



Cyber-MAR Vessel Pilot

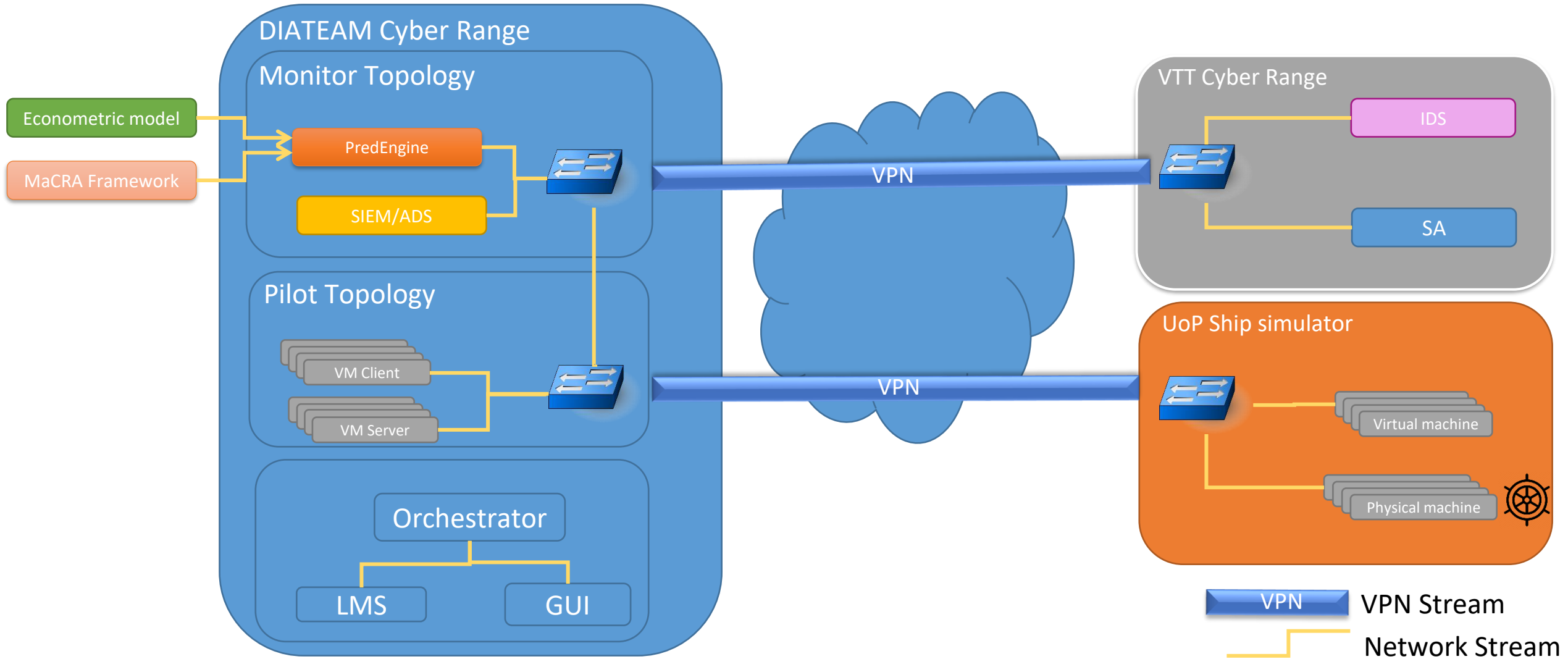
Cyber-MAR Platform and the Vessel Pilot

5th May 2022

Cyber-MAR Architecture

Aymeric Chincolla, Naval Group

Vessel pilot architecture



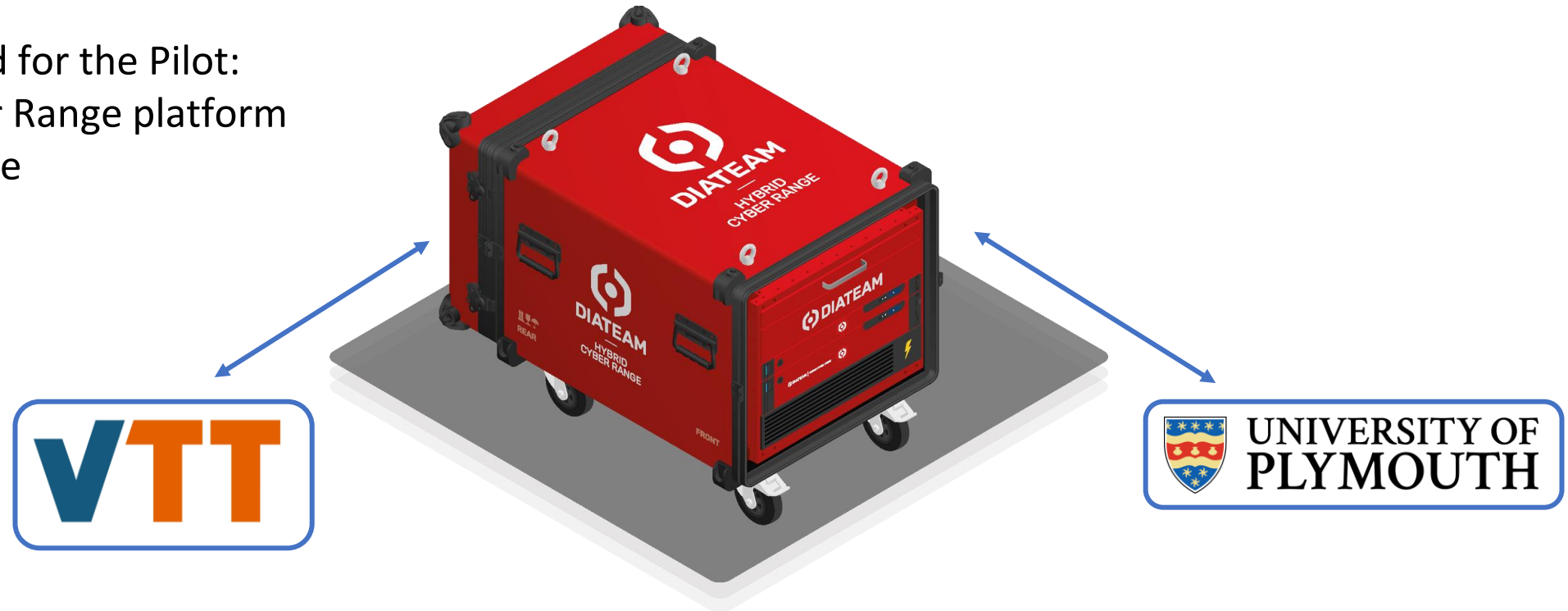
Cyber-MAR Cyber-MAR Range

Jonathan Winterflood, Diateam

SYSTEMS

Systems connected for the Pilot:

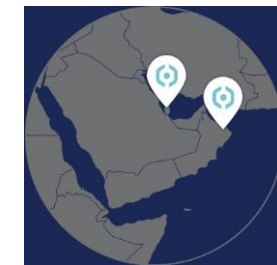
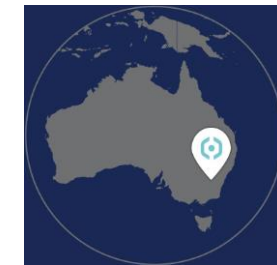
- DIATEAM's Cyber Range platform
- VTT's Cyber Range
- UoP's Simulator



SYSTEMS

Core: DIATEAM's Cyber Range platform

- Virtual environment to realistically simulate cyber systems for cyber combat training, system/network development, testing and benchmarking.
- Designed and developed by DIATEAM in Brest, France
- Founded 2002
- Industry-leading systems & solutions sold worldwide
- Universities / State services / Companies / Cybersecurity teams / ...



SYSTEMS



Core: DIATEAM's Cyber Range platform

Focus on training:

" REINFORCE THE HUMAN FIREWALL "

Our rule of thumb

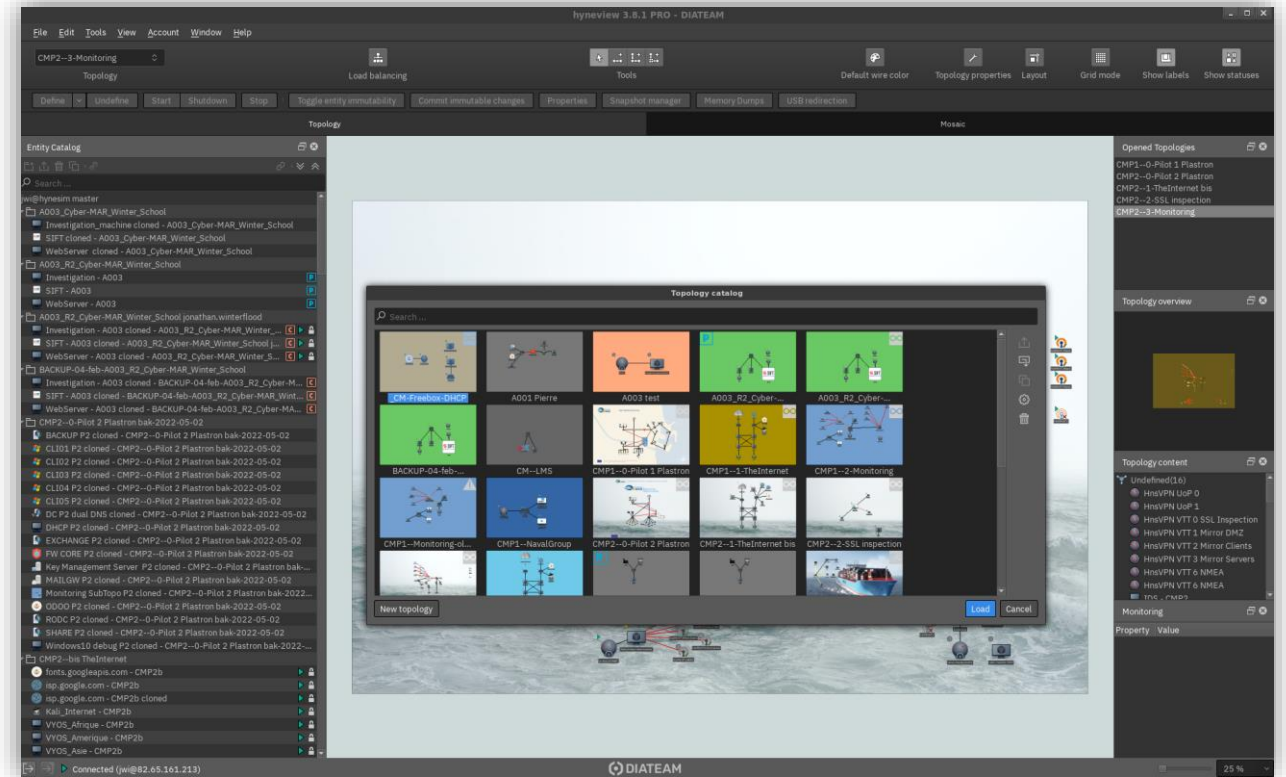
- 20% of well-designed equipment
- 80% of experienced security experts



SOFTWARE

Core: DIATEAM's Cyber Range platform

- Multi-user, scalable system
- Full graphical interface for building and interacting with simulated network topologies
- Hybrid connections: connect simulations to real-world equipment, other ranges via VPN
- API for building/controlling the simulations

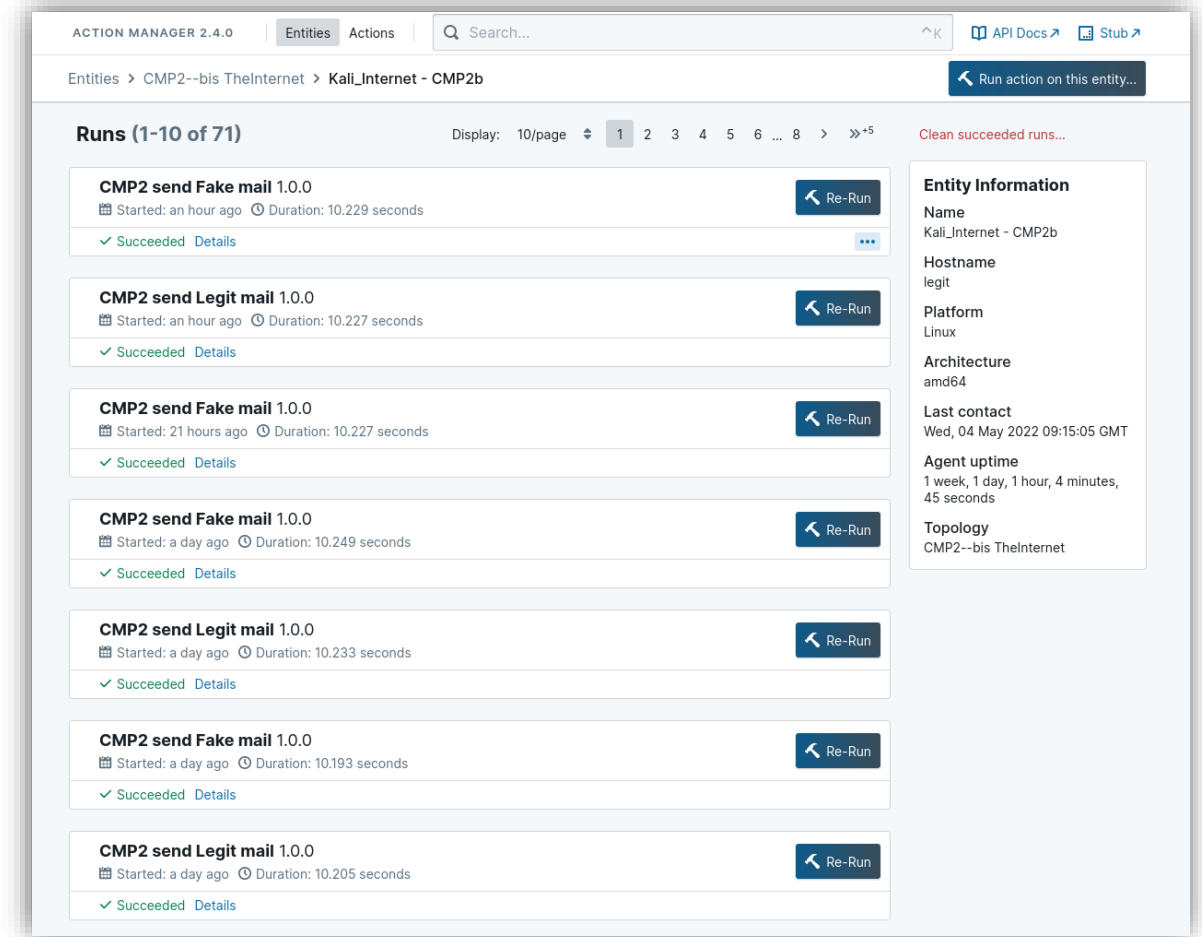


SOFTWARE

Integrated tools in DIATEAM Cyber Range:

ActionManager

- Executes actions inside the Machines in the simulation
- Independent of the simulated network
- API for programmatic control
- -> Execute preparation or scenario actions in the simulation



The screenshot displays the Action Manager 2.4.0 interface. The top navigation bar includes 'Entities' and 'Actions' tabs, a search bar, and links for 'API Docs' and 'Stub'. The current view is for the entity 'Kali_Internet - CMP2b'. A 'Run action on this entity...' button is visible. The main content area shows a list of runs (1-10 of 71) with columns for 'Runs (1-10 of 71)', 'Display: 10/page', and 'Clean succeeded runs...'. Each run entry includes the action name, start time, duration, and a 'Re-Run' button. The runs listed are:

- CMP2 send Fake mail 1.0.0 (Started: an hour ago, Duration: 10.229 seconds)
- CMP2 send Legit mail 1.0.0 (Started: an hour ago, Duration: 10.227 seconds)
- CMP2 send Fake mail 1.0.0 (Started: 21 hours ago, Duration: 10.227 seconds)
- CMP2 send Fake mail 1.0.0 (Started: a day ago, Duration: 10.249 seconds)
- CMP2 send Legit mail 1.0.0 (Started: a day ago, Duration: 10.233 seconds)
- CMP2 send Fake mail 1.0.0 (Started: a day ago, Duration: 10.193 seconds)
- CMP2 send Legit mail 1.0.0 (Started: a day ago, Duration: 10.205 seconds)

On the right side, the 'Entity Information' panel shows:

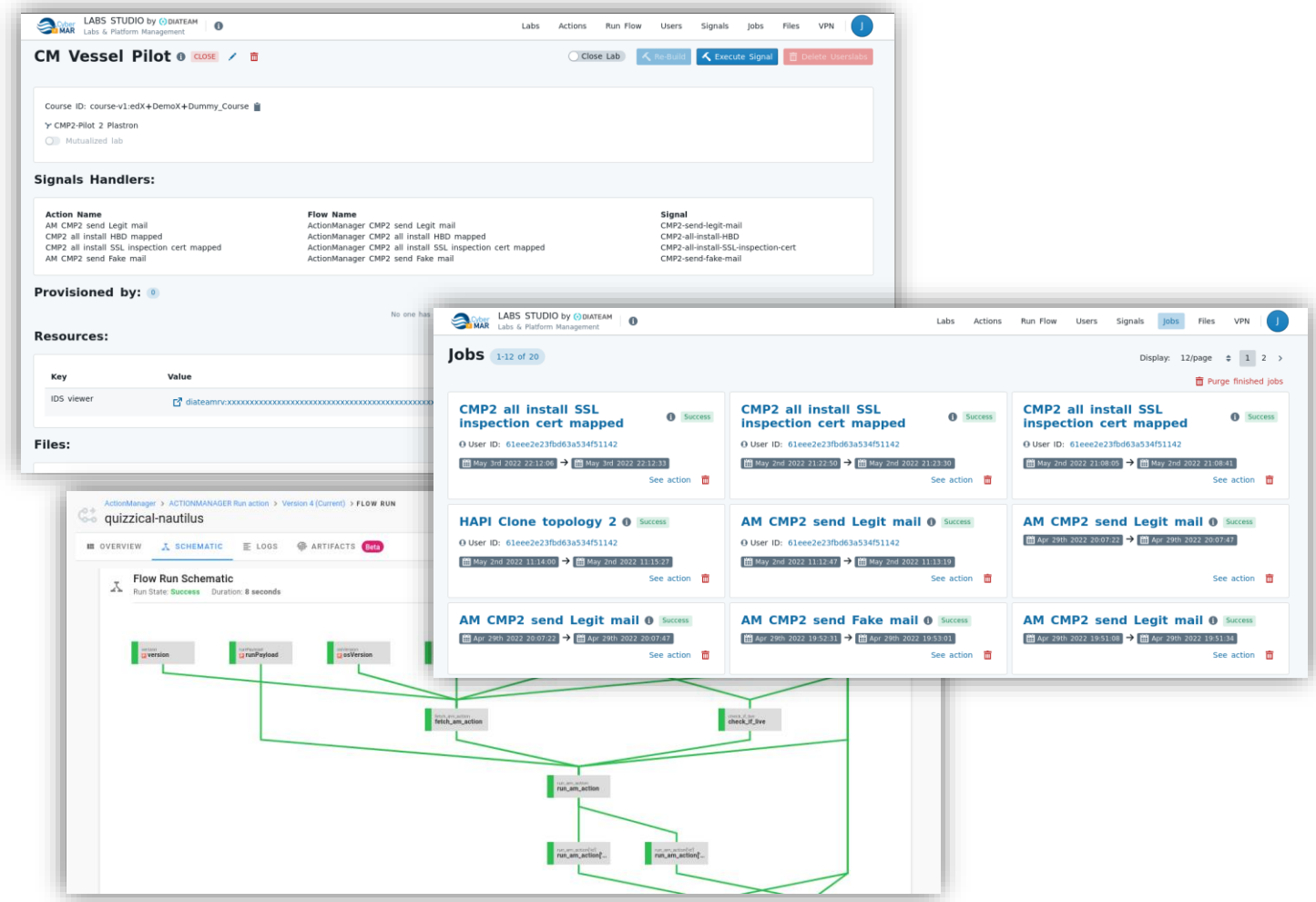
- Name: Kali_Internet - CMP2b
- Hostname: legit
- Platform: Linux
- Architecture: amd64
- Last contact: Wed, 04 May 2022 09:15:05 GMT
- Agent uptime: 1 week, 1 day, 1 hour, 4 minutes, 45 seconds
- Topology: CMP2--bis TheInternet

SOFTWARE

Integrated tools in DIATEAM Cyber Range:

Orchestrator & Workflow

- Manages the Cyber-Range simulations/via APIs:
 - Simulation control
 - Scenario & Scenario actions control
- Hands-On Labs:
 - Manages automatic provisioning of simulations for individuals/teams
 - Used for trainings/events, with integration to LMS systems
- Workflow system handles administrator-customizable action flows

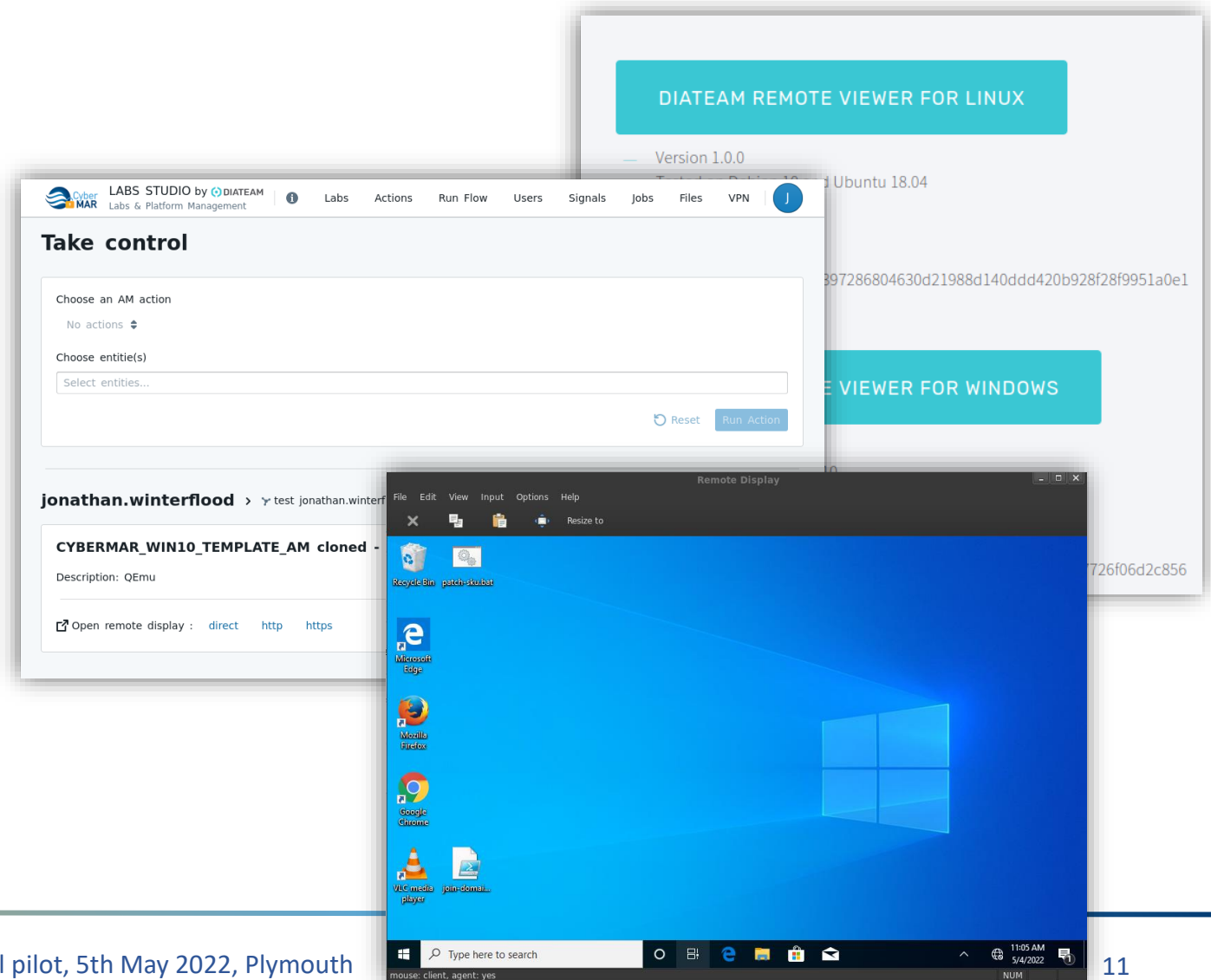


SOFTWARE

Integrated tools in DIATEAM Cyber Range:

One-click **Remote Viewer**

- Direct access to Virtual Machines from the Orchestrator Web UI
- Lightweight native client on Windows/Linux



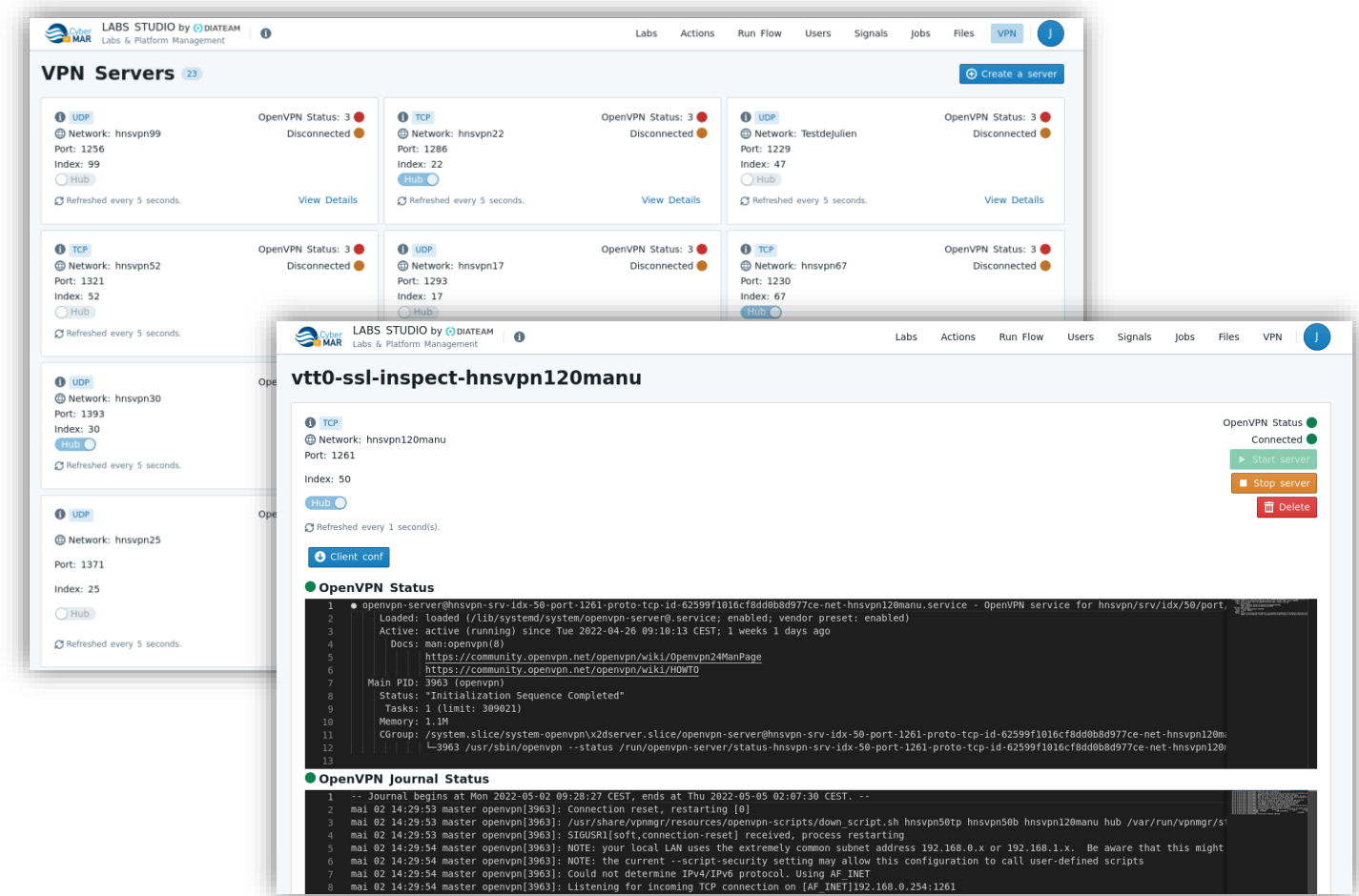
SOFTWARE

Integrated tools in DIATEAM Cyber Range:

VPN Manager

Creates and manages VPN servers on the platform:

- L2 VPNs connect directly into the simulated networks
- Connect the simulations across multiple ranges and platforms
- Connect individual users into simulations for training, etc.

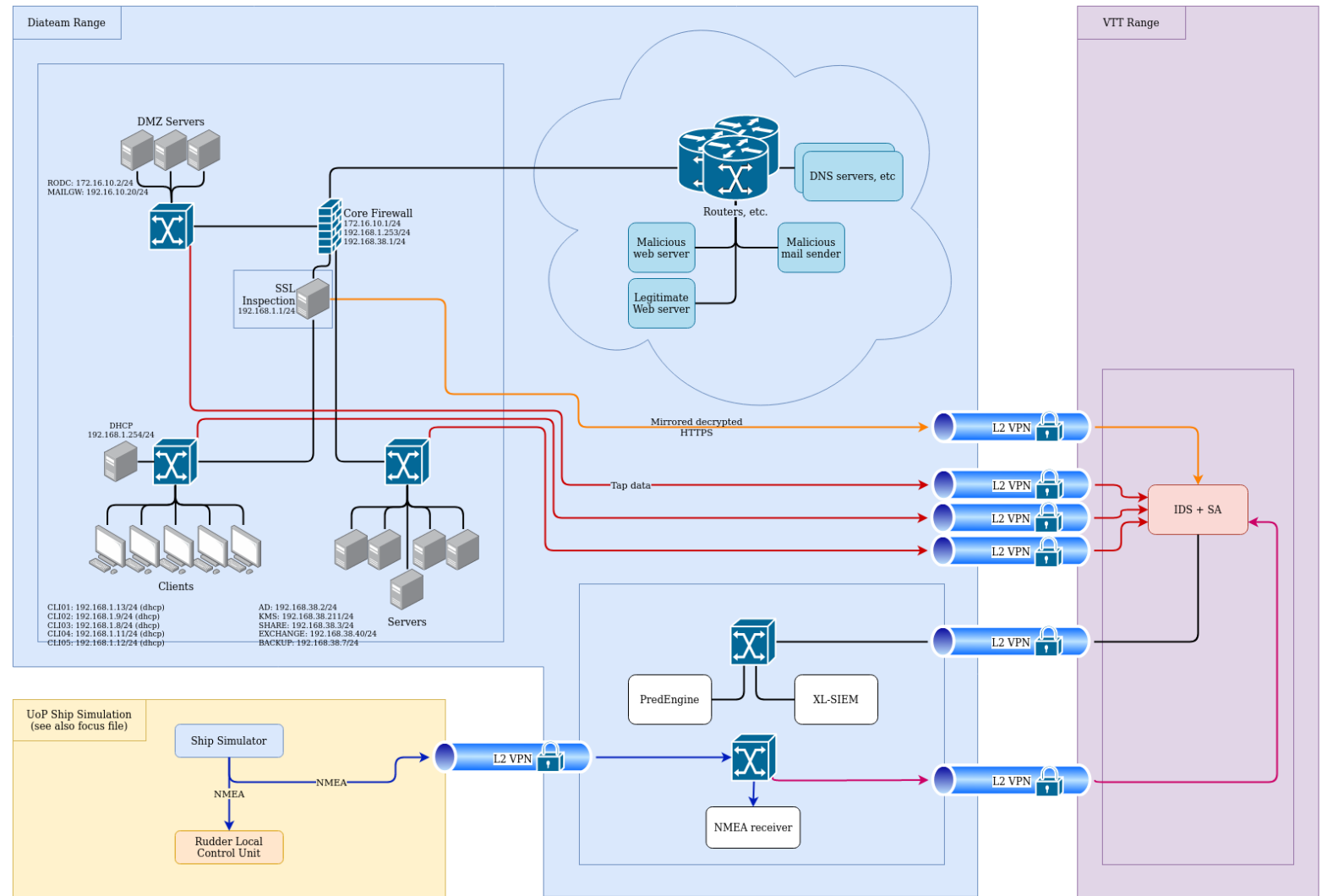


The image displays two screenshots of the 'LABS STUDIO by DIATEAM' interface. The top screenshot shows a 'VPN Servers' dashboard with a grid of server cards. Each card displays the protocol (e.g., UDP, TCP), network name, port, index, and status (e.g., Disconnected). A 'View Details' button is present for each server. The bottom screenshot shows a detailed view of a specific server named 'vtt0-ssl-inspect-hnsvpn120manu'. This view includes a 'Client conf' button, a status indicator (Connected), and a terminal window. The terminal output shows the OpenVPN service is active and running, along with journal logs indicating connection resets and listening for incoming TCP connections.

Simulated Network Topologies

Network Topologies for the pilot:

- Cyber-MAR Marine services:
 - Main network
 - The Internet
 - SSL Inspection
 - Monitoring
 - IDS/SA
- Ship: NMEA transfer to the IDS



Intrusion Detection and Situational Awareness

Jukka Julku, VTT


- Security Onion based Intrusion Detection System
 - Signature-based detection (Suricata)
 - Network security monitoring (Zeek NSM)
 - Situational Awareness dashboards for security events and alerts
 - Cyber-MAR specific extensions
- Deployed in VTT's cyber-range environment
 - Integrated to the other two cyber-ranges over VPN connections

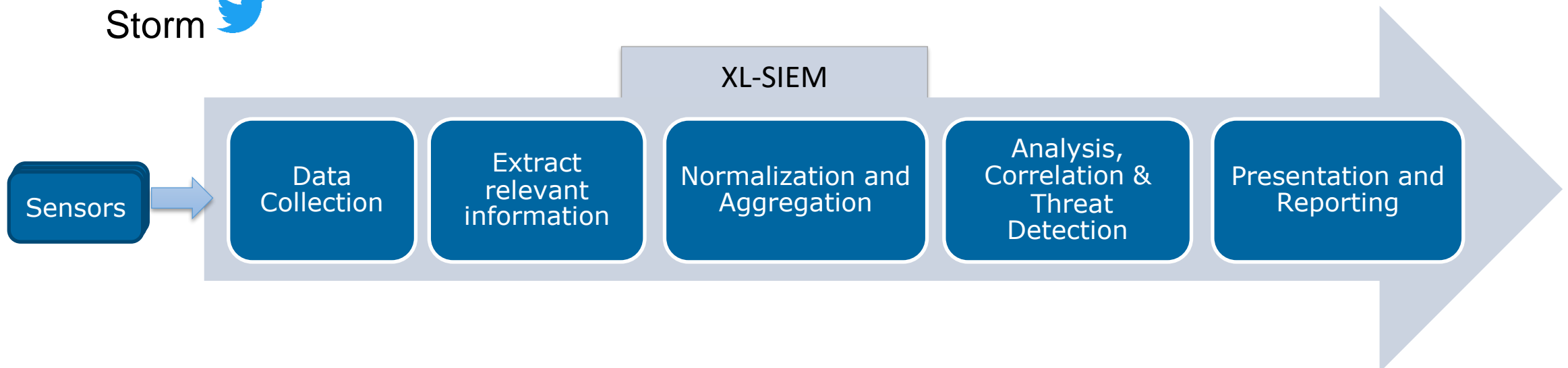
- The intrusion detection and network monitoring system in organization's IT network
 - Three network probes in routes between different network segments
 - SSL inspection proxy for outgoing HTTPS traffic
 - Signature-based detection with Suricata and Zeek engines
- Indicators of Compromise for the attack
 - Details of the traffic related to the malicious domain (e.g., DNS, HTTP)
 - Details of the malicious firmware binary (file hash)

- Intrusion detection systems are not that common in ship OT networks
 - The nature of used network technologies, e.g., serial data buses, and the lack of security features, makes reasoning about the traffic difficult
 - Domain specific protocols, e.g., various NMEA protocol versions
 - Most IDS tools available are for IP-based networks and Internet protocols
- Pilot scenario: NMEA 0183 traffic over TCP
 - Zeek dissectors for NMEA 0183 traffic, logging details into the IDS database
 - No actual intrusion detection in place
 - Situational Awareness modules for data visualization, e.g., for IR/FOR

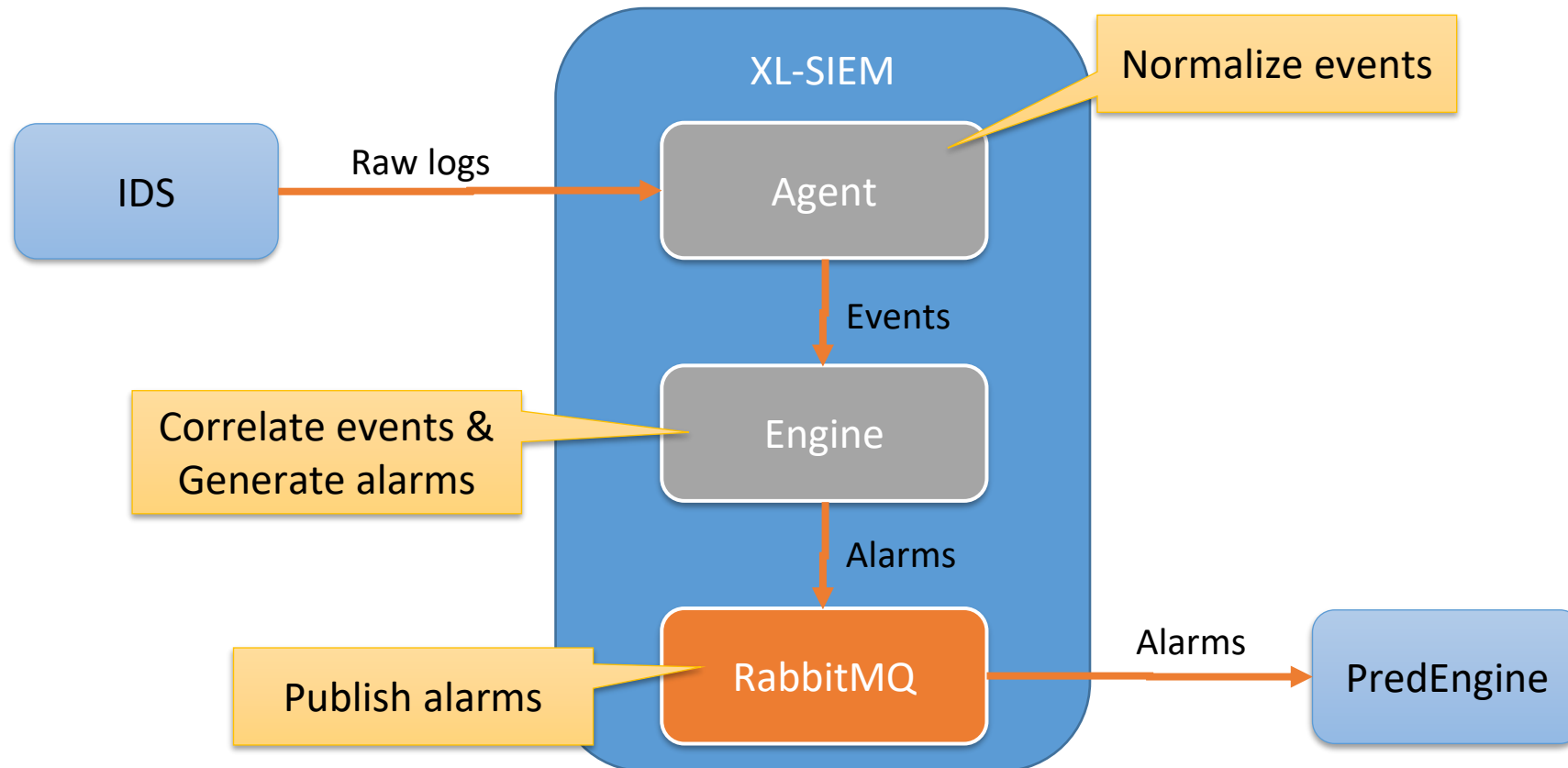
XL-SIEM Event Management System

Jesus Villalobos, ATOS

- SIEM = SIM + SEM = Security Information and Event Management
- Distributed and near real-time aggregation, dissemination and processing of events received from different data sources (sensors)
- Correlation of events based on correlation rules (Esper EPL) for generating alarms
- High resilience embedded by design -> XL-SIEM processes running on Apache Storm 



XL-SIEM in Vessel Pilot



XL-SIEM in Vessel Pilot – Alarm example

Correlation Rule

Directive SID *	11
Name *	Phishing Victim detected downloading malicious file
EPL Pattern	pattern [b=Phishing_mail -> every-distinct(a.src_ip, 300 seconds) a=Traffic_malicious_website -> c=Phishing_malicious_file (a.src_ip = c.dst_ip)]
Category	Alarm
Subcategory	Attacks
Reliability *	10
Priority *	5

Alarm

#	Alarm	Risk	Date	Source	Destination	Correlation Level
1	Phishing Victim detected downloading malicious file	10	2022-05-03 12:13:36	67.199.248.101:https	192.168.1.11:50408	2
2	ET TROJAN Blacklisted file SHA1 - northseaautomation phishing campaign	10	2022-05-03 12:13:36	67.199.248.101:https	192.168.1.11:50408	1
3	ET POLICY DNS Query for known malicious domain	4	2022-05-03 12:12:52	192.168.1.11:52694	192.168.38.2:domain	1
4	ET POLICY E-MAIL Content contains known malicious domain	4	2022-04-26 10:28:15	8.1.2.3:54340	172.16.10.20:smtp	1

Events sequence



Prediction Engine

Markos Antonopoulos, ICCS

Overarching Idea of the engine

- The ICCS Prediction Engine in Cyber-MAR aims at:
 - **Systematically model past knowledge** on attack behavior patterns
 - **Provide real-time predictions** concerning vulnerable parts of the infrastructure.
 - **Facilitate educated decisions** based on **past knowledge** and **possible risks and/or economic impacts** during an ongoing cyberattack.
- For each simulated attack scenario, the engine receives, processes and fuses information from:
 - IDS sensors
 - XL-SIEM output events
 - Risk models
 - Econometric models

Event and Event Sequence Modeling

- What the engine will perceive as an **event** is defined as a triplet of

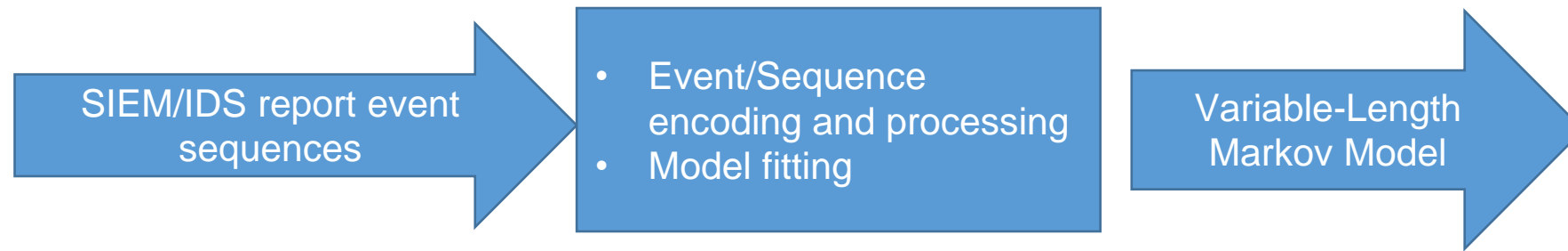
(Event_type, Source_subnetwork, Dest_subnetwork)

Where:

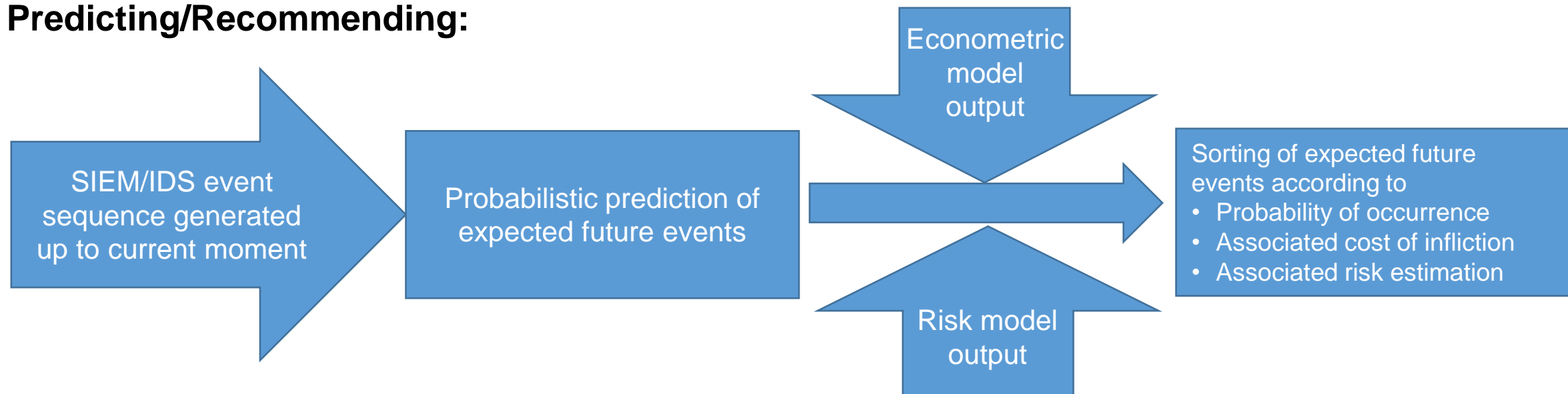
- **Event_type** is either the alert type of the corresponding IDS alert or the SID_NAME of the corresponding SIEM event.
- **Source_subnetwork, Dest_subnetwork** may be any relevant subnetwork of the infrastructure.
- Each **event** is matched to a **code word**, i.e. a string of characters. This essentially encodes a **sequence of events** into a **sequence of strings**.

Probabilistic Prediction Engine Logic

Modeling:



Predicting/Recommending:



Exemplary output

Timestamp	batch ID	origin (IDS/SIEM)	Description	Source	Destination	Probability lb	Probability lb(#)	Probability ub	Probability ub(#)	Delayed Vessels	Avg. Delay/Vessel (days)	Eq. Downtime (days)	Loss lb (USD)	Loss m (USD)	Loss ub (USD)
2022-05-02T11:57:05	2	IDS	ET POLICY HTTP Host header contains known malicious domain	Clients	OUT	0.35	26	0.6	5	0	0	0	0	0	0
2022-05-02T11:57:05	3	IDS	ET POLICY HTTP Traffic to known malicious IP address	Clients	OUT	0.2	5	0.33	6	0	0	0	0	0	0
2022-05-02T11:57:05	4	IDS	ET POLICY DNS Query for known malicious domain	Clients	Servers	0.12	26	0.12	26	21	2.3883	10.46154	1.3E+10	4.12E+10	7.53E+10
2022-05-02T11:57:06	1	SIEM	Malicious domain traffic detected	Clients	Servers	0.14	14	0.33	3	21	2.3883	10.46154	1.3E+10	4.12E+10	7.53E+10
2022-05-02T11:57:06	2	SIEM	Phishing Victim detected downloading malicious file	OUT	Clients	0.08	12	0.14	14	21	2.3658	9.384615	1.3E+10	4.12E+10	7.53E+10
2022-05-02T11:57:06	3	SIEM	Malicious domain traffic detected	Servers	OUT	0.07	14	0.08	12	0	0	0	0	0	0
2022-05-02T11:57:06	4	SIEM	Malicious domain traffic detected	Clients	OUT	0.07	14	0.08	12	0	0	0	0	0	0

Abbreviations: lb, lower bound
 m, mean value
 ub, upper bound
 #, number of samples for probability estimation

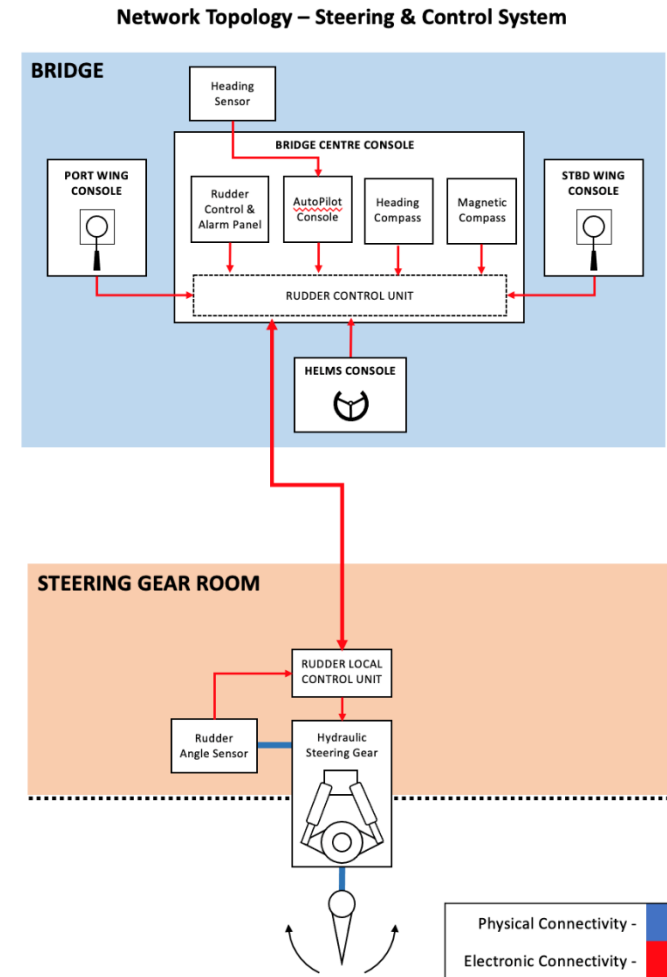


Ship Simulator, Rudder Physical Twin and MACRA

Kevin David, UoP

- Ship Simulator and Rudder Physical Twin

- The ship simulator is type certified ship simulator that is used within the platform to host the vessel, the vessel's immediate environment and to investigate how vessels would realistically behave when given different stimuli.
- The rudder control equipment is modelled by the rudder physical twin, which is an asset which models the rudder control and the rudder's physical operation.
- Rudder physical twin interfaces with ship simulator to create model of both ship's bridge and ships rudder control infrastructure.



(Dynamic) Maritime Cyber-Risk Assessment Framework – MaCRA

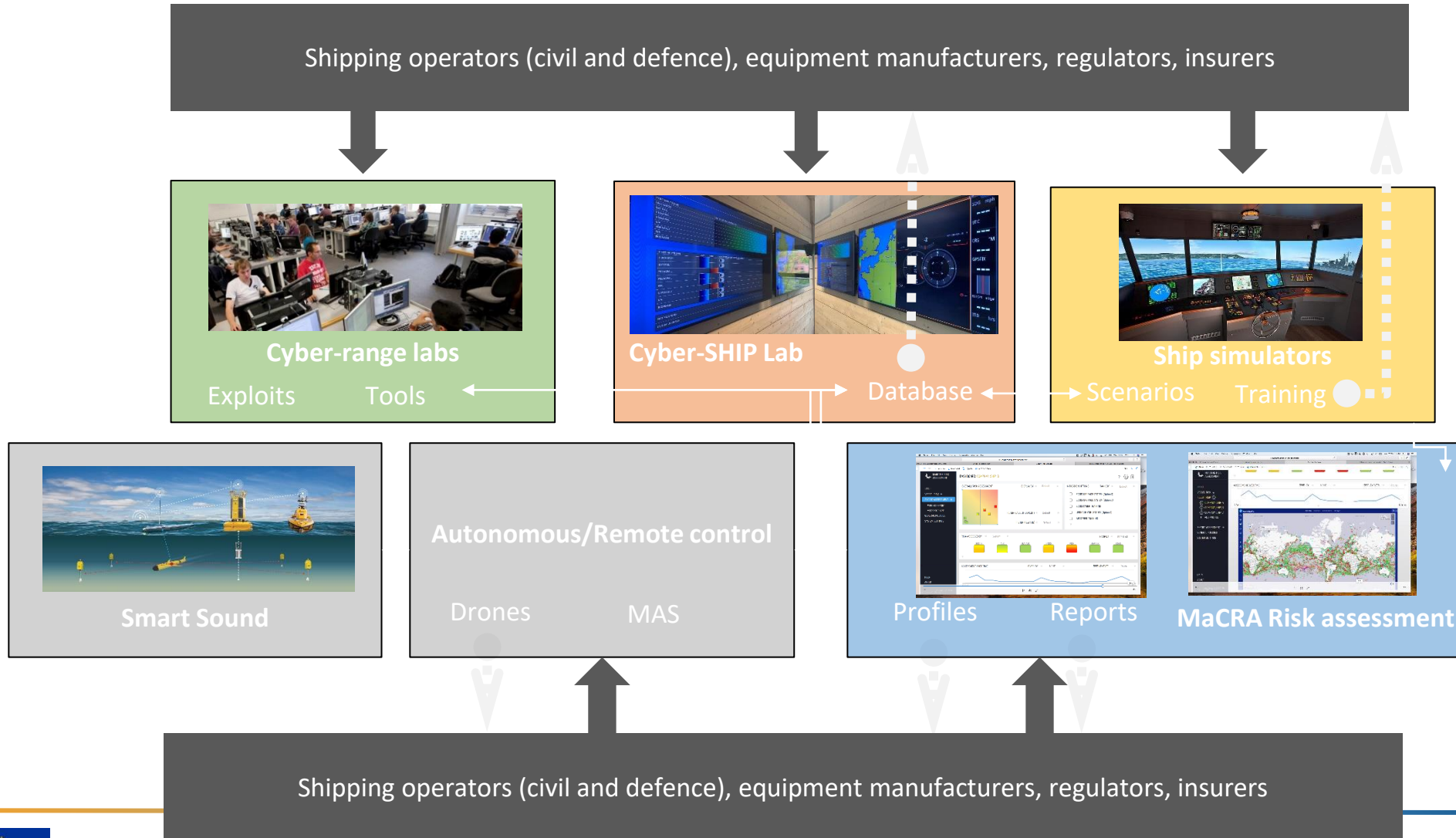


In order to analyse the cyber-risks that maritime ports and vessels face due to the possibility of cyber-attacks, it is important for the nature of the cyber-risks that these enterprises face to be characterised and cyber-risk models developed.

MaCRA provides a structured manner in which one can model and analyse risks. The framework provides tools that allow a stakeholder to assess, project (visualise) and analyse cyber risks.



Tools Within The Plymouth Uni Marine “ecosystem”





-  www.Cyber-MAR.eu
-  [Cyber_MAR](#)
-  [Cyber-MAR EU Project](#)
-  [Cyber-MAR](#)
-  info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION



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