Cyber-MAR

An Innovative Simulation Environment

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

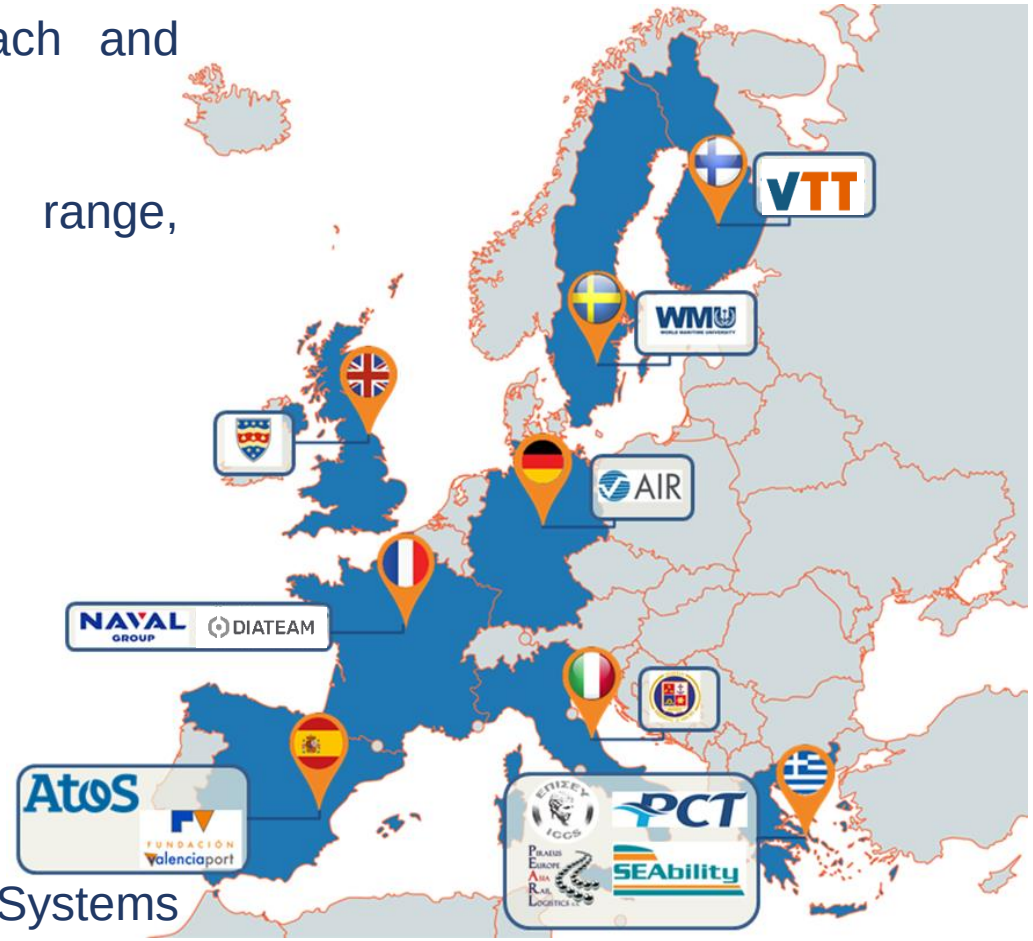
Funded scheme: IA – Innovation Action

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)

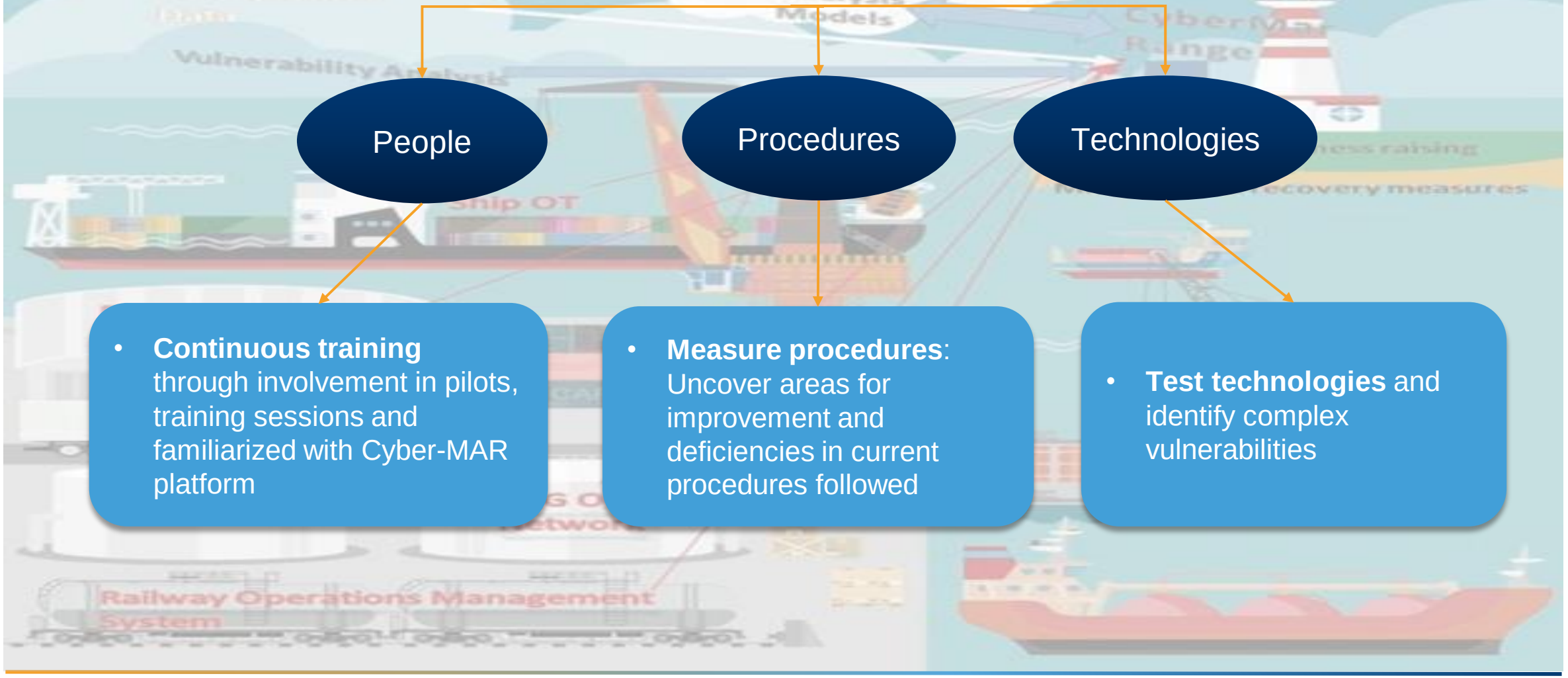
Develop recommendations based on findings and outcomes from Cyber-MAR pilots and simulations

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

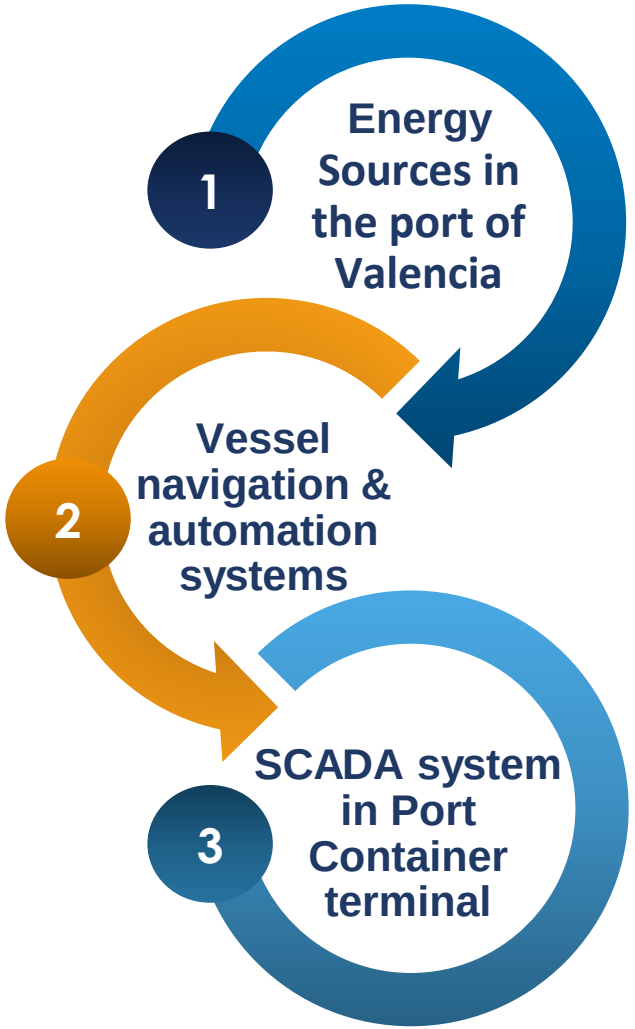
Create a maritime Malware Information Sharing Platform (MISP) community, engage at least 2 CERT/CSIRTs in pilot activities

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.

Approach and methodology of demonstration activities

Approach and methodology of Cyber-MAR demonstration activities

The demonstration programme is incrementally implemented in 3 distinct phases (15 months total duration):

- **Phase 1: Interconnection of legacy infrastructure with Cyber-MAR CR**
  - **1st Pilot on December 2020 – Valencia Port topology - Virtual OT**

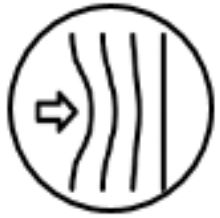
- **Phase 2: Addition of high-TRL Cyber-MAR CR, Cyber-MAR LMS, MaCRA framework and preliminary Cyber-MAR EM components and interconnected capability with other cyber ranges**

- **Phase 3: Full integration of all Cyber-MAR platform components.**

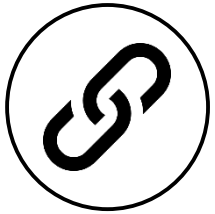
Expected Impacts

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.



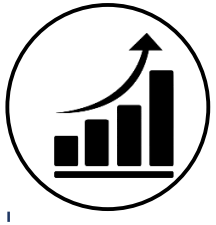
Impact on Supply Chain Efficiency



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

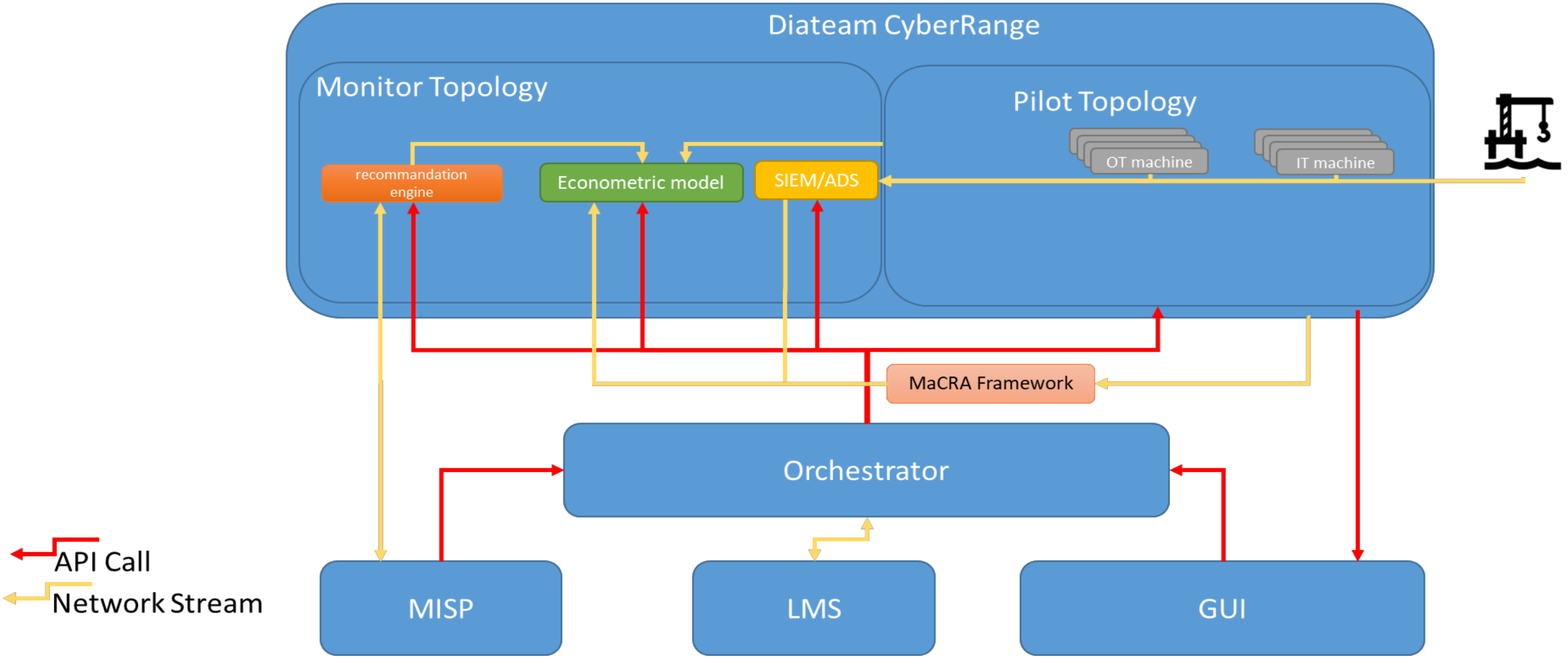
Benefits of using Cyber-MAR

- 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

Cyber-MAR Architecture & Technical Modules

Architecture



Technical Modules

Orchestrator	CyberRange	Recommendation Engine	Econometric Model	Tools

• Main controller
• Synchronise all components
• Create any topology
• Drive any scenario
• Common API
	• Produce & manage VE
	• Inter-Connection with real IT/OT
	• Create, view and interact with all VMs
		• Concentrate a lot of data
		• Evaluate risk and econometric
		• Near real-time evaluation
			• Evaluate economical impact of an attack scenario
			• Raise Awareness
				• Intrusion Detections System (Host/Network)
				• SIEM
				  • Event correlation
				  • Behavioural Analysis
				• MISP
				• MaCRA framework

Cyber-MAR Pilots

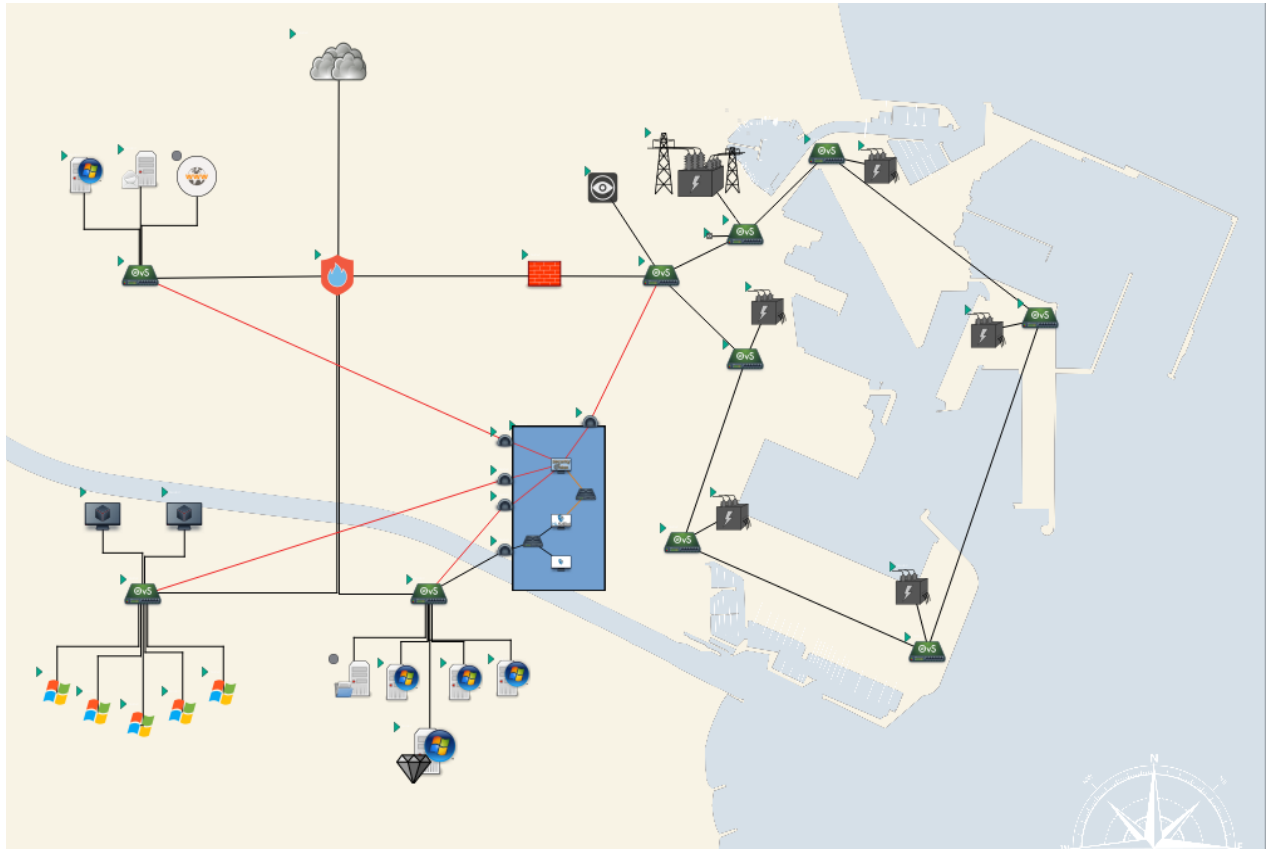
List of Pilots

- Valencia Energy Sources **[Completed]**
- Piraeus Port: SCADA Container Terminal
- University of Plymouth: Ship Simulator

Cyber Attack Scenario | Valencia Pilot

- IT segment: Server/Users/DMZ nets
- OT network: Scada Supervision (PcVue) PLC (Physical & Virtual)
- Monitoring segment
- Remote attack from the Internet

TARGETED TOPOLOGY



<u>Port Power cut & Cryptolock of key machines.</u>

- **1st Target:** Active Directory
- **How:** Spearphishing
- **Who:** the OT Manager
- **When:** Friday PM
- **What:** Malware through Macro
- **Bonus:** Ransom & Leaks

Cyber Attack Scenario | Valencia Pilot

Step 1
A spear phishing email has been sent from the adversary to the OT operator. The spear phishing email contains a malicious document (.docx) with the embedded malicious code (macro). MS Office macro-execution is usually either enabled by default or is allowed by a single mouse click upon opening the malicious file. This creates a large margin for "user errors" and increases the probability of a successful attack. The adversary waits for certain actions to be taken by the OT operator (opening the document, run the macro) in order to gain unauthorized access to the OT computer.

Step 2
Upon establishing a foothold inside the network via a command & control channel, the adversary placed the malicious code in a place inside the victim's workstation in order to persist from reboots. Then, through the command & control channel the adversary executed arbitrary commands, looking for other assets inside the network including the domain controller, and they exploited the Zerologon vulnerability (CVE 2020-1472) on the identified Active Directory in order to obtain an unauthorized domain administrator access to the entire Domain.

- **Attacking Schneider Electric Modicon M580**
  - **Modicon STOP command (Modbus)**
- **Cryptolock (triggered by C&C, launched by the already propagated malware**

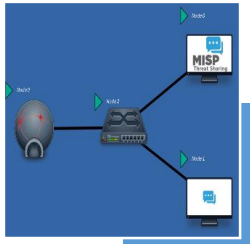
Blue Team Tools | Valencia Pilot

Security Onion

- Open Source, Linux Distribution
- Threat Hunting
- Alerting System
- Log Management
- Enterprise Security Monitoring Awareness
- Easy Setup in Minutes
- Collection of tools for network/host based intrusion detection

XL-SIEM

- Distributed and near-real time aggregation, dissemination and processing of events
- Corelation of events from application (service) layer
- High resilience embedded by design
- Possibility to deploy it as a service
- Improved detection



MISP

- Malware Information Sharing Platform
- Open Source Threat Intelligence
- Indicator of Compromises sharing
- Trusted members
- Community and Organization

Conclusions | Valencia Pilot

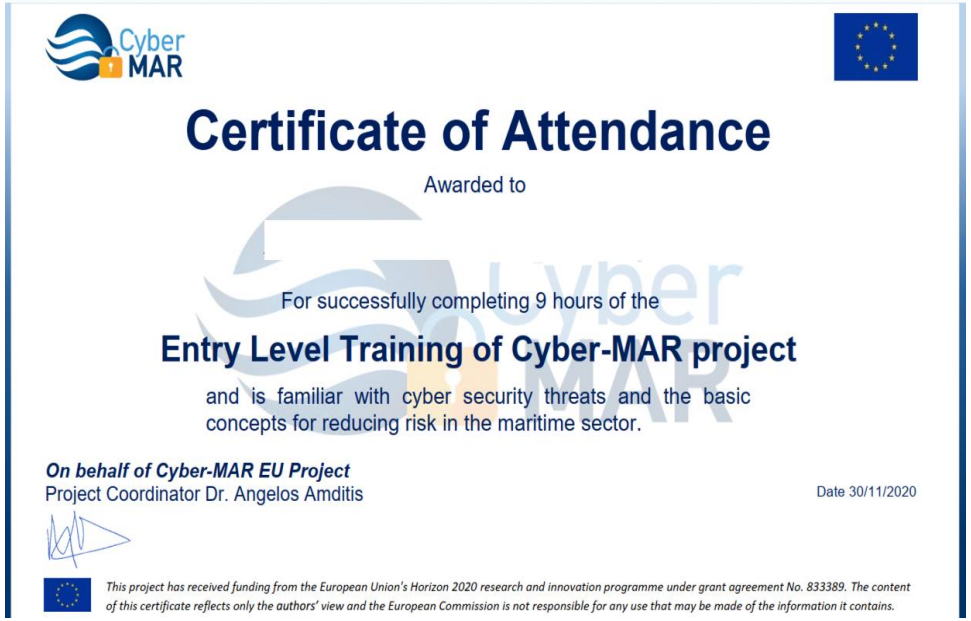
- Importance of cyber-security
- Big economic impact on a port infrastructure
- Cyber-range added value
  - Test all kind of vulnerabilities in your systems
  - Training for all the company personnel

Cyber-MAR Training

Training

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

- Training Level 1 (Entry Level) has been completed
  - Module 1: Introduction & Scenarios
  - Module 2: The Regulatory Framework for Cyber Security in Critical Infrastructure
  - Module 3: Attack Issues in deep
  - Module 4: Mitigation and Recommendation
  - Module 5: Knowledge Check Session
  - Module 6: Mini master on cyber security(entry level)
  - Module 7: Hacking and Defensive Tools
  - Module 8: Overview of real cases
  - Module 9: Knowledge check session



Cyber MAR

Certificate of Attendance

Awarded to

For successfully completing 9 hours of the

Entry Level Training of Cyber-MAR project

and is familiar with cyber security threats and the basic concepts for reducing risk in the maritime sector.

On behalf of Cyber-MAR EU Project

Project Coordinator Dr. Angelos Amditis

Date 30/11/2020

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

Training – Next Steps (LMS)

- Cyber Security Awareness (Entry Level)
- Tools for Cyber Range (Intermediate Level)
- CyberRange (HNS) Pro user training
- Econometric training
- PIREAUS CONTAINER TERMINAL attack pilot
- Autonomous boat attack simulation

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