. Cyber Range added value

5. Importance of testing all kind of vulnerabilities in your systems

6. Training is needed for personnel

Cyber-MAR 2nd Pilot

The Vessel Pilot demonstrated how various elements of the Cyber-MAR solution are integrated allowing the platform to model a complex **ship bridge cyber-attack** and its impacts.

Simulation of a cyber attack that allowed the attacker to alter the course of a large container vessel and thus causing a blockage on the approach channel:

- Downloading and Propagation of Attack (within IT Infrastructure)
- Installing and Initiating the Attack on Vessel Control System
- Attack realisation and crew response

Recording available on YouTube:
https://youtu.be/MAfErgM4zOA

Cyber-MAR 2nd Pilot
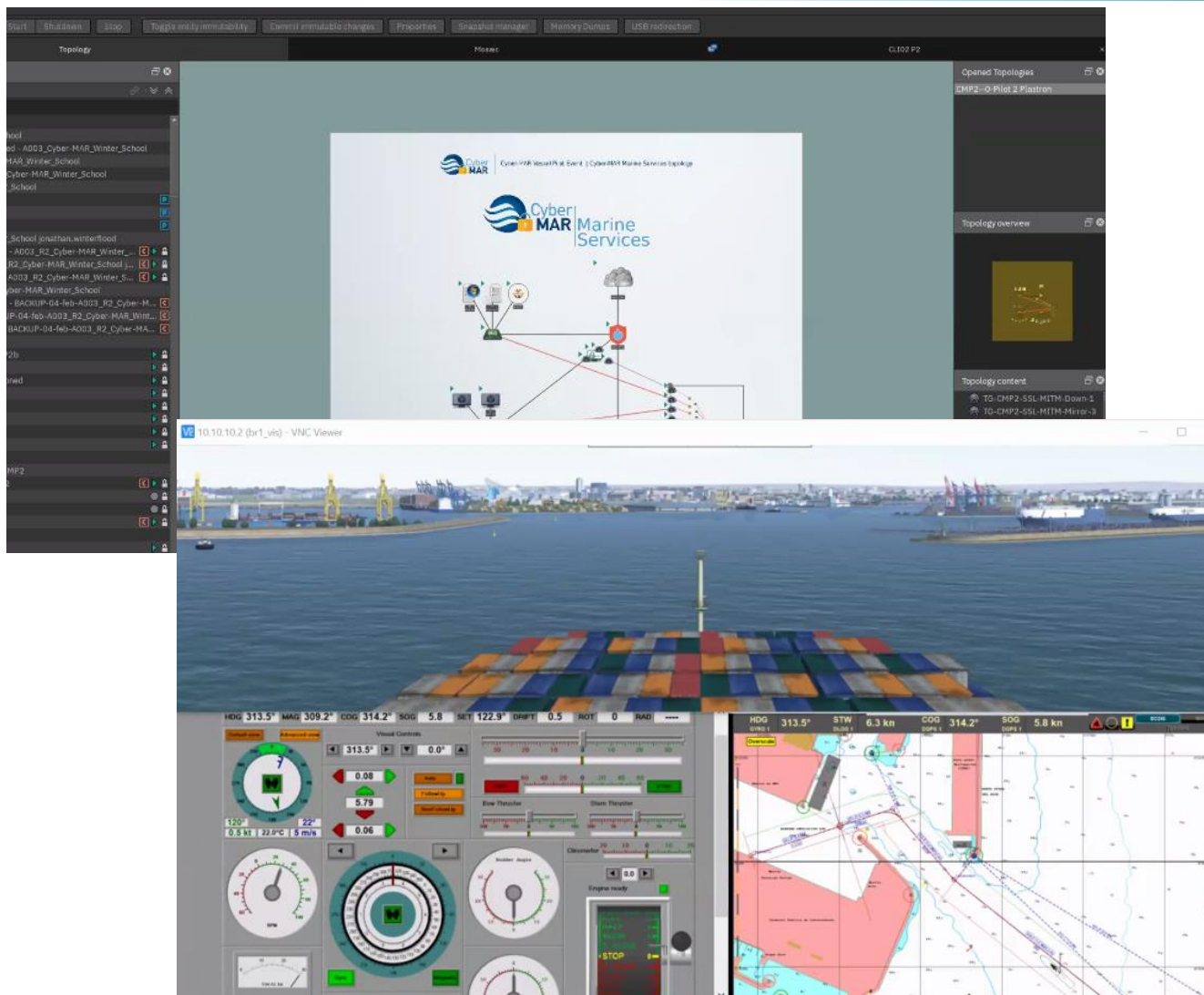
Pilot Conclusions:

1. Consequences to a port terminal when a cyber attack targets a visiting vessel

2. Quantified the economic impact of cyber attacks with a focus on port disruption

3. Importance of robust cybersecurity practices on board ships to ensure safety and security of operations

4. Raised cybersecurity awareness for seafarers

5. Validated the added value of the Cyber-MAR platform

Cyber-MAR 3rd Pilot

Testing and validating the final version of the Cyber-MAR platform in the scope of a combined SCADA attack scenario on the port's train gates network and smart grid, in the **Port of Piraeus**

Simulation of a remote access attack on the port's IT and OT infrastructure.

- compromising the level crossing barriers at the train yard leading to a collision between train and tracks
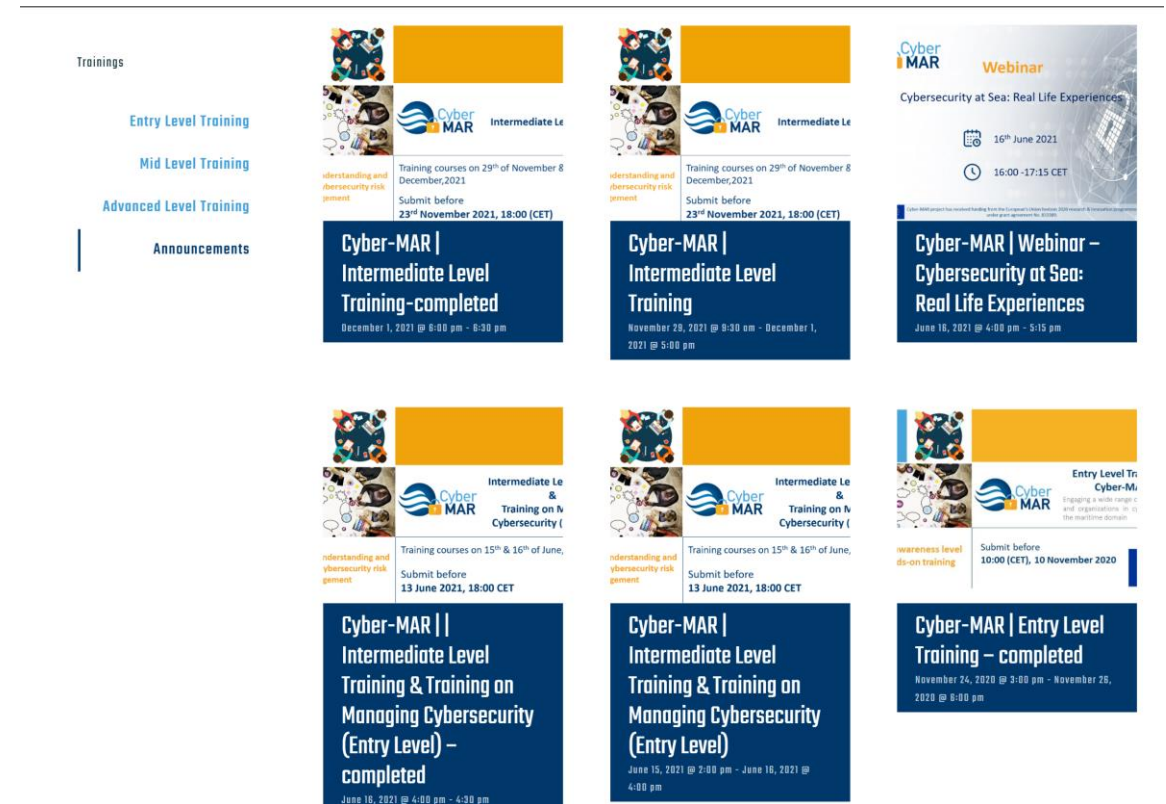- wiping out the whole grid's IT and OT infrastructure, cutting off port's power supply

Cyber-MAR Training

Cyber-MAR Training Activities

Providing an agile learning process by following a hybrid training approach (physical and virtual):

- Cyber-MAR LMS platform has been implemented and integrated into the Cyber Range

- Formulation of Cyber-MAR training packages with a focus on hands-on and practical training

- Successfully held Entry, Intermediate and Advanced level trainings

- Further trainings through the Cyber-MAR LMS platform are being organized

  - Including a major CTF competition (Jan-23)

https://www.cyber-mar.eu/trainings/

Cyber-MAR Project Achievements

Project Achievements

- Developed an innovative platform of **interconnected Cyber Ranges** providing capabilities of **network monitoring** and **visualisation**, **data fusion** and **probabilistic prediction** for increasing **situational awareness,** supporting decision making and offering **specialised cybersecurity training**

- Interconnected a **Ship Simulator** platform for simulating a complete ship bridge and validate it in the Vessel pilot

- Integrated **Network Monitoring Tools** (IDS, L-ADS, XL-SIEM) for intrusion/anomaly detection and alerting

- Created and connected a maritime **MISP community** for increased threat intelligence and facilitating the communication with CERT/CSIRT networks

- Introduced and validated the **Maritime Cyber-Risk Assessment (MaCRA) framework** for quantifying and understanding cyber risks in the maritime sector

- Developed an **Econometric Model** to quantify, in terms of monetary losses, the impact of cyber-attacks across different product groups and industries

Project Achievements

- Developed a Data Analysis and **Prediction Engine** that models attack behavior patterns, analyses network alerts and events and provides probabilistic predictions of future events of an attack, fused with the results from MaCRA and Econometric Model to support decision making

- Utilised **Situational Awareness** tools for visualising network monitoring data, alerts, predictions and cybersecurity risk level of the attacked infrastructure

- Demonstrated and validated in real-life conditions the Cyber-MAR platform in 3 pilot cases

- Deployed a **Learning Management System** within the Cyber Range environment and implemented a **hybrid cybersecurity training program** targeted to the needs of the maritime domain

  - 9 training sessions / 350 trainees (Entry Level: 2, Intermediate Level: 4 and Advanced Level: 3)

- **Liaison Activities** with other EU funded projects and maritime associations

- Produced **Guidelines and Recommendations** to be shared within the Maritime domain

- Developed a joint exploitation and **go-to-market strategy** for the Cyber-MAR offerings

Cyber-MAR Target Audience and Benefits

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

Benefits of using Cyber-MAR

Adopting a platform like Cyber-MAR can have multiple benefits for an organization, at multiple levels of operation and for different categories of members.

Employees:

- Experiencing real-world threats in a safe environment
- Learn how to recognize threats
- Develop and expand cybersecurity skills

Security Operator:

- Transfer information from the cyber range for immediate use
- Measure knowledge and capabilities of internal or external cyber security teams
- Raise awareness (technical/high level)
- Penetration Testing exercises
- Simulate real threat actor TTPs and learn from them

Management:

- Keep your employees trained
- Improve overall cybersecurity education
- Security Assessments in general
- Test processes and technologies
- Evaluate Cyber-Risk based also on its economic impact and take cost-effective decisions

Research and Development:

- Design and Build Prototypes, Testbeds technologies and experimental environments (e.g. IoT, ICS, robotics, smart grids, BigData, VR/AR etc.) and test them against cyber-attacks
- Design, Develop and Test new tools and methods for Cyber-Security

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Giorgos Papavassiliou, ICCS

giorgos.papavassiliou@iccs.gr