Valencia Pilot

Cybermar - Architecture and technical modules

Aymerick Chincolla, Naval Group

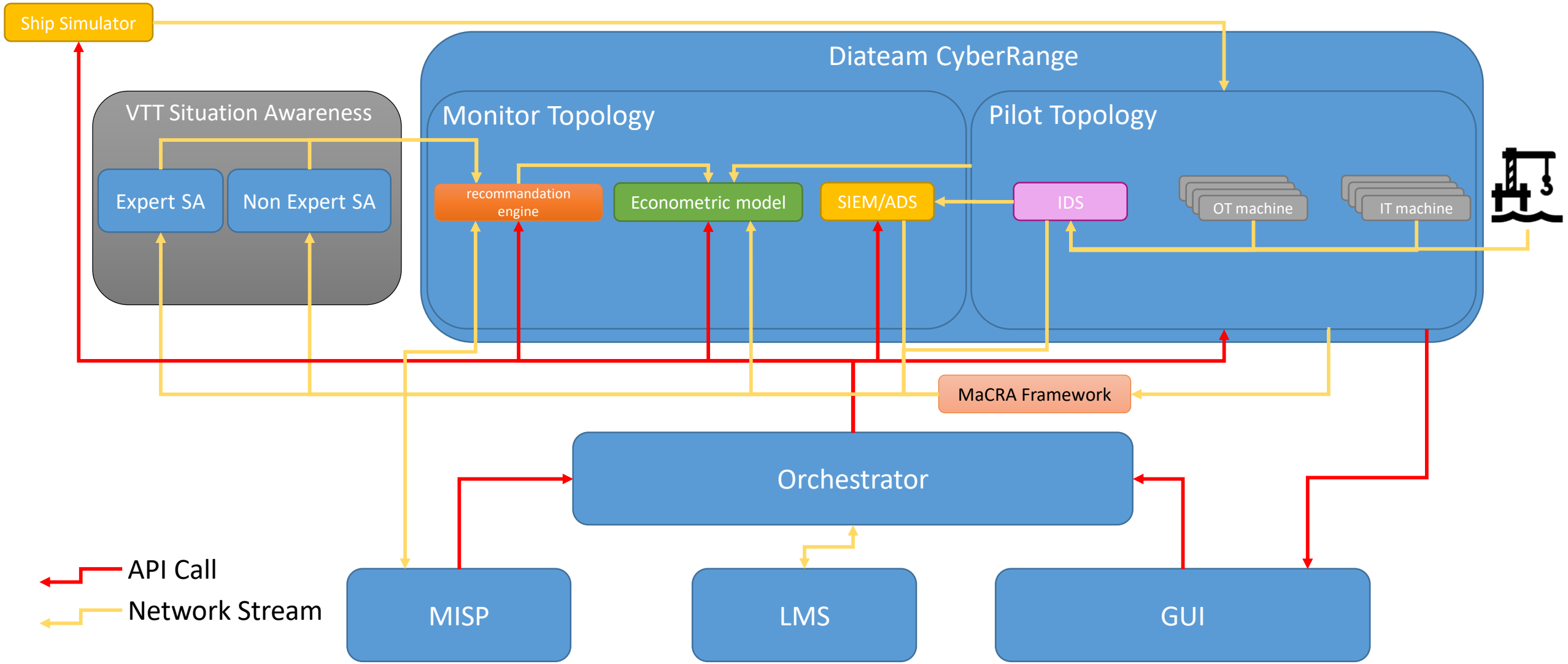
3 December 2020

Summary

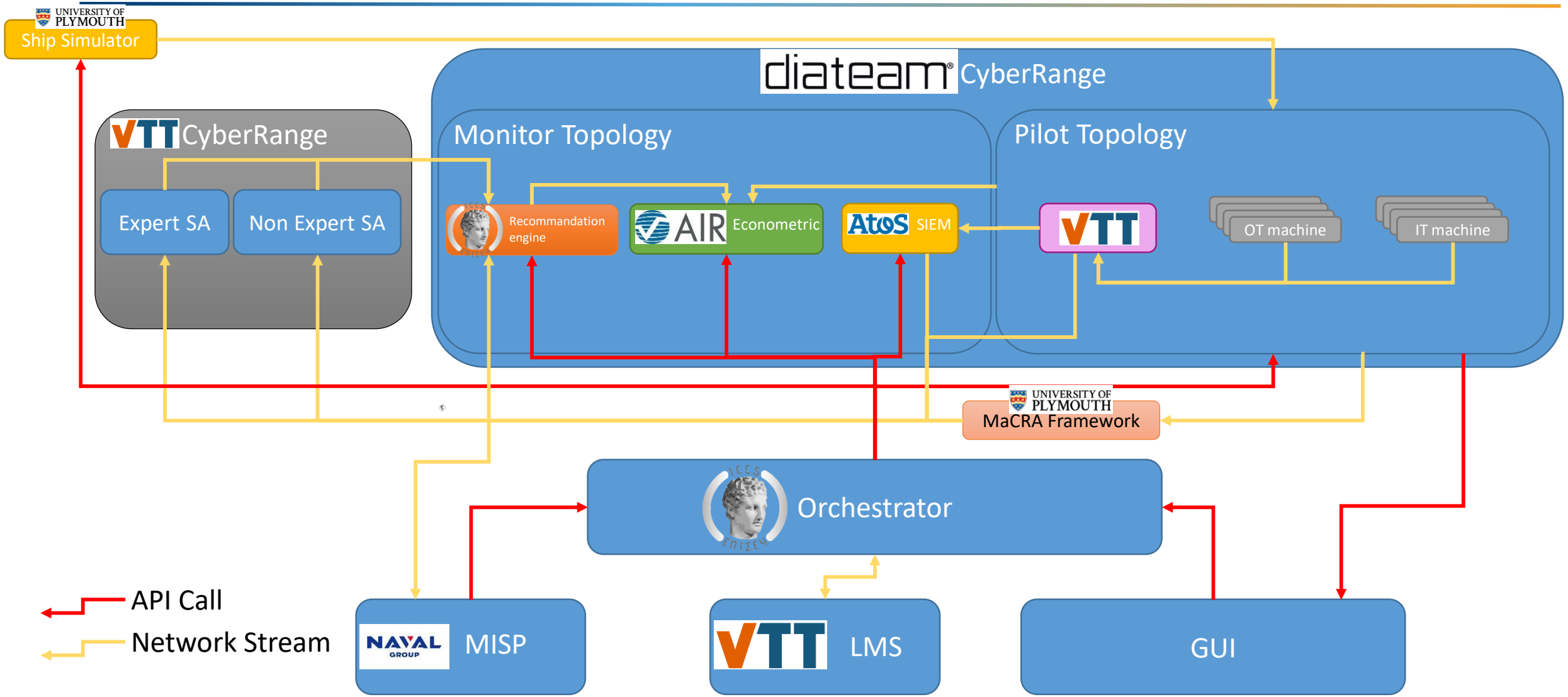
1. Global architecture
2. Main components :
    1. Orchestrator
    2. Diateam CyberRange
    3. VTT Tools
    4. Recommendation engine
    5. Economic model
    6. SIEM/ADS
    7. MISP
    8. Macra

Global architecture

Global architecture



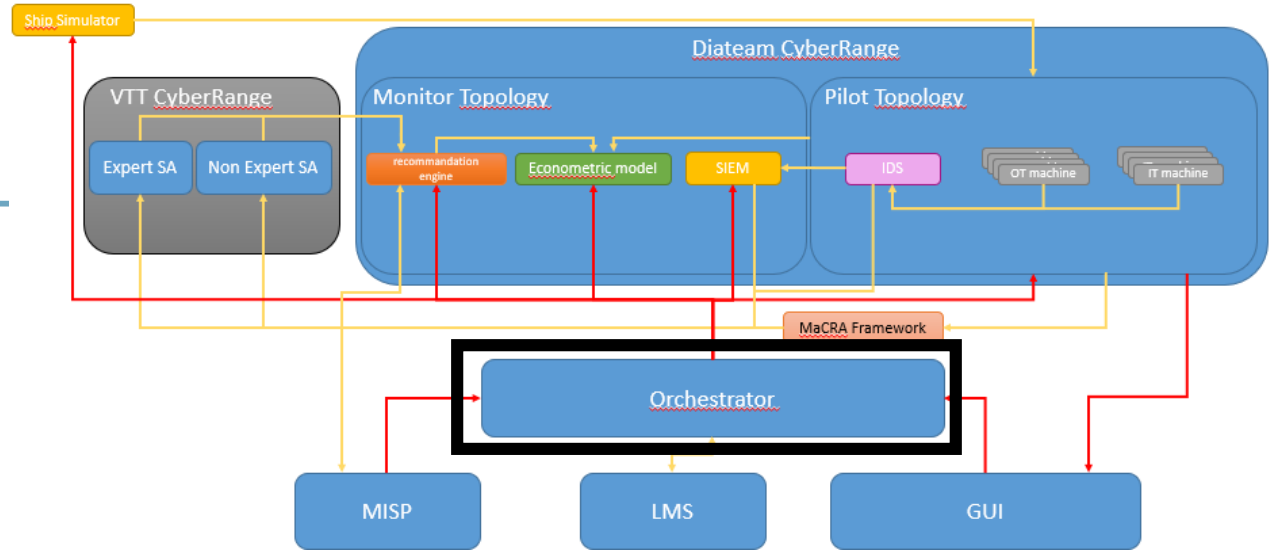
Global architecture - Partners

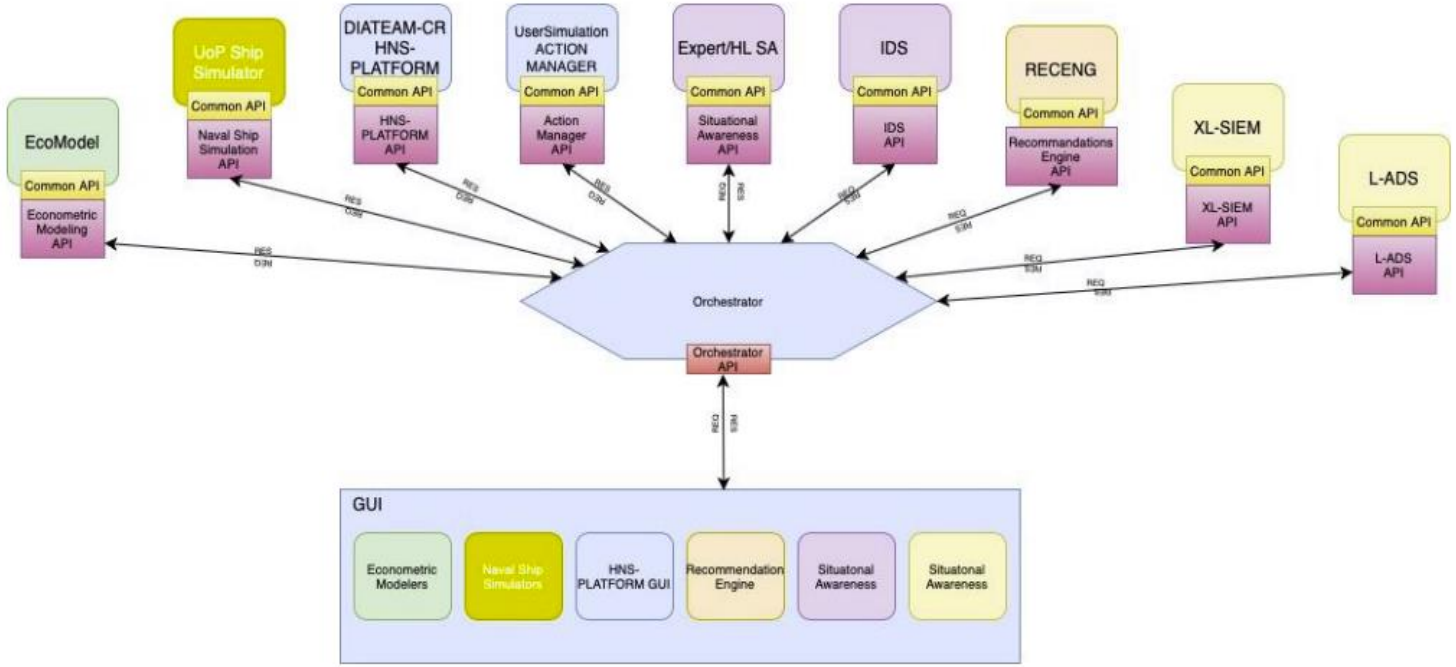


Technical modules

Orchestrator

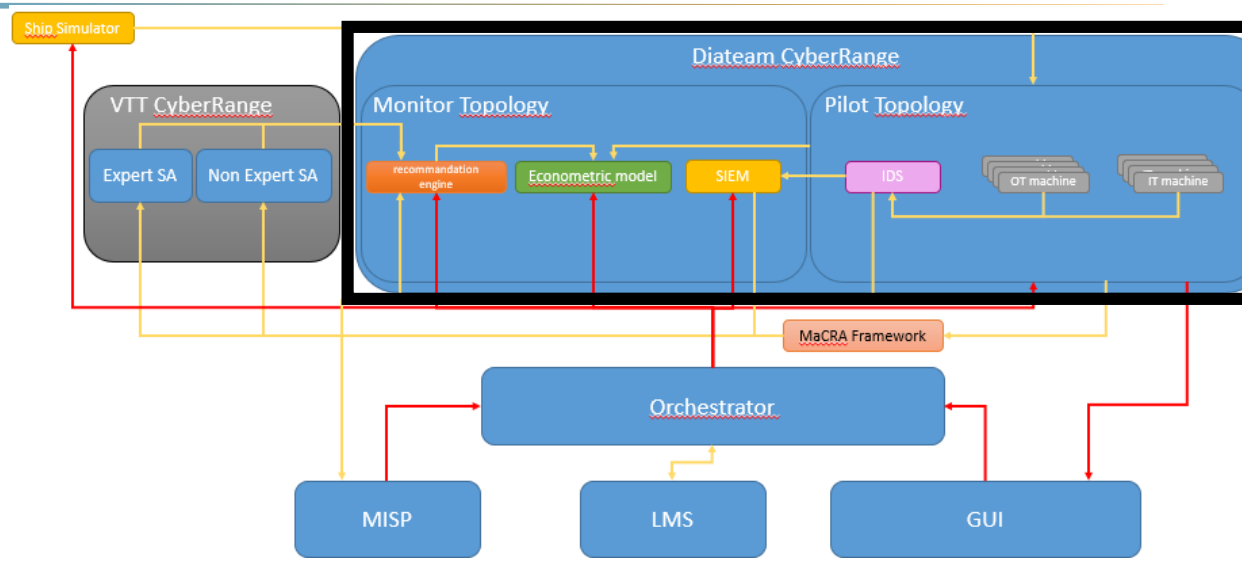
- Main controller
- Synchronise all components
- Create any topology
- Drive any scenario
- Common API

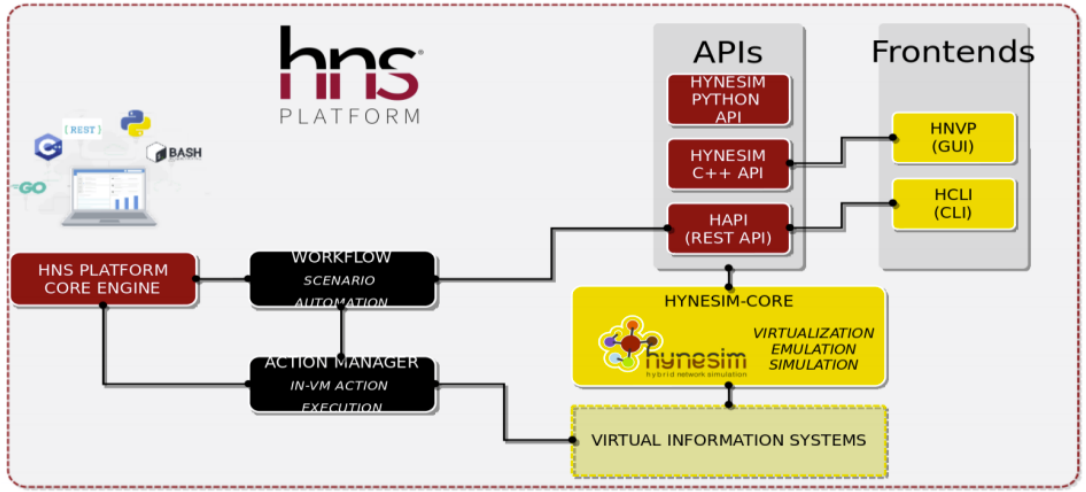




Technical Modules –Diateam CyberRange

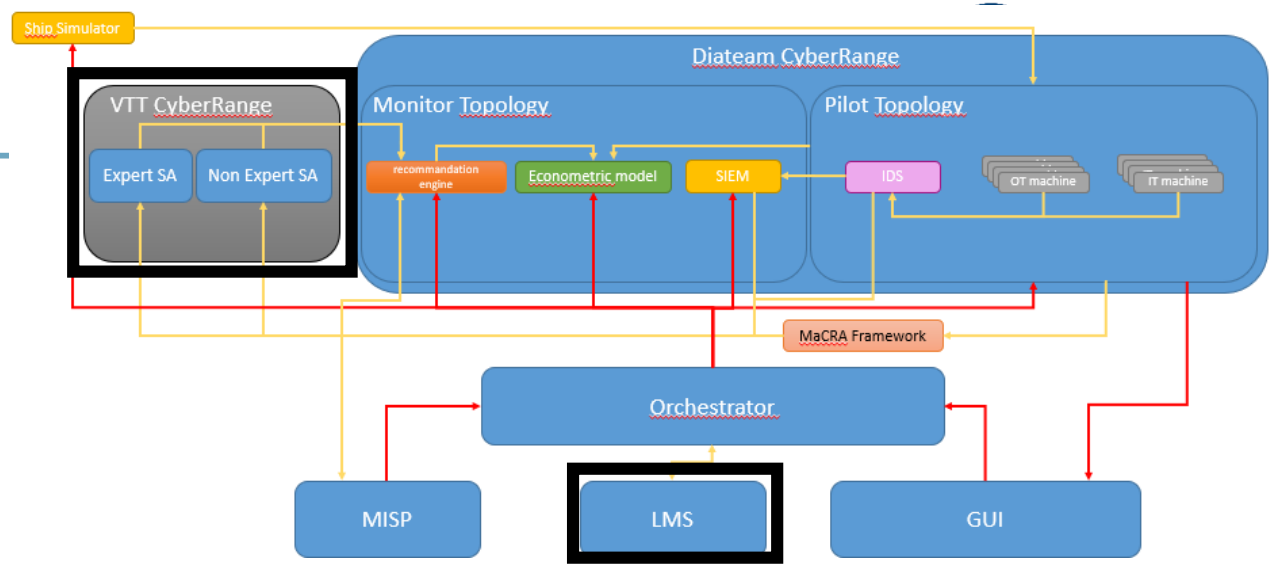
- Main cyber range:
  - Produce and manage virtual environment
  - Inter-connection with real IT or OT equipment
  - Create any virtual environment
  - View and interact with all virtual machine

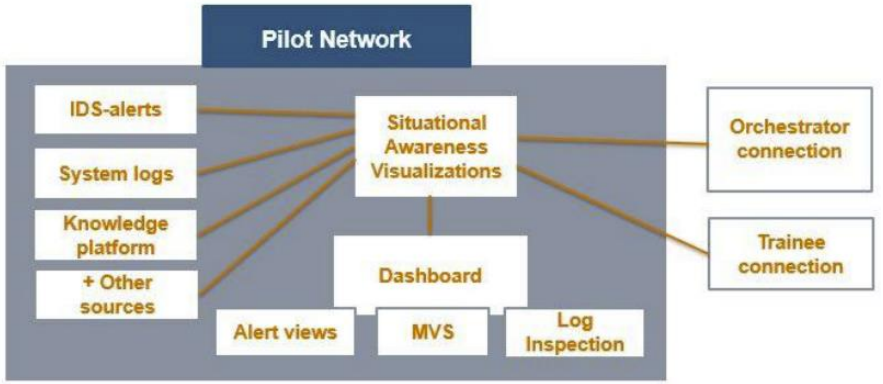




VTT tools

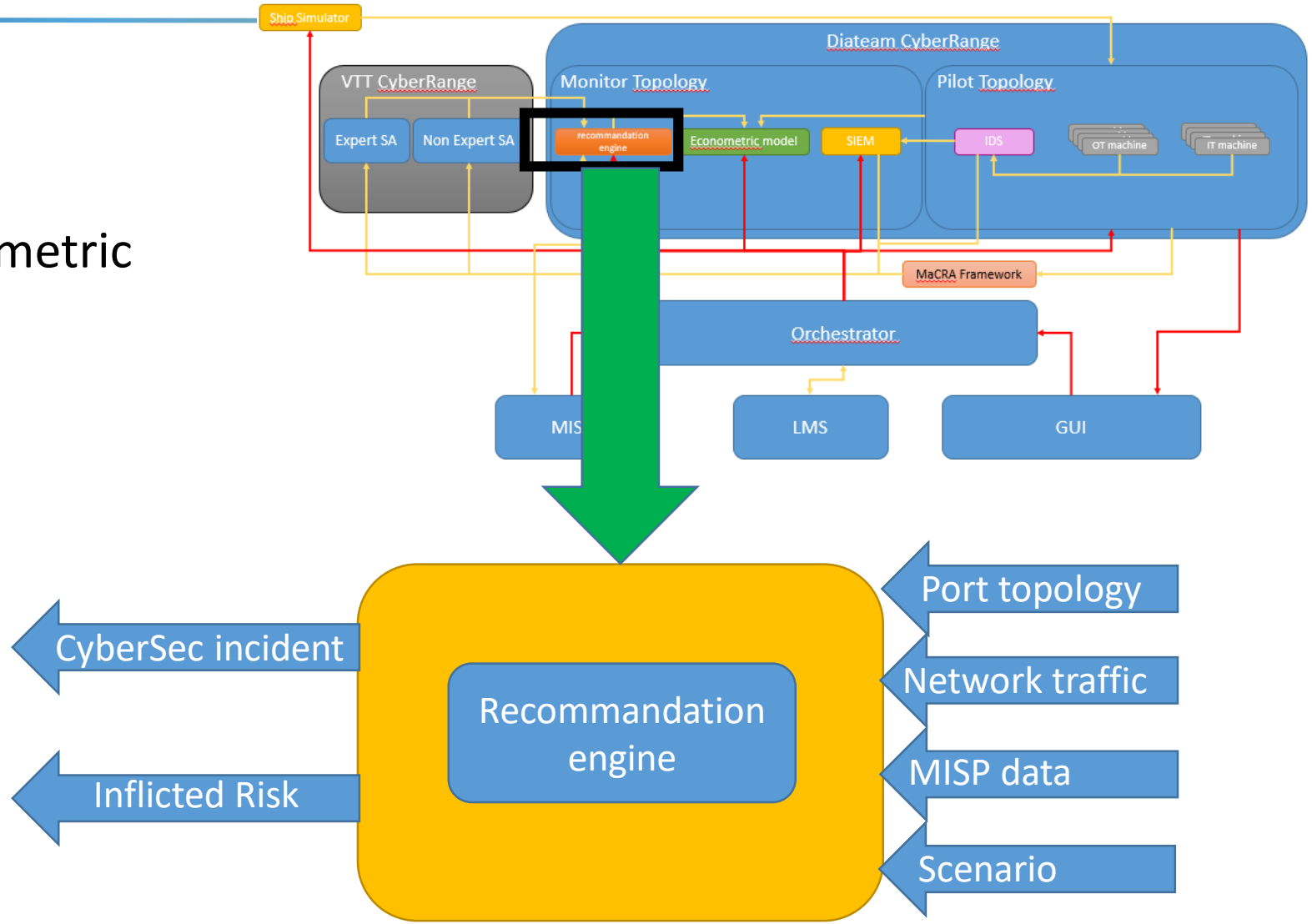
- Provide a collection of open source network monitoring tool and the LMS
- Take all security alert from all security component and give a clear dash board of the situation.
- Detect and capture evidence of cyberattack for situational awareness
- 2 modules : 1 for technical expert and 1 for high-level profiles



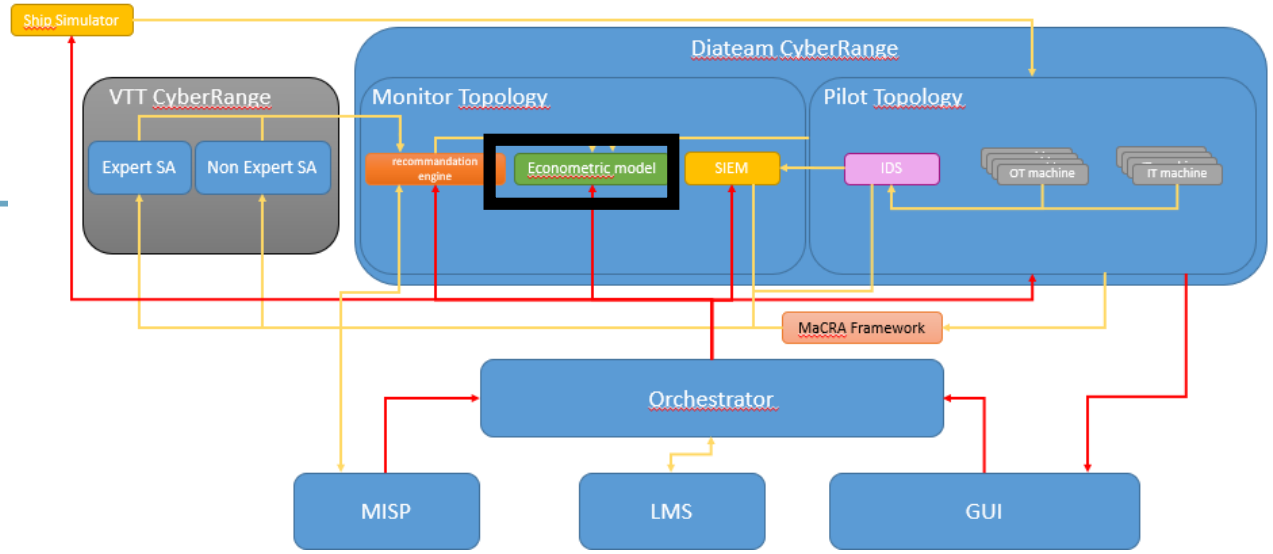


Technical Modules – Recommendation engine

- Concentrate lot of data
- Evaluate Inflicted Risk and econometric
- Non realtime evaluation

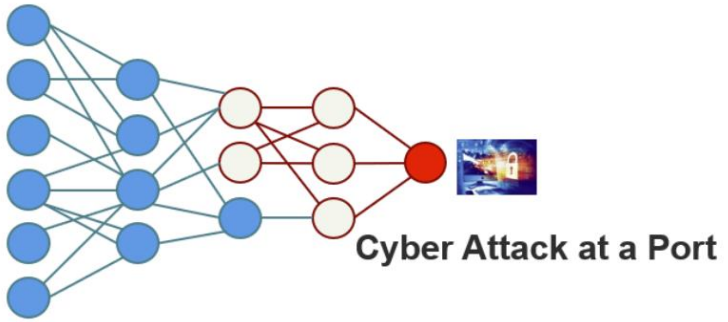


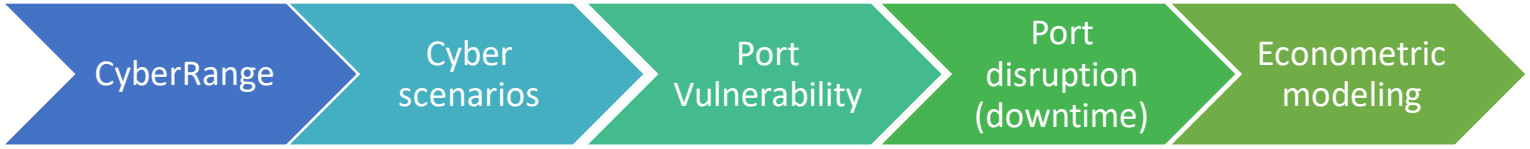
Econometric Model



Main econometric component

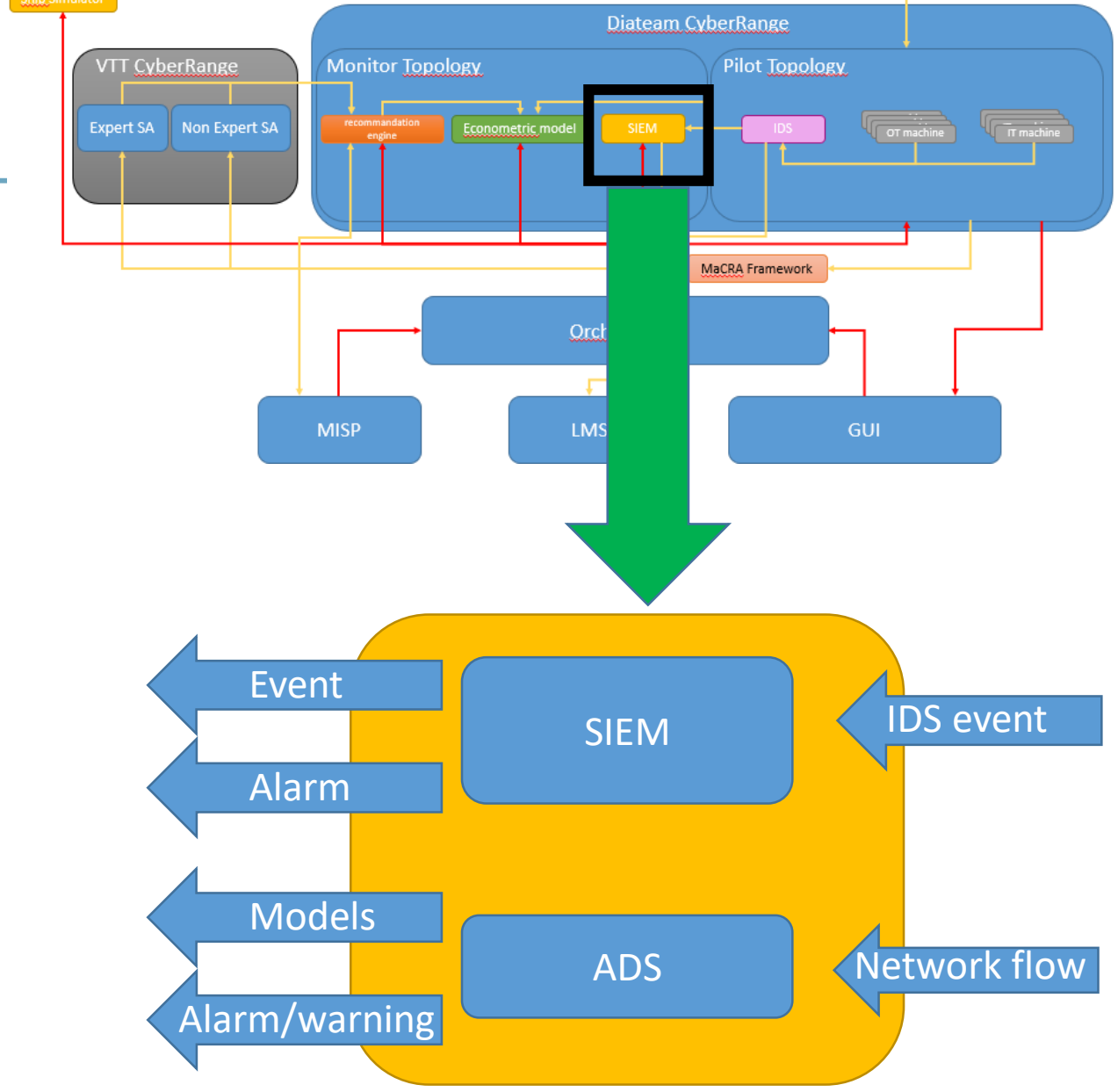
- Create Econometric
- Evaluate economical impact of an attack scenario
- Awareness of students





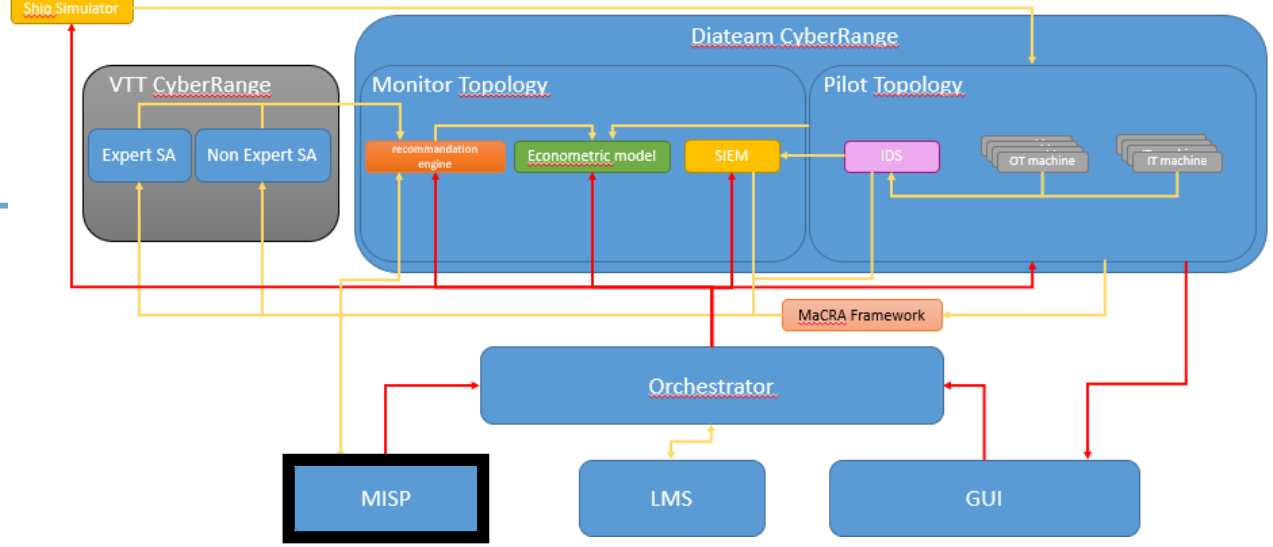
Technical Modules – SIEM/ADS

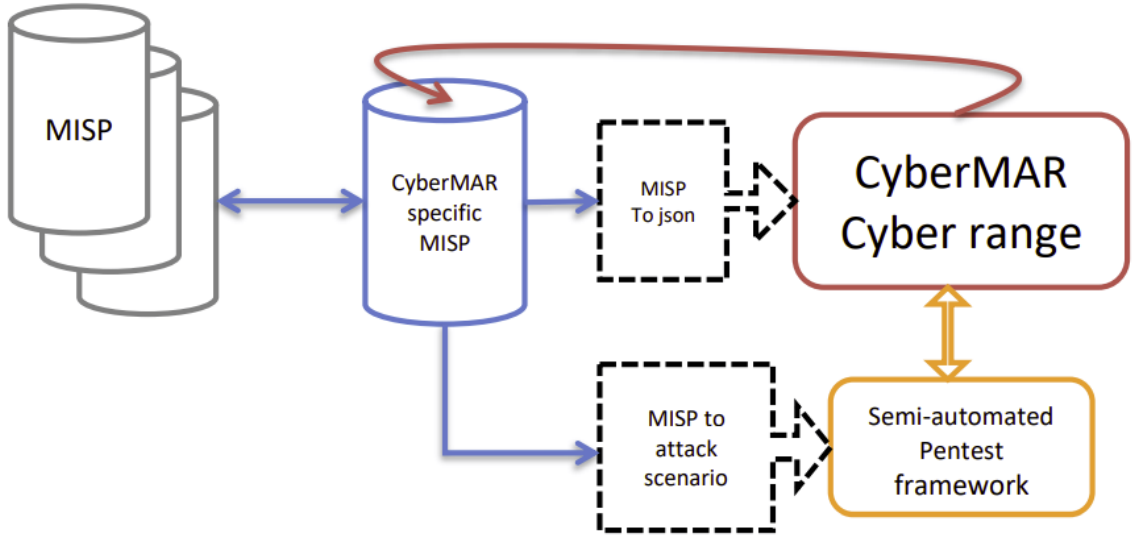
- Security monitoring platform:
  - Corelation of security event
  - Give status of the machine and the scenario
- Behavioural Analysis:
  - Check in real time network flow
  - Component identify where to update the system's configuration.



Technical Modules – MISP

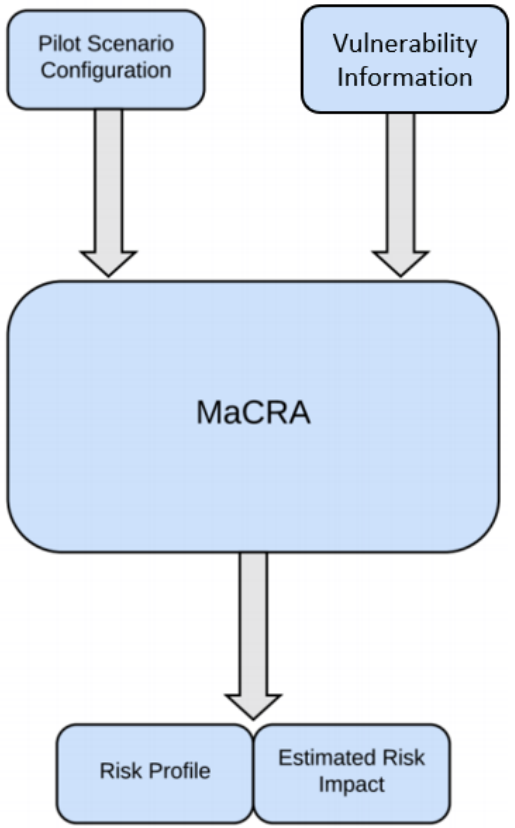
- Malware Information Sharing Plateform:
  - Based on real technical and operational data
  - Record and replay any kind of attack
  - Give a real cyber-attack scenario of maritime sector
  - Interconnect any CERT of MISP community

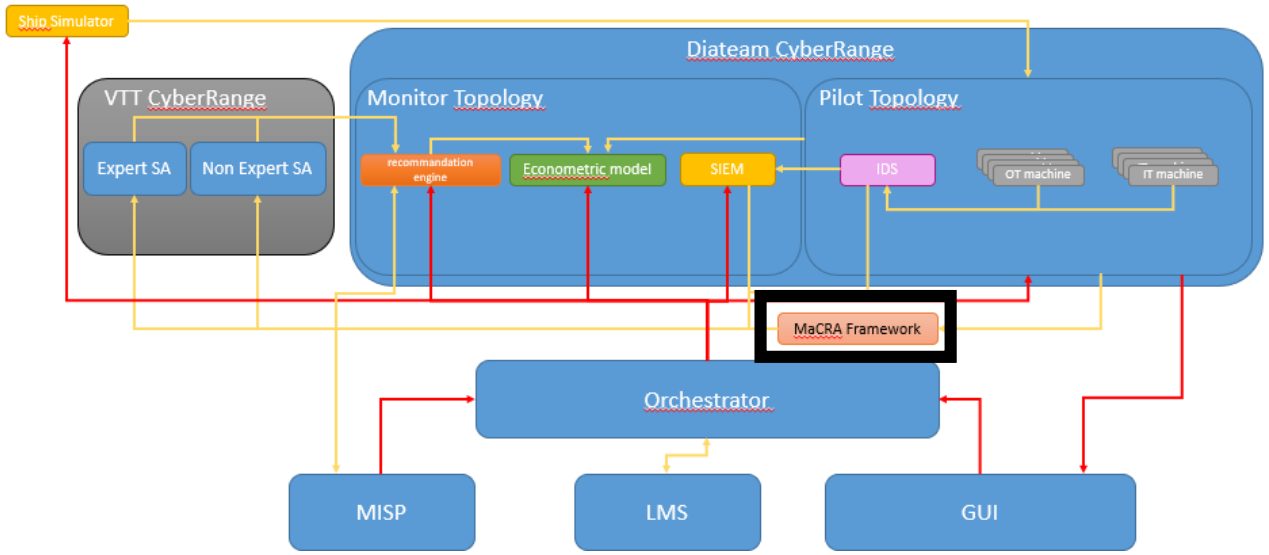




Technical Modules – MaCRA

- Framework of cyber-risk exposure:





List of pilots

- Valencia port: Energy sources
- Piraeus port : SCADA Container terminal
- University of plymouth : Ship simulator

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Aymerick Chincolla, Naval Group

Aymerick.chincolla@naval-group.com

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