HYBRID CYBER RANGES FOR MARITIME NEEDS

2nd ENISA Maritime Cybersecurity Conference

European Maritime Safety Agency, Lisbon

14th October 2022

ABOUT US

Founded in 2002, DIATEAM is an indie French software research and development company specializing in cyber security and innovative information systems.

> Founded in 2002 in Brest, France.

> R&D company specializing in computer security.

> Industry-leading systems for cybersecurity training and testing labs.

> Developing highly innovative cyber range solutions.

BREST

Guillaume PRIGENT
Chairman & Co-founder
(DIATEAM)

- DIATEAM relies on a team of around thirty highly qualified employees who are loyal to the company, the majority of whom (around 75%) are under the age of 40
- The company is recognized as one of the technological nuggets of the sector, worldwide.

CYBER RANGE EDITOR
&
CYBER CONTENT PROVIDER

DIATEAM

TLP:CLEAR

DIATEAM OFFERS ITS EXPERTISE IN EUROPE AND WORLDWIDE

As a pioneer of cyber combat simulation through cyber range environment, DIATEAM has been innovating continuously.

CATEGORIES OF CLIENTS

- State services, Ministries …

- Large companies

- Operators of vital importance

- IT services companies, audit, legal and accounting firms

- Universities, Digital schools, Tech Education

- ISS teams (SOC, CSIRT/CERT, Audit, Incident Response Group, Red Team/Blue Team, …)

TLP:CLEAR

WHAT IS A CYBER RANGE ?

A Cyber Range is a virtual environment that enables organizations to simulate cyber combat training, system/network development, testing and benchmarking.

› Virtualization, emulation and simulation of IT, IOT & OT/ICS infrastructures.

› Provides complete action learning/training platform.

› Provides a safe & secure, reality-based environment.

› Hybrid capacity allowing to interconnect real equipment.

TLP:CLEAR

MULTIPLE USES

Our solutions are designed and developed to meet a wide array of cybersecurity needs.

CYBER TRAINING SOLUTION

› Cyber Awareness

› Cyber Training

› Exercise & Crisis Management

CYBER LAB SOLUTION

› Deployment Testing / Benchmarking / Analysis

› Prototyping / Designing / Pentesting

› Patch Management / Security Assessment

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

› Hybrid connection between real IT/OT maritime/port systems and simulation

› High realism, open architecture, lower cost

› Fully featured navigation bridge

› Real ECDIS

› Simulated RADARs and 3D environment

› PNT systems (GPS)

› SATCOM and COMMs console

› CMS-like console

› Propulsion, air cooling management with real or virtual PLCs

DIATEAM

TLP:CLEAR

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

PORT HYBRID CYBER RANGES: CURRENT RESULTS

› Port smart-grid scenario

› Physical and virtual PLCs

› Fully featured IT environment

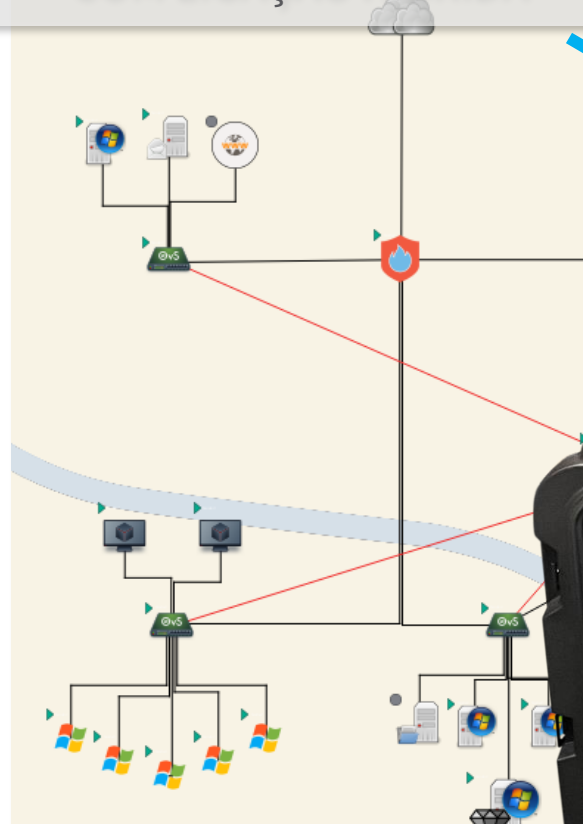› Advanced realistic ransomware scenario

Cyber MAR
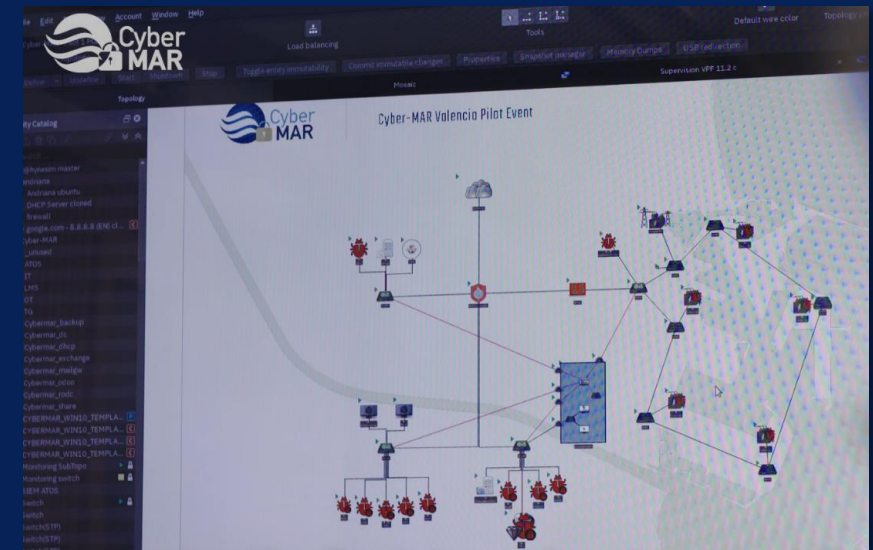
- SIMULATION OF A REMOTE ACCESS ATTACK ON PORT INFRASTRUCTURE

- Cyberattack on the Port of Valencia infrastructure (ransomware + smartgrid shutdown)

- European H2020 Project

TLP:CLEAR

LET'S PLAY THE GAME !

TARGETED TOPOLOGY

- IT segment: Server/Users/DMZ nets

- OT network: Scada Supervision (PcVue) & PLC (Physical & Virtual)

- Monitoring segment

- Remote attack from the Internet

CONTROLADOR INDUSTRIAL COM LIGAÇÃO HÍBRIDA

A COMPLETA VIRTUALIZAÇÃO DA INFRA-ESTRUTURA PORTUÁRIA

TLP:CLEAR

THE KILL CHAIN*

1. RECONNAISSANCE
2. WEAPONIZATION
3. DELIVERY
4. EXPLOITATION
5. LATERAL MOVEMENT
6. PROPAGATION
7. ACTION ON OBJECTIVE

PREPARATION — INTRUSION — ACTIVE BREACH

Source: Lockheed Martin

TLP:CLEAR

MANY THANKS !
QUESTIONS ?

TLP:CLEAR