Cyber-MAR Valencia Pilot Event

Simulation of a remote access attack on Port infrastructure

VPF, ICCS, DIATEAM, VTT, ATOS, NAVAL GROUP

16th December 2020

About DIATEAM | Valencia Pilot Event

- Founded in 2002 on the French MoD needs
- R&D company specialized in computer security
- Developing highly innovative cyber range solutions
- Industry-leading systems for cybersecurity training and testing labs

CYBER RANGE EDITOR

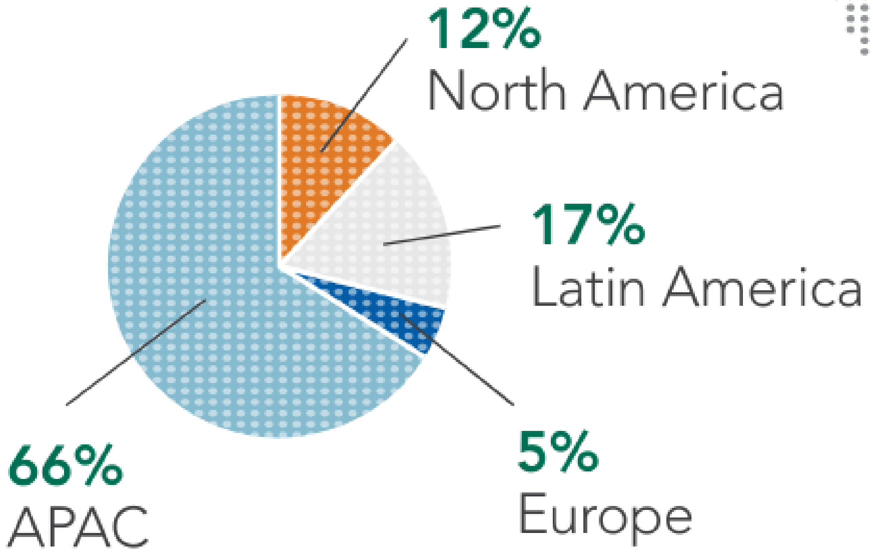
CYBER CONTENT PROVIDER

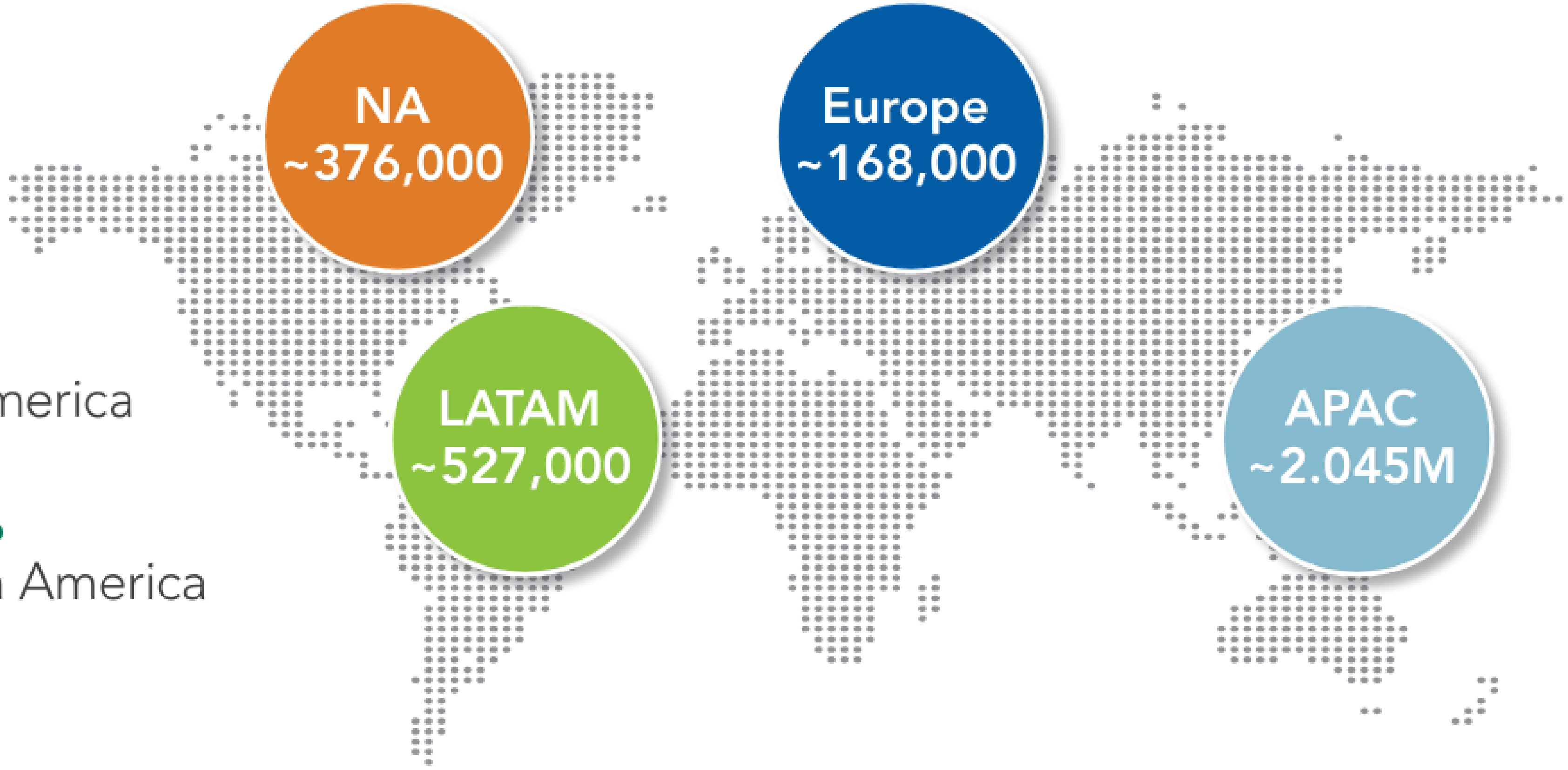
DIATEAM

MILITARY & CIVIL CYBERSECURITY SOLUTIONS

Cybersecurity workforce gap | Valencia Pilot Event

Global
~3.12M





Source: (ISC)²'s Cybersecurity workforce study, 2020

Human, the weakest link? | Valencia Pilot Event

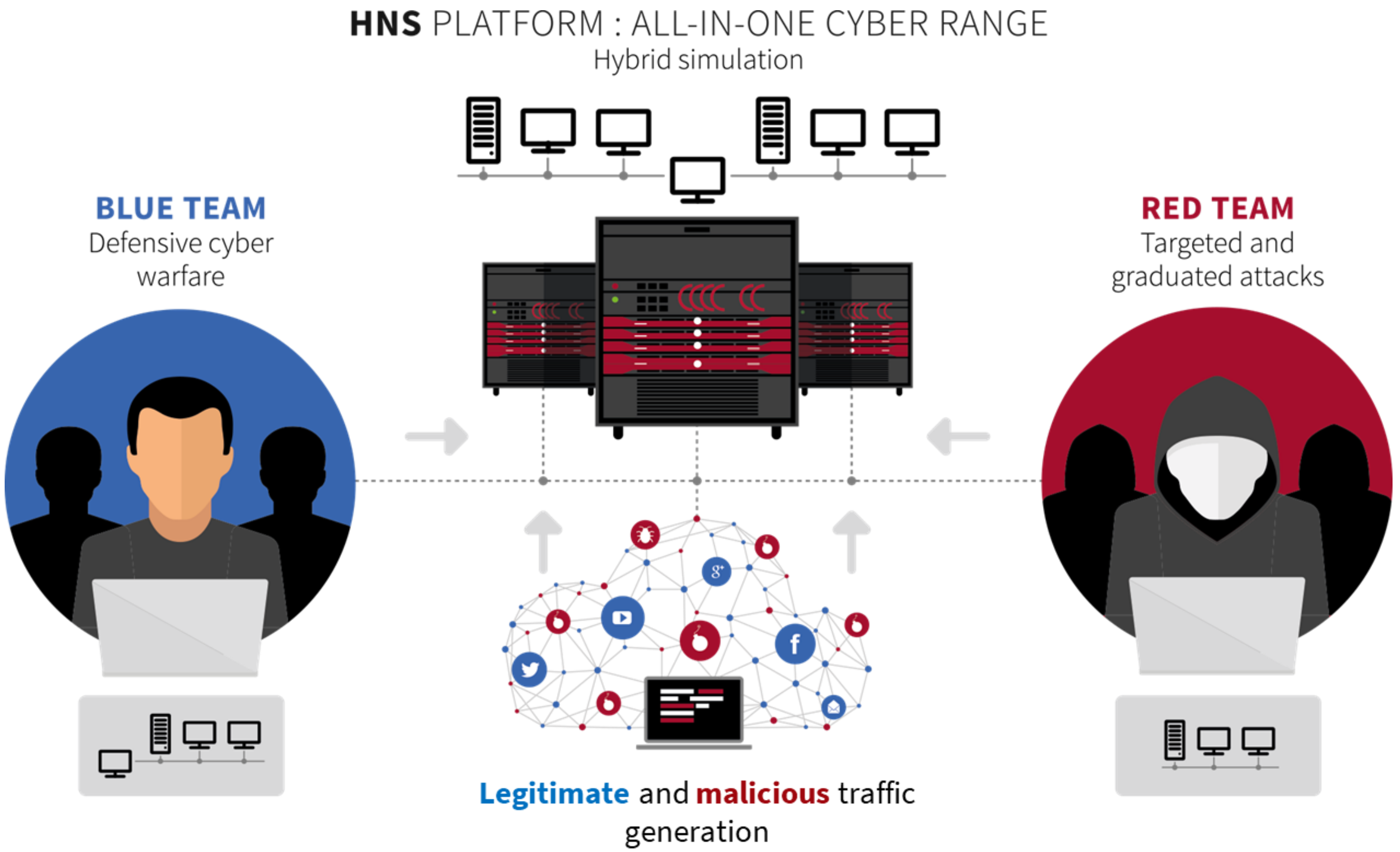
- **Cyber security efficiency relies mainly on employees awareness and operational team experience**

REINFORCE THE
« HUMAN FIREWALL »

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Cyber Range Benefits | Valencia Pilot Event

Overview of Hybrid Cyber Range



HNS PLATFORM : ALL-IN-ONE CYBER RANGE

Hybrid simulation

BLUE TEAM

Defensive cyber warfare

RED TEAM

Targeted and graduated attacks

Legitimate and **malicious** traffic generation

DIATEAM

MILITARY & CIVIL CYBERSECURITY SOLUTIONS

Cyber Range: what for? | Valencia Pilot Event

CYBER TRAINING CENTER	CYBER LABS SOLUTIONS	FILLING THE WORKFORCE GAP
Cyber Awareness	Deployment Testing / Benchmarking / « malware » analysis	Education
Cyber Training	Prototyping / Designging / Pentesting	Recruitment / Skills assessment
Exercise & Crisis Management	Patch Management / Security Assessment	Certification

Cyber Range Features | Valencia Pilot Event

- Virtualization, emulation and simulation of complex IT & OT networks
- Hybrid feature: connect real equipment to the simulation
- Easy to use through a user-friendly HMI
- Multi-architecture, multi-user, multi-view
- Network capture, USB redirection, memory dumps
- Fully automatable through APIs

Cyber-MAR Valencia pilot

Demonstration details

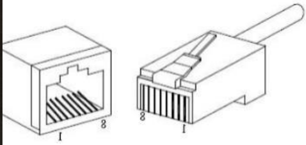
Jonathan WINTERFLOOD, DIATEAM

16th December 2020

Hybrid Cyber Range | Valencia Pilot Event

- 3 servers
- 768 GB RAM
- 108 cores / 216 threads
- 10 GbE internal network
- 16 hybrid ports

- Hybrid Capacity > PLCs



Cyber Attack Scenario | Valencia Pilot Event

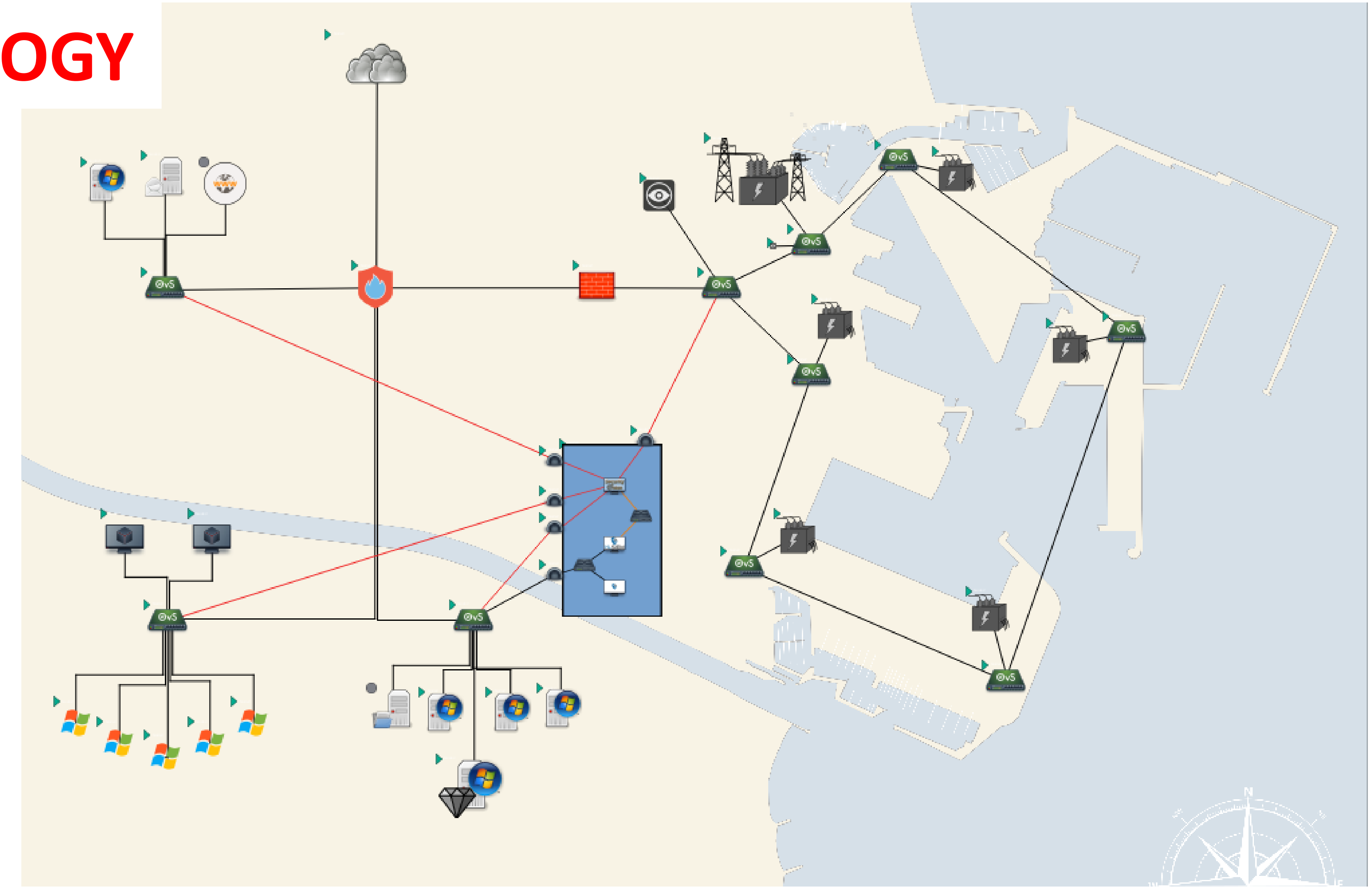
TARGETED TOPOLOGY

- IT segment:
Server/Users/DMZ nets

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

- Monitoring segment

- Remote attack from the Internet



Cyber Attack Scenario | Valencia Pilot Event

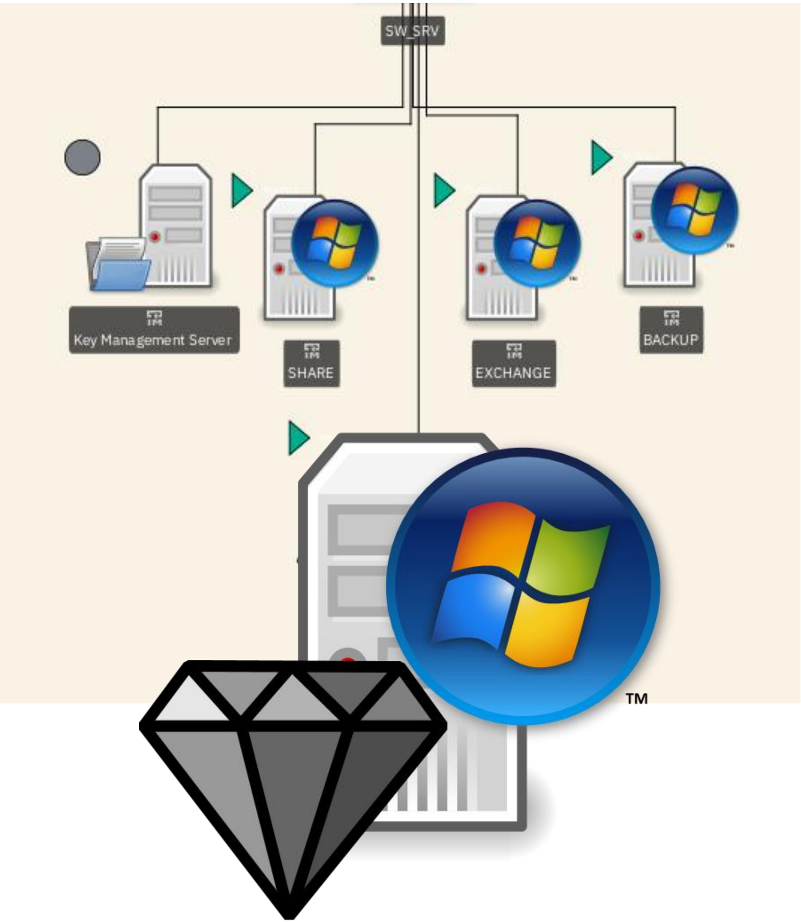
The Holy Grail for an attacker :

Active Directory (AD) aka Domain Controller (DC)

An administrator on the Domain Controller can perform any action on any machine in the Windows network.

- manage accounts/ passwords
- remotely execute software immediately (WinRM) or recurrently (Group Policy Object).

If an attacker were to gain access to the Active Directory, they could perform any action on any machine in the network

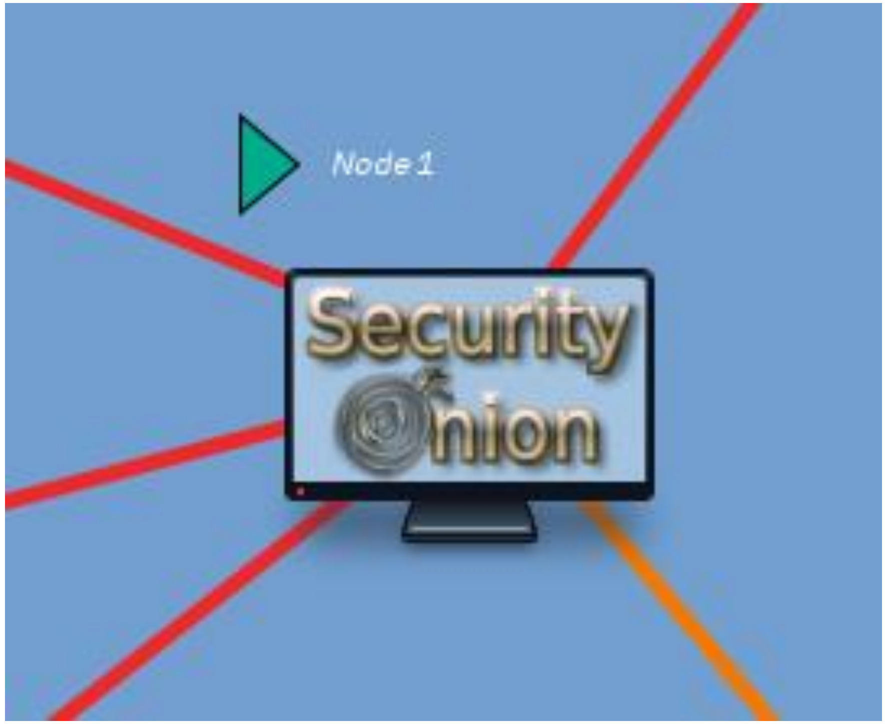


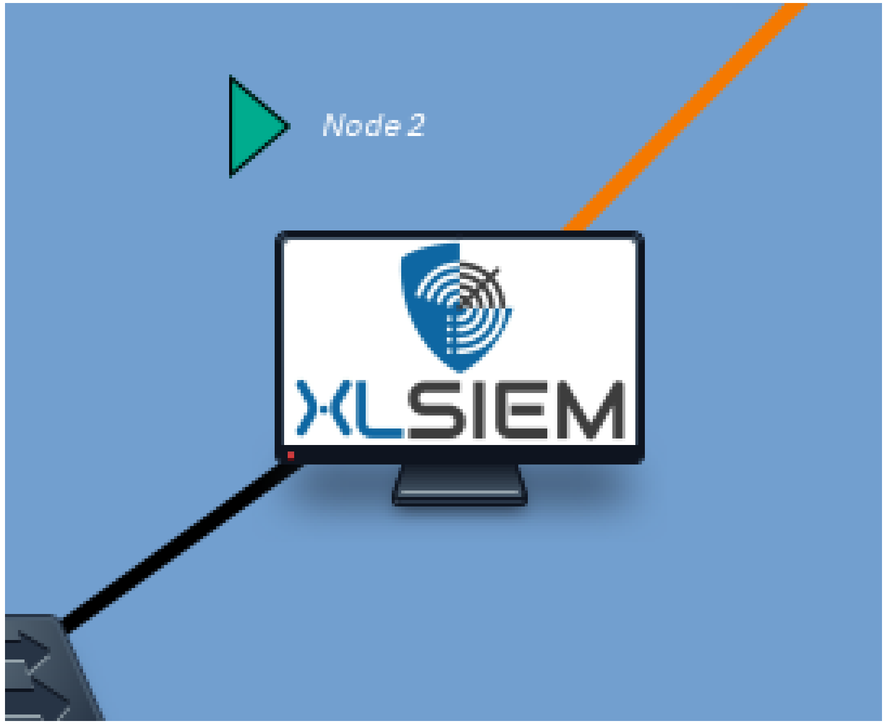
One AD to rule them all

Blue Team Topology | Valencia Pilot Event

Zoom on the monitoring network:

Blue Team : Monitoring tools by VTT & ATOS





Cyber MAR

Cyber-MAR Valencia pilot

Network Security Monitoring and Intrusion Detection

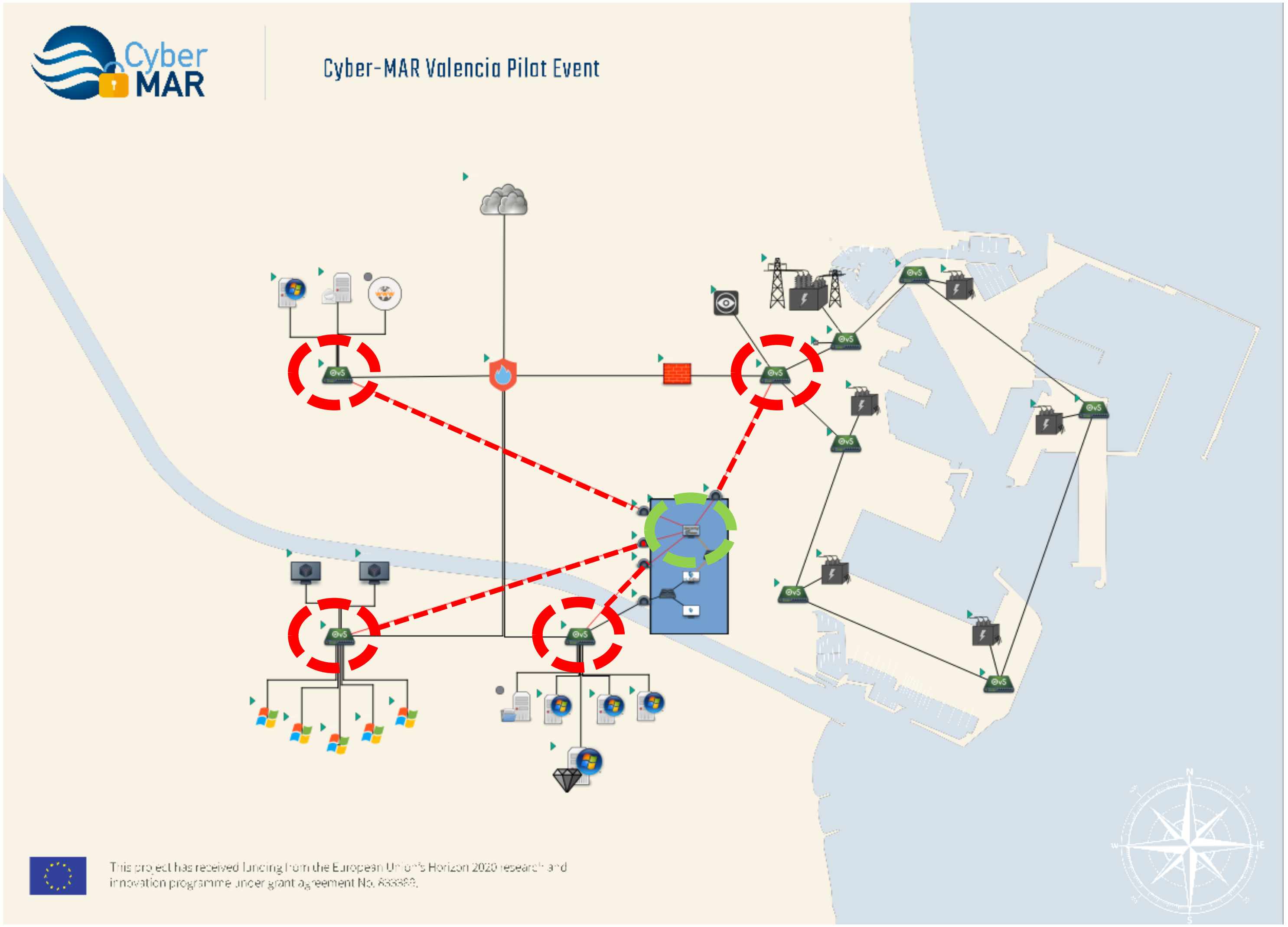
Jukka JULKU, VTT

16th December 2020

Blue Team | Valencia Pilot Event

- Network Intrusion Detection System (IDS)
  - Four sensors to capture and inspect network traffic
  - Security events and alerts generated according to detection rules
  - Master sends events to SIEM for aggregation, correlation, analysis, and actions
- No host-based IDS present in this pilot scenario

VTT



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

Blue Team| Valencia Pilot Event

- Security Onion is a free, open source, Linux distribution for threat hunting, enterprise security monitoring awareness, and log management
- Easy to setup in minutes
  - Graphical setup Wizard
  - Evaluation mode and Production mode
  - Scalable, can be distributed
  - Good documentation, community support
- Collection of tools for network and host-based security monitoring and analysis
  - E.g., Snort, Suricata, Zeek, Logstash, ElasticSearch, Kibana, Sguil, WireShark, NetworkMiner

https://docs.securityonion.net

Cyber-MAR Valencia pilot

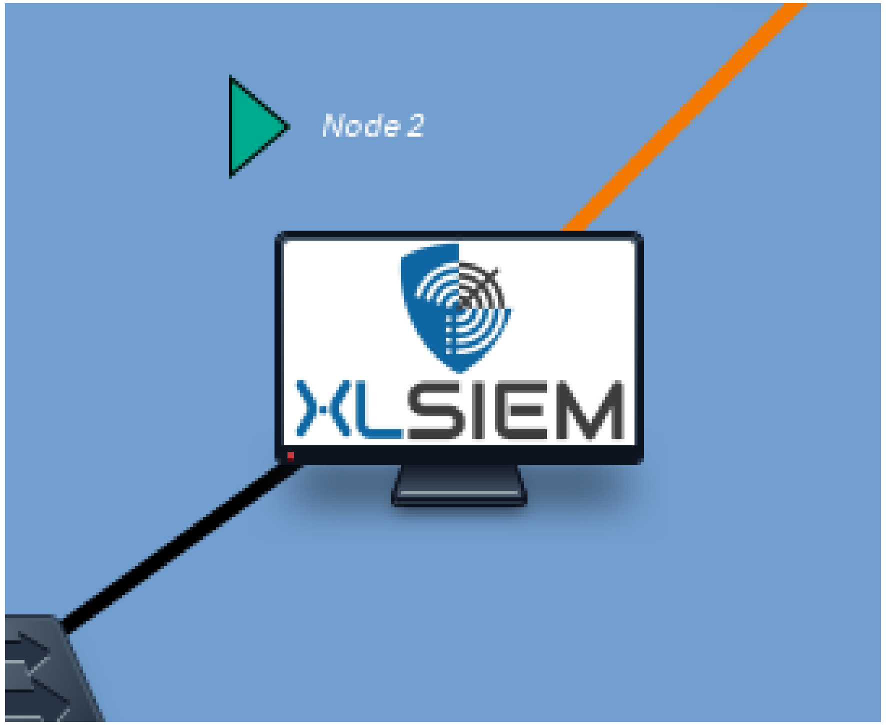
XL-SIEM Event Management System

Jesus VILLALOBOS NIETO, ATOS

16th December 2020

Zoom on the monitoring network:

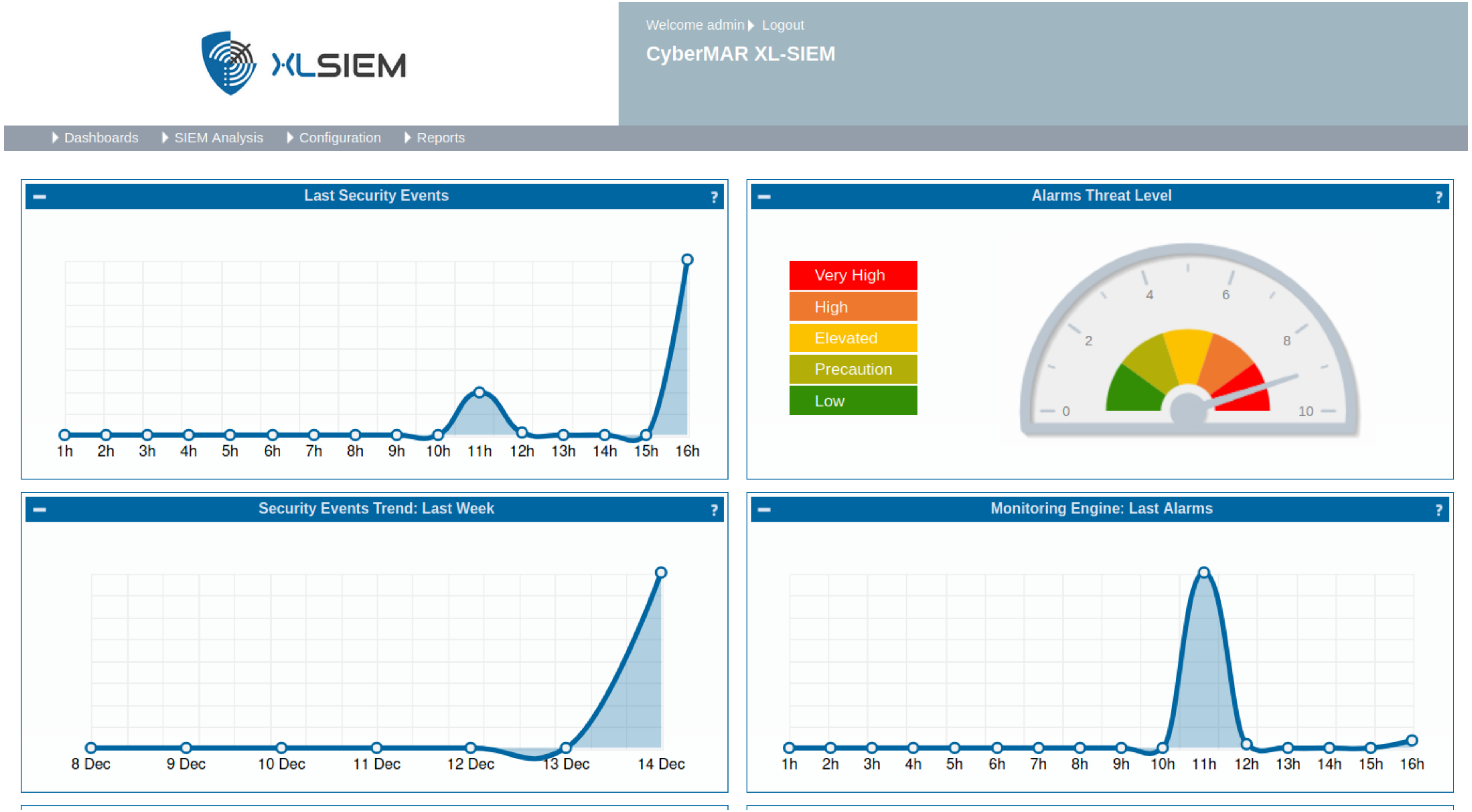
XL-SIEM by ATOS



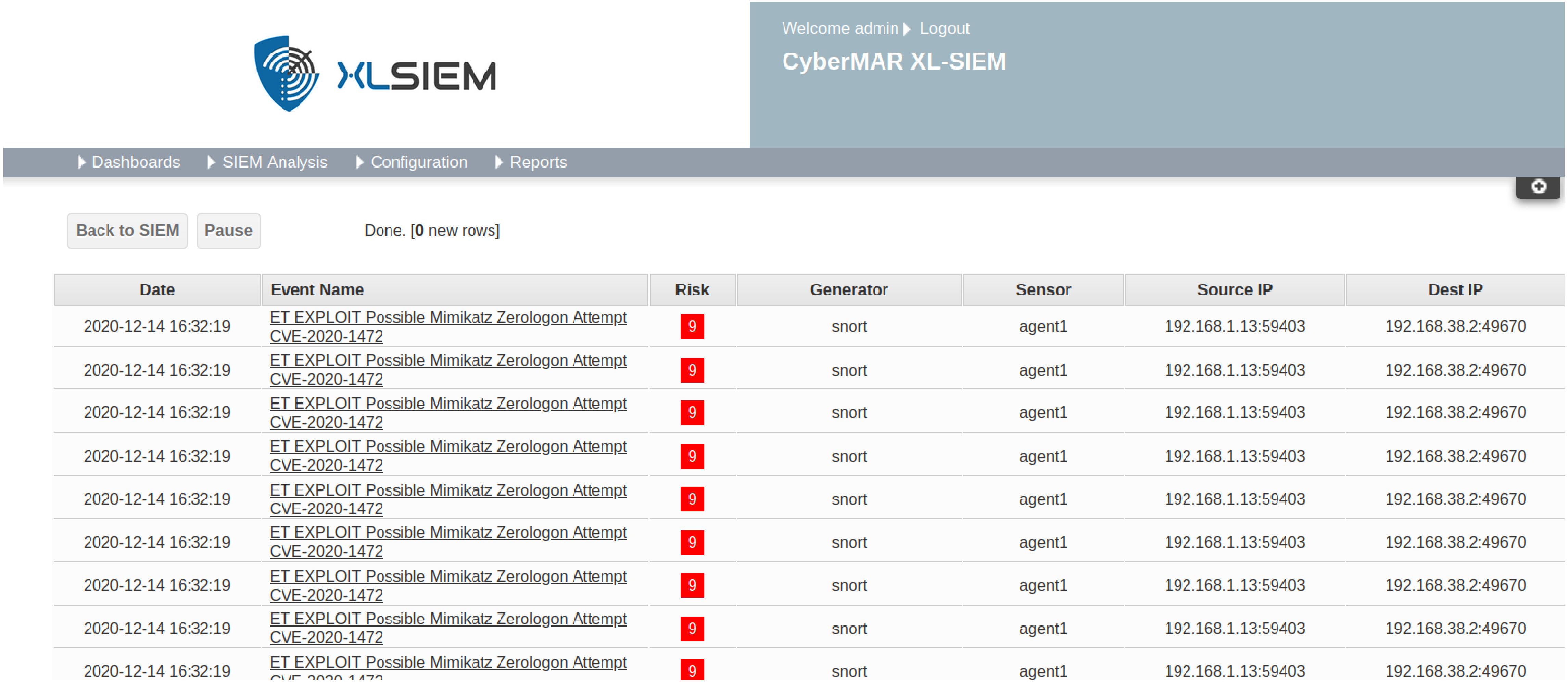
XL-SIEM – Cross-Layer Security Information and Event Manager

- Distributed and near real-time aggregation, dissemination and processing of events.
- Correlation of events from application (service) layer
- High resilience embedded by design.
- Possibility to deploy it as a service.
- Improved detection: correlation across layers and integration of external information
- Target users are organizations that need low cost and highly flexible SIEM solution

XL-SIEM - Dashboard



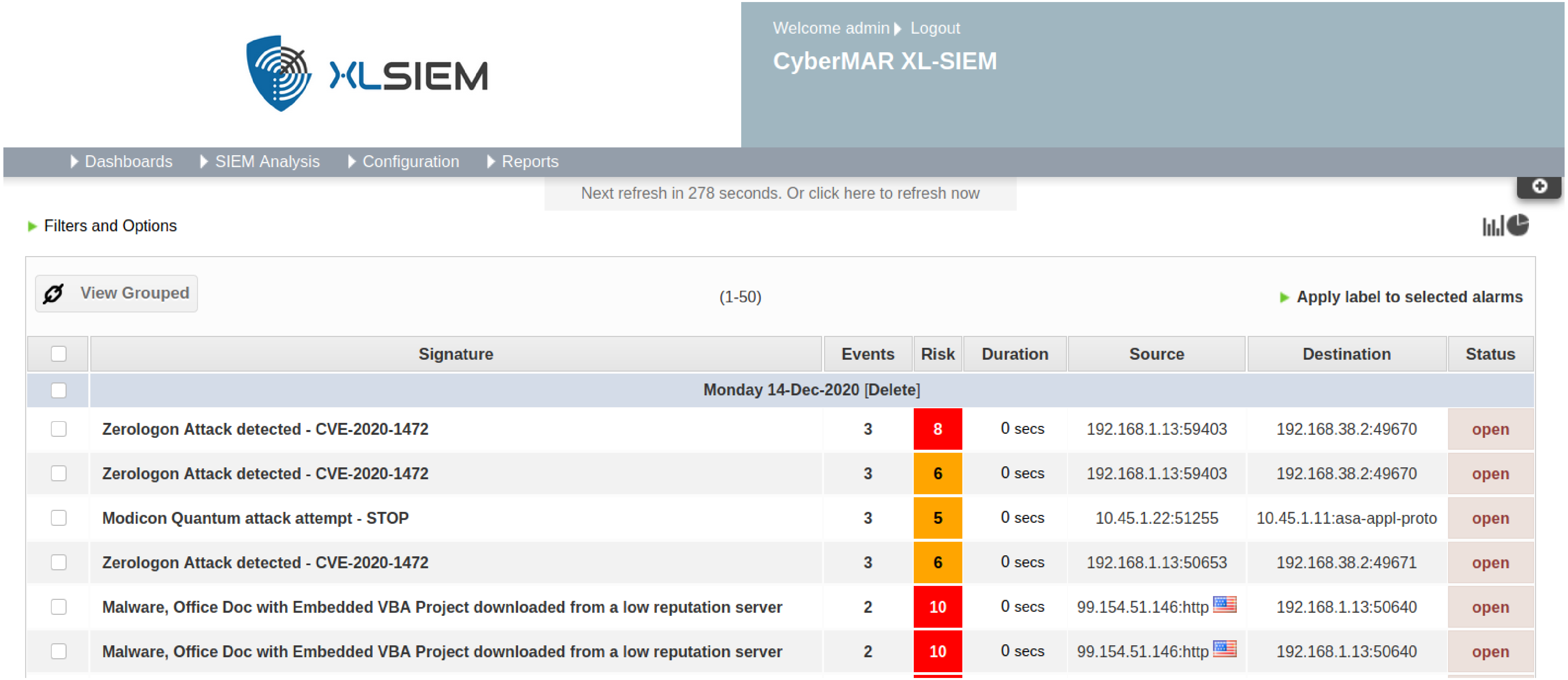
XL-SIEM - Events



Done. [**0** new rows]

Date	Event Name	Risk	Generator	Sensor	Source IP	Dest IP
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670
2020-12-14 16:32:19	ET EXPLOIT Possible Mimikatz Zerologon Attempt CVE-2020-1472	9	snort	agent1	192.168.1.13:59403	192.168.38.2:49670

XL-SIEM - Alarms



CyberMAR XL-SIEM

Next refresh in 278 seconds. Or click here to refresh now

Filters and Options

(1-50)

Apply label to selected alarms

□	Signature	Events	Risk	Duration	Source	Destination	Status
□	Monday 14-Dec-2020 [Delete]						
□	Zerologon Attack detected - CVE-2020-1472	3	8	0 secs	192.168.1.13:59403	192.168.38.2:49670	open
□	Zerologon Attack detected - CVE-2020-1472	3	6	0 secs	192.168.1.13:59403	192.168.38.2:49670	open
□	Modicon Quantum attack attempt - STOP	3	5	0 secs	10.45.1.22:51255	10.45.1.11:asa-appl-proto	open
□	Zerologon Attack detected - CVE-2020-1472	3	6	0 secs	192.168.1.13:50653	192.168.38.2:49671	open
□	Malware, Office Doc with Embedded VBA Project downloaded from a low reputation server	2	10	0 secs	99.154.51.146:http	192.168.1.13:50640	open
□	Malware, Office Doc with Embedded VBA Project downloaded from a low reputation server	2	10	0 secs	99.154.51.146:http	192.168.1.13:50640	open

Cyber-MAR Valencia pilot

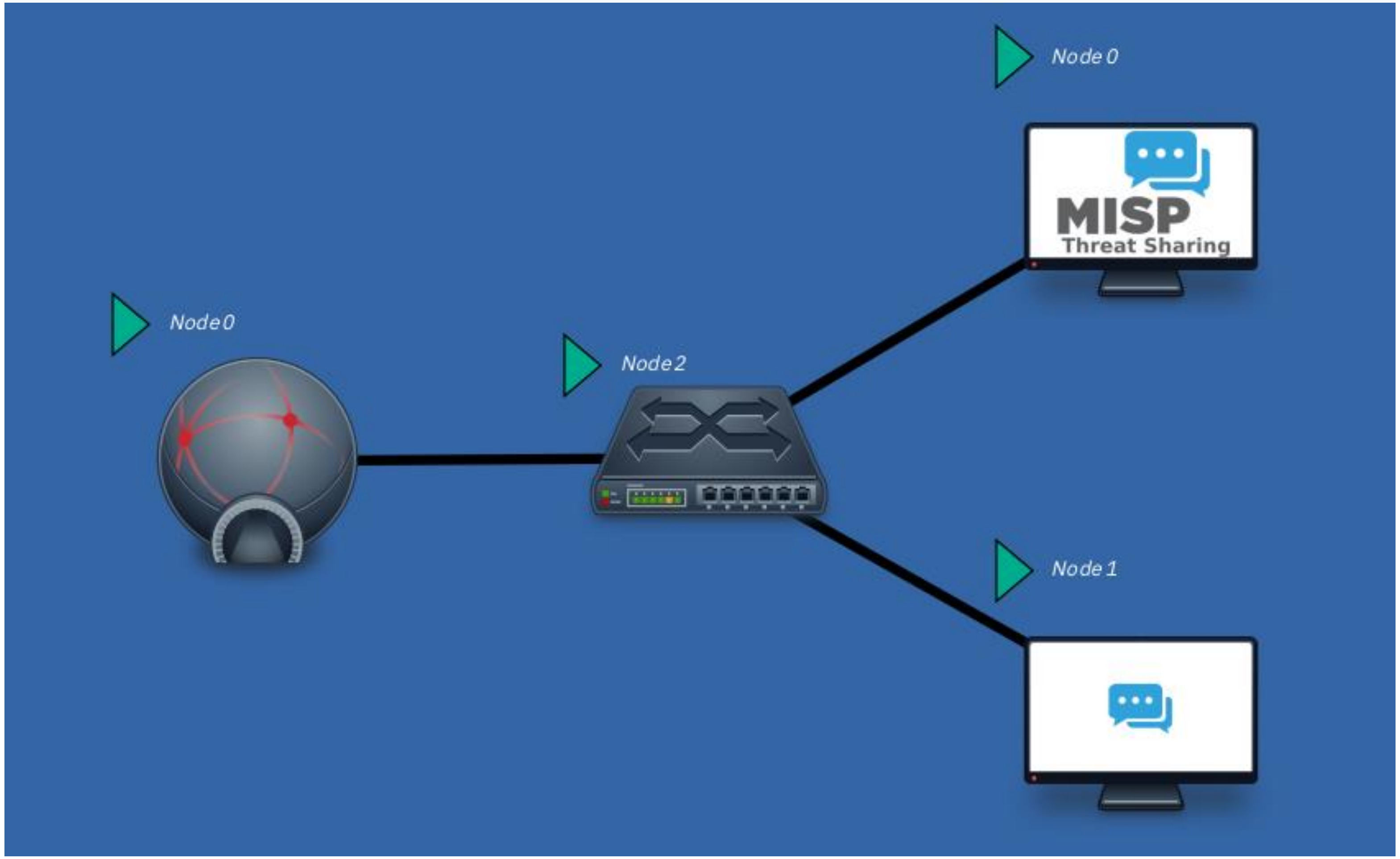
MISP tool introduction

Jean-Baptiste COHET, NAVAL GROUP

16th December 2020

CERT – MISP Topology | Valencia Pilot Event

MISP network presentation



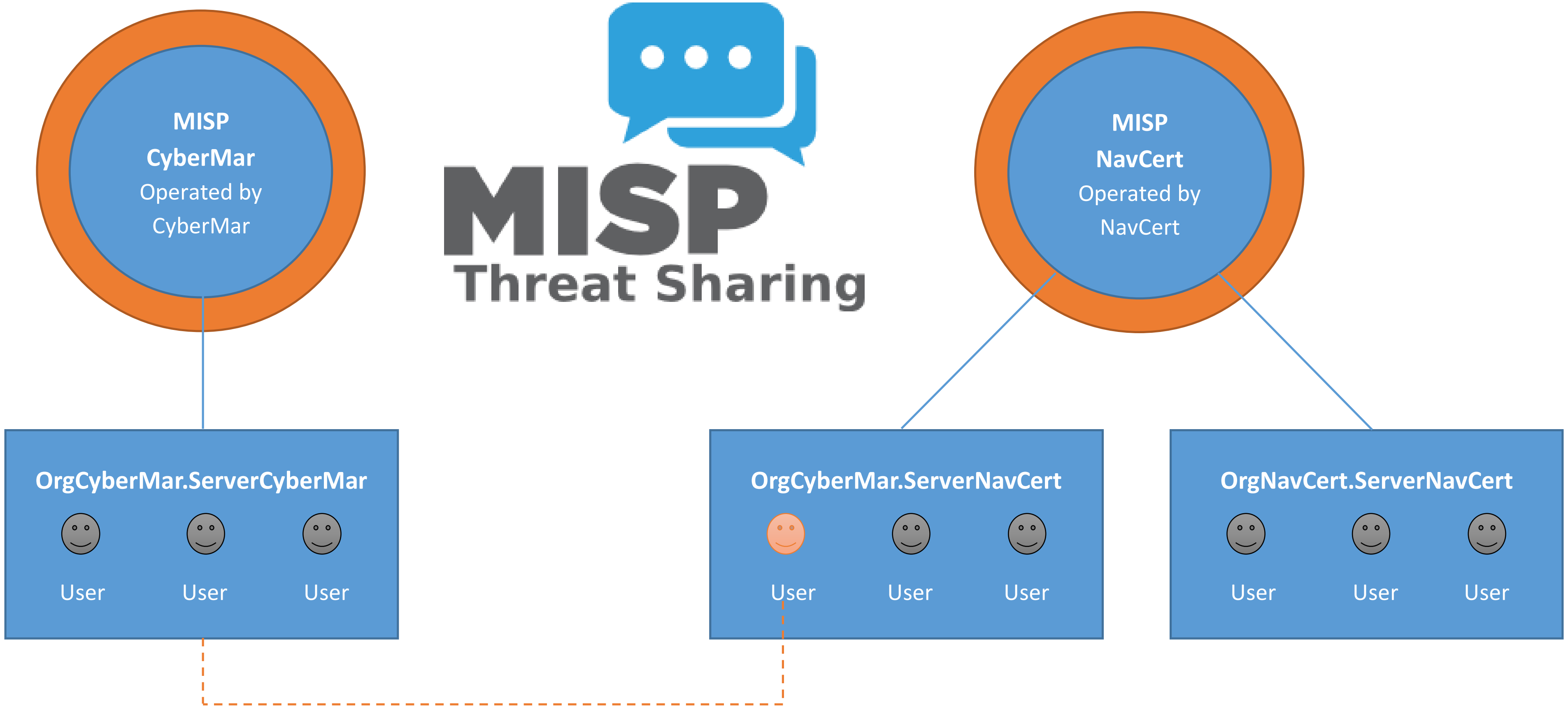
CERT – MISP Topology | Valencia Pilot Event

MISP
Threat Sharing

- Malware Information Sharing Platform
- Open Source Threat Intelligence
- IOCs sharing
- Trusted members
- Community and Organisation

CERT – MISP Topology | Valencia Pilot Event

Synchronisation between two MISP servers



Cyber-MAR Valencia pilot

Cyber Attack Scenario

Jonathan WINTERFLOOD, DIATEAM

16th December 2020

Cyber Attack Scenario | Valencia Pilot Event

In A Nutshell

What for : Port Power cut & Cryptolock of key machines.

1st Target : Active Directory

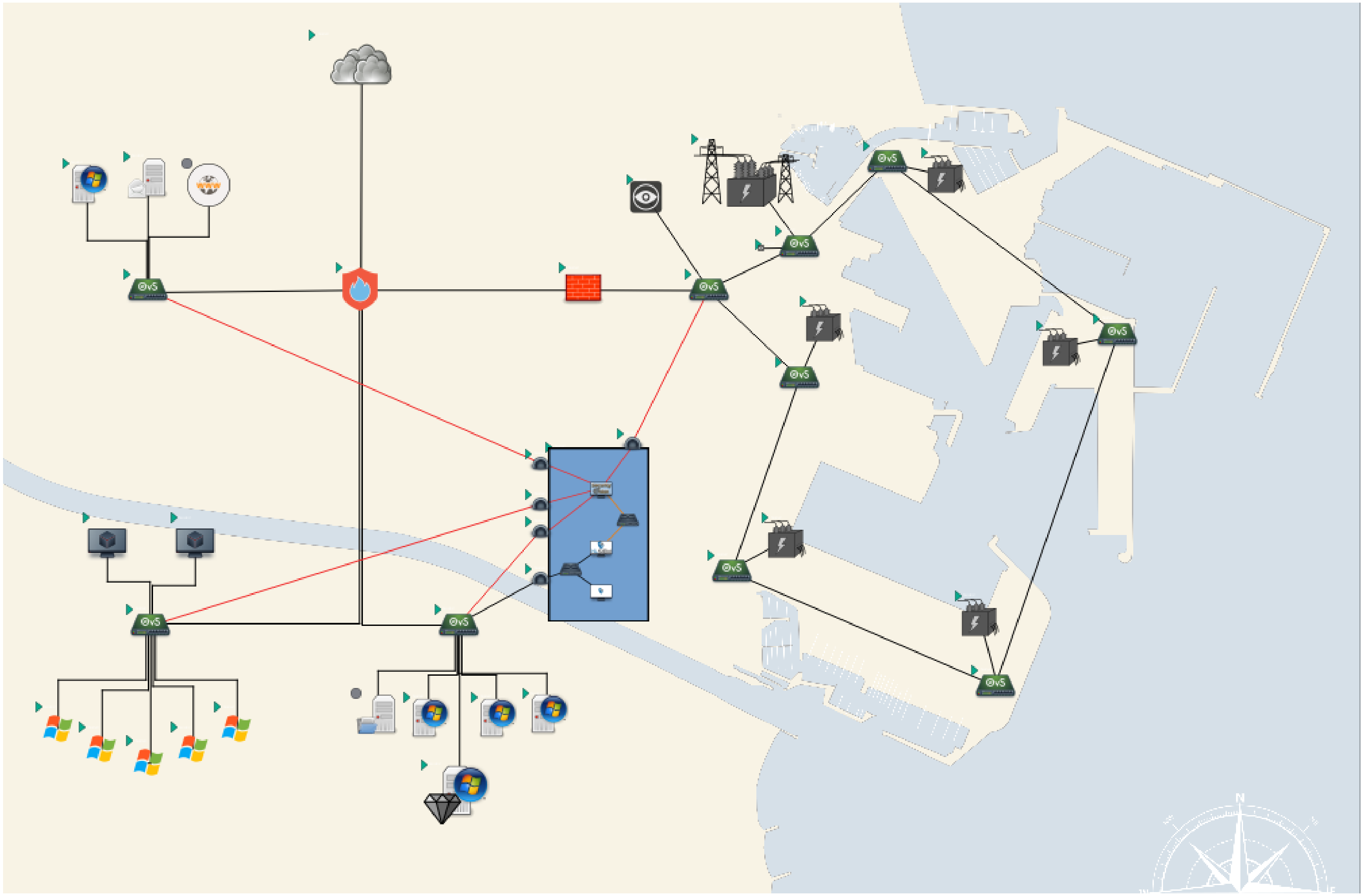
How : Spearphishing

Who : the OT Manager

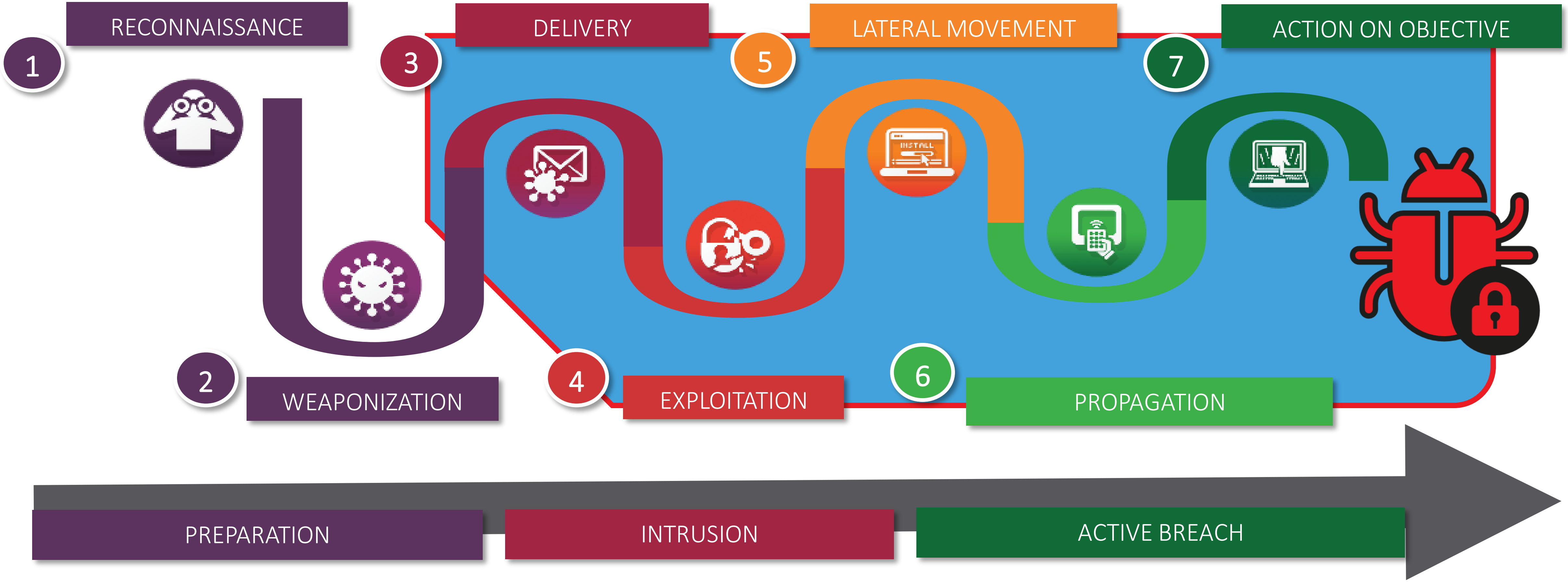
When : Friday PM

What : Malware through Macro

Bonus : Ransom & Leaks



Presentation of scenario through 7 steps



Cyber Attack Scenario | Steps 1 & 2

1

RECONNAISSANCE

Research, identification and selection of targets

- Identify targets in the network (eg. insider leak)
  - Name/surname of OT Manager
- Targeted entity’s email Address formatting

Estimated Execution Time : hours to months

2

WEAPONIZATION

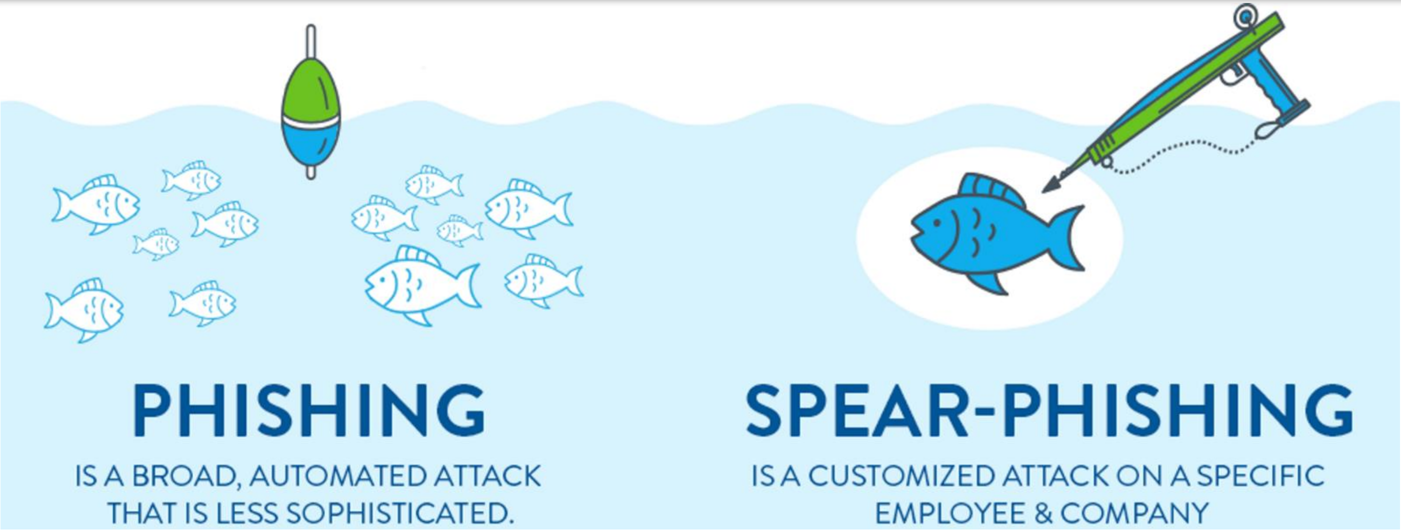
Pairing remote access malware with exploit into a deliverable payload

hours to days

Cyber Attack Scenario | Step 3

DELIVERY

3


PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.
SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

Spear-phishing: targeting a particular employee

Transmission of weapon to the target’s email address

Seconds

Cyber Attack Scenario | Step 4

EXPLOITATION

4

Once delivered, the weapon's code is triggered thanks to a macro
NB : Attackers usually rely upon User Execution to gain execution.

Persistence : User- or Admin-level persistence depending on the users' rights

- Domain membership Check
- Fetch Domain
- Check ZeroLogon CVE (NetLogon)
- Launch ZeroLogon Exploit
- → Administrator Account (Hash Dump)

Seconds to minutes

Cyber Attack Scenario | Step 5

LATERAL MOVEMENT

5

- ➢ Abuse of the SMB protocol to launch payload on the remote Domain Controller
- ➢ Persistence : admin level by insertion in the **session** startup mechanism

Seconds to minutes

Cyber Attack Scenario | Step 6

PROPAGATION

6

The malware propagates itself throughout the domain with 2 techniques :

1. Windows Remote Management (WinRm)
2. GPO for persistent propagation

Minutes to hours depending on the profile of the threat actor.

Cyber Attack Scenario | Step 7

ACTION ON OBJECTIVE

7

If the computer is SCADA Supervision machine, then the malware stops and reflashes the PLC

On all other machines, the malware launches its ransomware/Cryptolocker

Seconds to minutes

Cyber Attack Scenario – DEMO | Valencia Pilot Event

DEMO via Cyber-MAR Cyber Range

Let’s play the game !

Lateralisation / Propagation

User persistence

User persistence
+
Cryptolocking

Administrator persistence

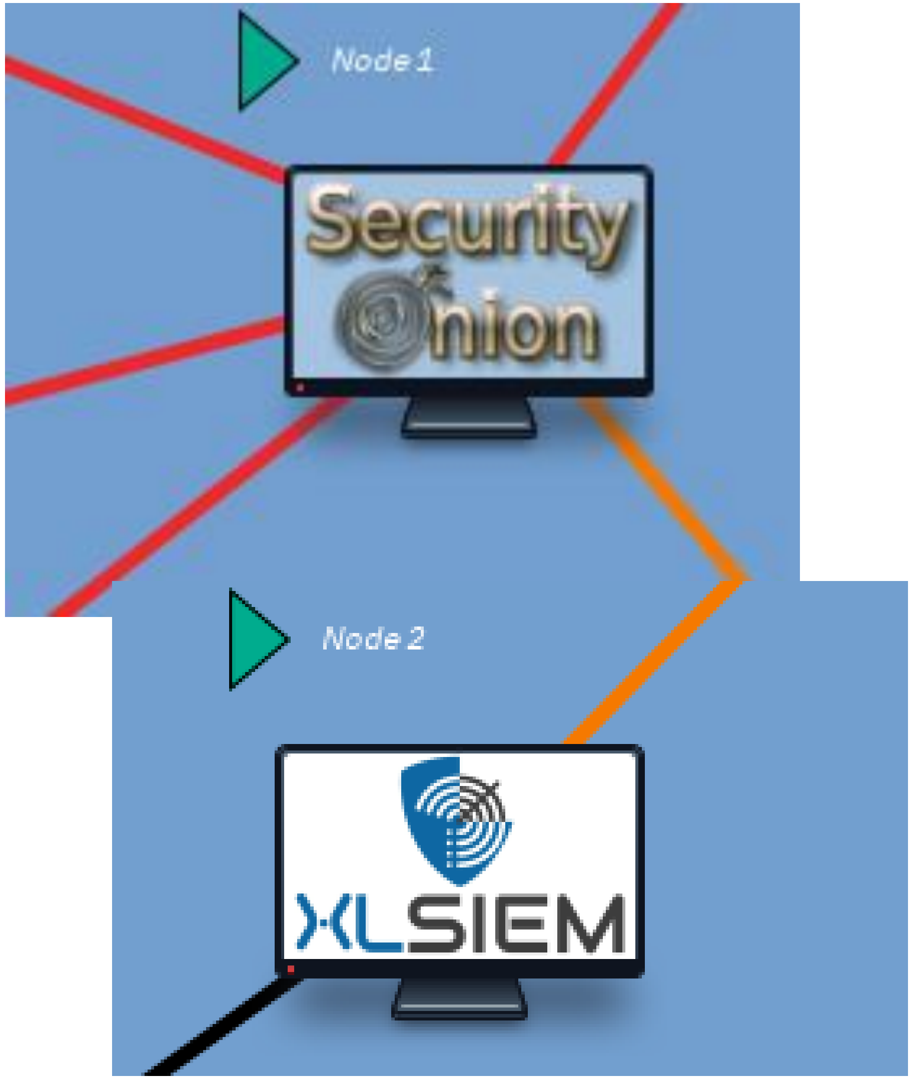
Administrator persistence
+
Crytolocking

Blue Team | Valencia Pilot Event

MONITORING RESULTS & COMMENTS AFTER ATTACK

VTT – IDS

ATOS – XL-SIEM



From the CERT Point of View

NAVAL GROUP – MISP

DEMO Debrief | Valencia Pilot Event

Feed Back & comments

by

FUNDACIÓN
VALENCIAPORT

Intro of the questionnaire

Conclusions | Valencia Pilot Event

- 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

Feedback of the Cyber-MAR Pilot platform and the Event

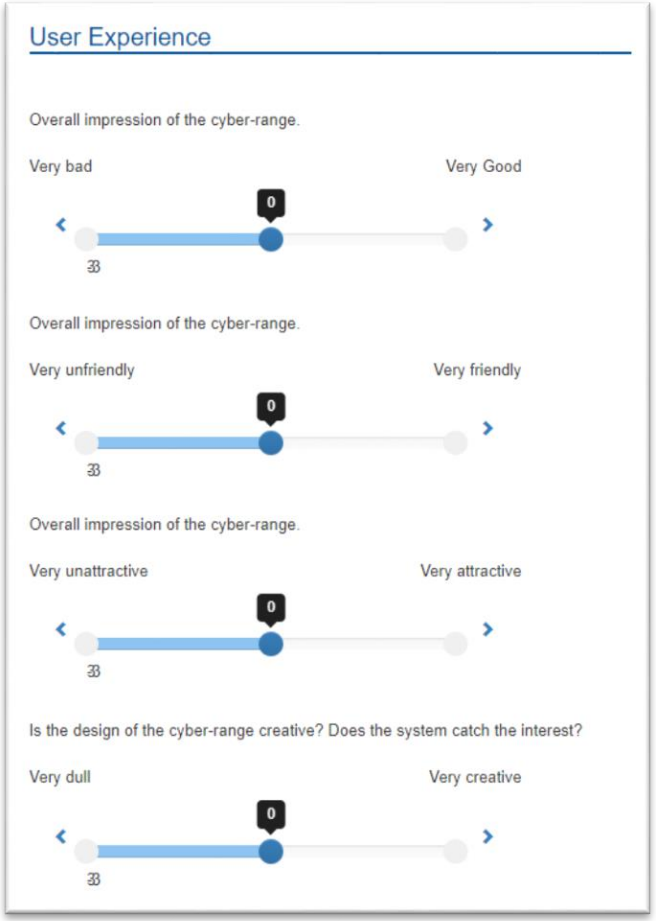
Feedback needed and valued for

- Cyber-MAR platform and cyber-ranges' development
- Further pilot events planning

Feedback questionnaire is online: (*link available in chat and email)

https://ec.europa.eu/eusurvey/runner/Cyber-MAR_Valencia-Pilot-2020

- Answering should take about 5 minutes.
- **Your support will help Cyber-MAR to improve and better serve your needs!**



User Experience

Overall impression of the cyber-range.

Very bad — Very Good

0

Overall impression of the cyber-range.

Very unfriendly — Very friendly

0

Overall impression of the cyber-range.

Very unattractive — Very attractive

0

Is the design of the cyber-range creative? Does the system catch the interest?

Very dull — Very creative

0

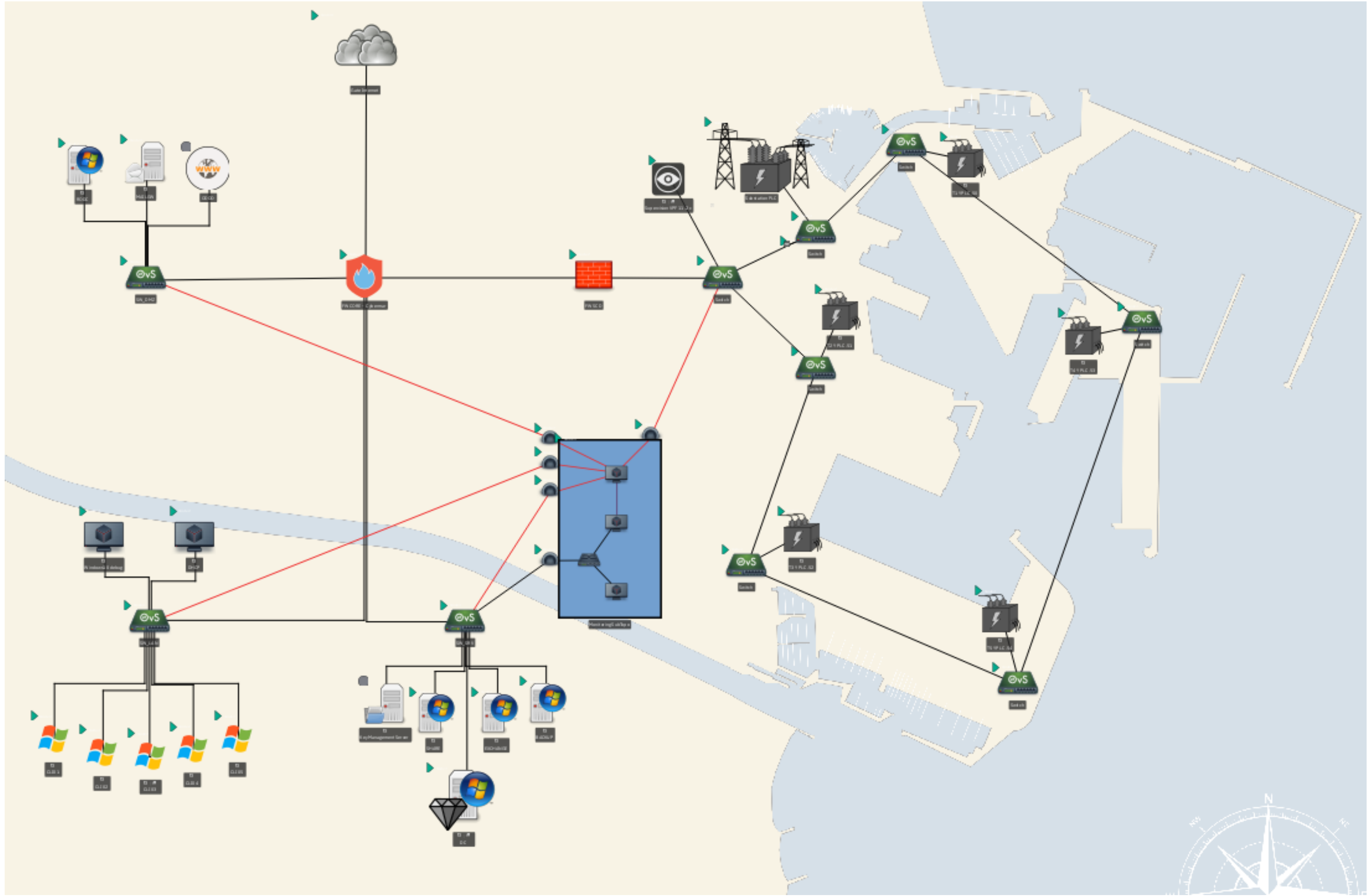
Global Q&A Session | Valencia Pilot Event

Topology Reset | Valencia Pilot Event

Cyber-range capability:
Immutability
> Easy reset

DIATEAM
MILITARY & CIVIL CYBERSECURITY SOLUTIONS

Thanks to :
All partners, All attendees
& our team !



Pablo Giménez, Fundación Valenciaport

✉ pgimenez@fundacion.valenciaport.com

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Feedback questionnaire is online: (*link available in chat and email)

https://ec.europa.eu/eusurvey/runner/Cyber-MAR_Valencia-Pilot-2020

VPF, ICCS, DIATEAM, VTT, ATOS, NAVAL GROUP

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