Securing your critical infrastructure

A cybersecurity roadmap for your OT assets.

Iraklis Mathiopoulos

Chief Services Delivery Officer

InfoCom, 27.04.23

OBRELA

1. OT – What is OT?
2. OT Incident Consequences
3. Security Objectives
4. MDR and OT
5. Further Resources

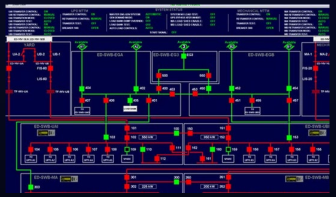
OT – Operational Technology What is it?

OBRELA

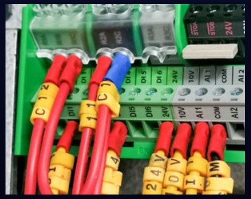
WHAT IS OT?

- Operational Technology (OT) encompasses all systems and devices that interact with the physical environment

- SCADA



- PLCs



- BAS

- PACS

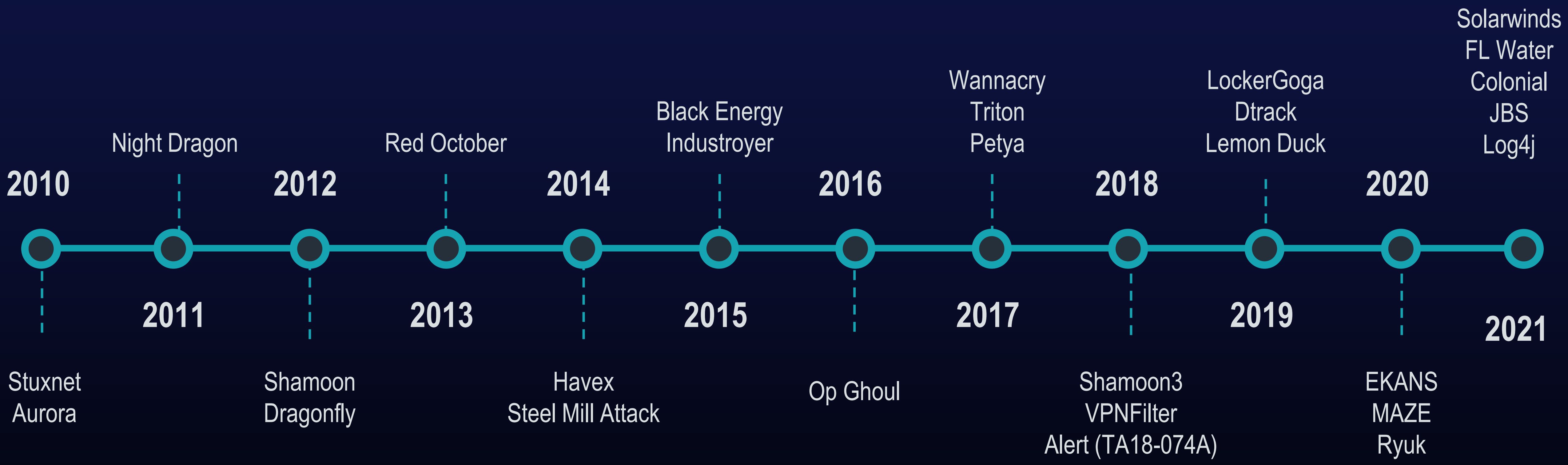
- IIoT

OT Incident Consequences

OT INCIDENT CONSEQUENCES

- Impact on national security—facilitate an act of terrorism
- Reduction or loss of production at one site or multiple sites simultaneously
- Injury or death of employees
- Injury or death of persons in the community
- Damage to equipment
- Release, diversion, or theft of hazardous materials
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of brand image or customer confidence

MAJOR CYBER ATTACKS ON OT INFRASTRUCTURE



2010

Stuxnet
Aurora

2011

Night Dragon

2012

Shamoon
Dragonfly

2013

Red October

2014

Havex
Steel Mill Attack

2015

Black Energy
Industroyer

2016

Op Ghoul

2017

Wannacry
Triton
Petya

2018

Shamoon3
VPNFilter
Alert (TA18-074A)

2019

LockerGoga
Dtrack
Lemon Duck

2020

EKANS
MAZE
Ryuk

2021

Solarwinds
FL Water
Colonial
JBS
Log4j

Security Objectives for your OT environment

OBRELA

SECURITY OBJECTIVES FOR YOUR OT ENVIRONMENT

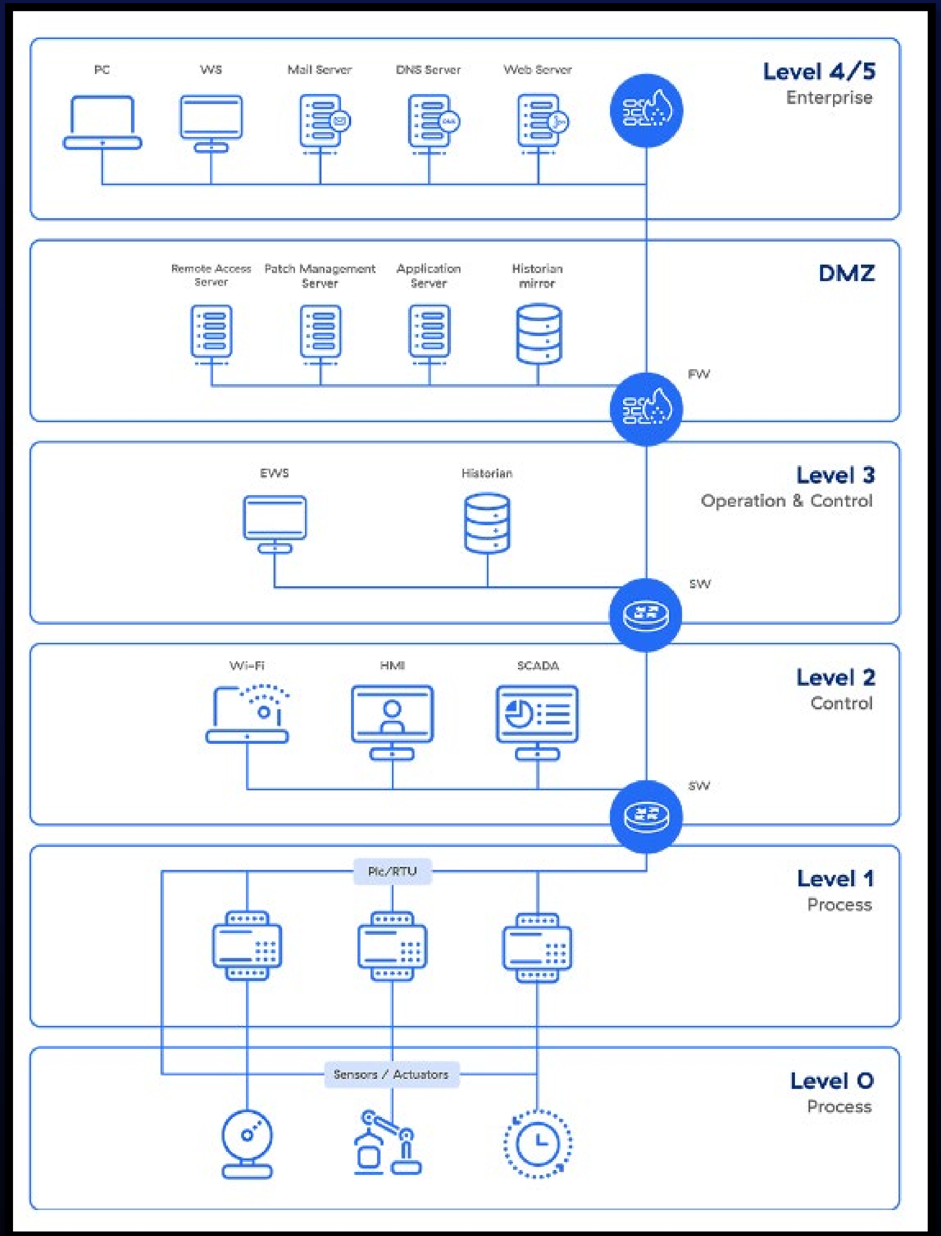
- Restrict logical access to the OT network, network activity, and systems
- Restrict physical access to the OT network and devices
- Protect individual OT components from exploitation
- Restrict unauthorized modification of data
- Detect security events and incidents
- Maintain functionality during adverse conditions
- Restore the system after an incident

SECURITY CHALLENGES

- OT systems operate under different environments and requirements than IT systems. For example, OT systems tend to prioritize availability and safety over other factors like confidentiality.
- IT programs or tools may not be suitable for OT systems. The security measures or tools that work well with IT systems may not work effectively in the OT environment.
- Compensatory measures may be an effective solution to secure an OT system without affecting system performance.
- Protecting OT systems is critical, and a cybersecurity incident on an OT system may have catastrophic consequences that affect human life and the environment.

PURDUE MODEL

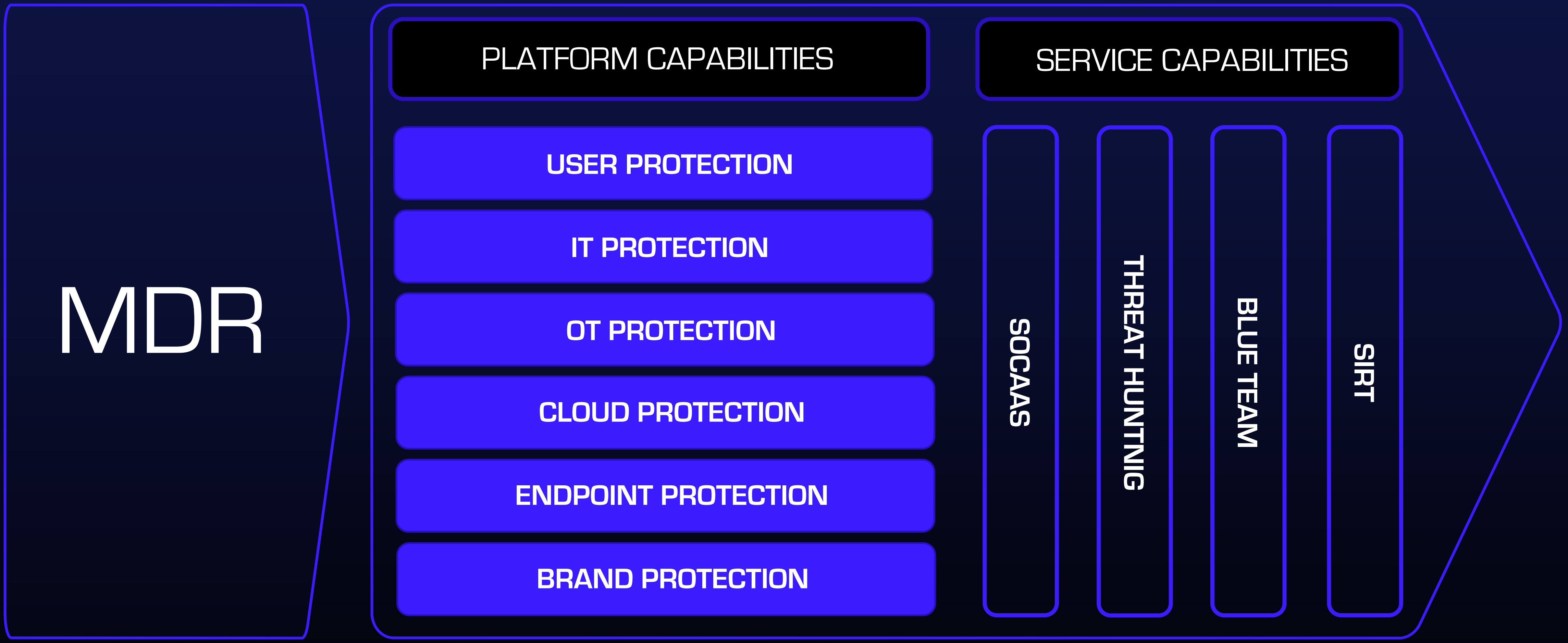
- Defender of IoT
- Dragos
- Claroty
- Nozomi Networks
- Others…



MDR and OT

OBRELA

MANAGED DETECTION AND RESPONSE



MDR

PLATFORM CAPABILITIES

- USER PROTECTION
- IT PROTECTION
- OT PROTECTION
- CLOUD PROTECTION
- ENDPOINT PROTECTION
- BRAND PROTECTION

SERVICE CAPABILITIES

- SOCAAS
- THREAT HUNTNIG
- BLUE TEAM
- SIRT

OBRELA

MDR over OT

MDR services enhance OT solution telemetry & alerts, by introducing augmented Use Cases and Playbooks to converge IT & OT under a single monitoring pane of glass.

OBRELA

MDR over OT

MDR services integrate OT source telemetry with IoT and IT to achieve:

- Unified Threat Intelligence
- Per Site vulnerability scoring
- Customer visibility in almost real-time of their environment status via the MDR platform

SECURITY OBJECTIVES FOR YOUR OT ENVIRONMENT

- Restrict logical access to the OT network, network activity, and systems
- Restrict physical access to the OT network and devices
- Protect individual OT components from exploitation
- Restrict unauthorized modification of data
- Detect security events and incidents
- Maintain functionality during adverse conditions
- Restore the system after an incident

OT SPECIFIC SECURITY USE CASES (1/2)

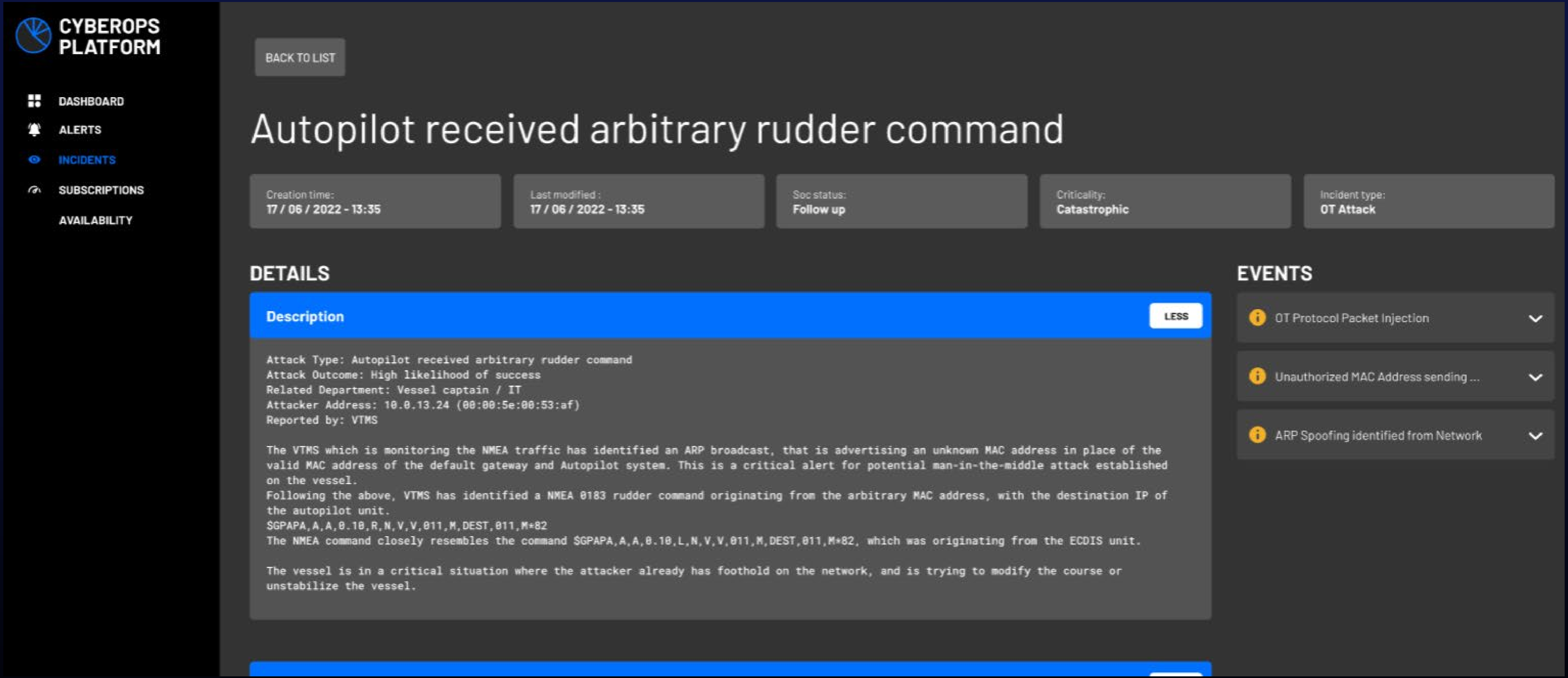
- Illegal function codes for ICS/SCADA traffic
- Unauthorized firmware updates
- Unauthorized PLC changes
- PLC insecure key state
- PLC stop
- Suspicious malware found in the network
- Multiple scans in the network
- Unauthorized SCADA node
- High bandwidth alerts
- Denial of Service

OT SPECIFIC SECURITY USE CASES (2/2)

- Physical Access Controls (if applicable)
- Corrupted OT packets
- Denial of control attacks
- Logic changes

- Attempts to access protocols that have no authentication built-in mechanisms, such as Modbus/TCP, EtherNet/IP, IEC 61850, ICCP and DNP3
- HVAC failures
- OT protocol hijacking
- Response injection attacks

USE CASE EXAMPLE



Autopilot received arbitrary rudder command

Creation time:	Last modified :	Soc status:	Criticality:	Incident type:
17 / 06 / 2022 - 13:35	17 / 06 / 2022 - 13:35	Follow up	Catastrophic	OT Attack

DETAILS

Description

```
Attack Type: Autopilot received arbitrary rudder command
Attack Outcome: High likelihood of success
Related Department: Vessel captain / IT
Attacker Address: 10.0.13.24 (00:00:5e:00:53:af)
Reported by: VTMS

The VTMS which is monitoring the NMEA traffic has identified an ARP broadcast, that is advertising an unknown MAC address in place of the
valid MAC address of the default gateway and Autopilot system. This is a critical alert for potential man-in-the-middle attack established
on the vessel.
Following the above, VTMS has identified a NMEA 0183 rudder command originating from the arbitrary MAC address, with the destination IP of
the autopilot unit.
$GPAPA,A,A,0.10,R,N,V,V,011,M,DEST,011,M*82
The NMEA command closely resembles the command $GPAPA,A,A,0.10,L,N,V,V,011,M,DEST,011,M*82, which was originating from the ECDIS unit.

The vessel is in a critical situation where the attacker already has foothold on the network, and is trying to modify the course or
unstabilize the vessel.
```

EVENTS

- OT Protocol Packet Injection
- Unauthorized MAC Address sending ...
- ARP Spoofing identified from Network

OT INCIDENT RESPONSE

- Evaluate if incident involves people safety
- Clarify whether restoration is the highest priority, or should containment and evidence gathering take precedence
- SOC Team will evaluate the external information regarding the incident (user reporting, threat intelligence feed, threat actor announcement) in respect to the people, systems, actions and timeframes that are involved
- SIRT Team will work towards containment of the threat by e.g. isolating the systems or blocking interactions with external IP/resources.
- If forensic analysis is required, the SIRT team will collect timestamps, visuals (photos), volatile and non-volatile information from the running IT systems in the OT environment, and proceed in further analysis and reporting of findings
- The restoration of the systems to a previous unaffected state will be performed by the Customers or their vendors.
- The root cause mitigation of the incident will be based on artifacts gathered from the above steps (log analysis, SIRT actions, forensics)
- The lessons learned will be collected and evaluated to recursively act as means of prevention for the future

Further resources

OBRELA

NIST SP 800-82

- Guide to Operational Technology (OT) Security r3 (DRAFT)

MITRE ATT&CK: ICS Techniques

- Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

SANS

- Industrial Control Systems Security Courses and Certifications

SECURITY OVER EVERYTHING

OBRELA

OBRELA

THANK YOU

London | Athens | Dubai | Frankfurt | Riyadh

www.obrela.com