OT SOC

Tales from the trenches, OT SOC from operator point of view

Karo Vallittu, 18.6.2026

A SUSTAINABLE
FUTURE THROUGH
DIGITALISATION

Who am I?

Karo Vallittu
Principal OT Security Lead
Elisa Cyber Security Center

Cybersecurity in one way or another for over 20 years

Worked with telecom industry, Maritime, and more recently with OT/ICS systems

Habitual student – currently Faculty of Law, University of Helsinki

Finnish National Defence Association (MPK) cyber instructor

Elisa cyber operations in a nutshell

Cyber Security Center founded in 2015

OT SOC service from 2021

100+ cyber specialists, 24/7 operation

5000+ security incidents handled per month

Over 90% incidents handled without customer escalation

Some definitions

IT SOC vs OT SOC

What to look for

Some definitions

Defining characteristics of OT systems

- Very long service life, slow update cycles
- Availability critical, maintenance breaks rare
- Often systems delivered by third party, and maintenance outsourced to vendor
- Proprietary protocols vs open protocols

Defining characteristics of OT systems

Safety vs Security

Two different, but close concepts

OT systems are cyber-physical systems (CPS), where programmable logic controllers control elements in a physical world, such as high pressures, large moving objects, strong electrical currents

Error situations can cause hazards, which can lead to severe accidents and even loss of life

Defining characteristics of OT systems

Safety vs Security

Safety = “Machine causes no harm to human”

Security = “Human causes no harm to machine”

IT SOC vs OT SOC

IT vs OT SOC

IT SOC

- Main concept is identity
- Most of the detections come from endpoints
- Monitoring based on agents installed on endpoints and devices
- Usually capability to perform active countermeasures
- Security

IT vs OT SOC

OT SOC

- Main concept is ‘asset’
- Most of the detection capability from network level
- Passive monitoring
- Limited capability to active countermeasures
- Safety

IT vs OT SOC

Differences

- OT field buses (profinet, modbus etc)
- Detection sources
- Playbooks for countermeasures
- Possibility to perform countermeasures
- IT and OT SOC can still support each other

What to look for - observations from existing projects

Architecture

- Can the OT system be monitored in the first place
- ‘Asset leaking’
- IDMZ
- Separation and isolation based on Purdue levels

Architecture, options

- Monitoring with firewalls on the edge of OT network
- Passive monitoring using sensors inside OT network
- Agent based monitoring (rare)
- Active scans inside OT network (very rare)

Architecture, decisions

- Monitoring strategy
- Inline vs spanned passive sensor
- Monitoring traffic, through the same OT network, or separate monitoring net?
- Management connections, how do you update and manage the sensors?
- Cloud or local management?

Architecture

- Security projects on OT systems practically always require the involvement of the system vendor
- Begin with the most obvious improvements and iterate from there
- “Do not let perfect be the enemy of better”

Threat models

- What / Who are you defending against?
- What is the most probable scenario?
- What is the ‘worst case’ scenario?
- Where not to spend money and resources?
- Different threat models in different systems

Connectivity

- Remote connections?
- Monitoring
- Access Control
- If SOC deployment, then also the SOC needs a connection

Use Cases

- What is actually relevant? And what is not
- “Behavioral Baseline”
- The more static the environment is, the better chance there is to create a reasonable baseline
- Baseline detections vs signature detections

Reacting to detection

- What capabilities do you have, when an anomaly is detected?
- Escalation from SOC to local engineers?
- Countermeasures?
- Isolation?

Reacting to detection

- What capabilities do you have, when an anomaly is detected?
- SOC analyst usually does not have a view to the actual process, which makes understanding the context difficult
- Reacting to OT event often resembles more threat hunting than incident response

Reacting to detection

- What capabilities do you have, when an anomaly is detected?
- Active countermeasures are often either difficult or outright impossible in OT environment
- Safety vs Security
- Practice!

Insider threat

- From SOC analyst point of view, the insider actions are often indistiguishable from normal events, as the legitimacy of those actions are mostly based on context
- Understanding the context and events surrounding the action are usually the only way to tell things apart


elisa
A SUSTAINABLE FUTURE THROUGH DIGITALISATION
Thank you!