Penetration Testing in Rail

Why, When, What, How?

Dear chat GPT, should we PT our trains?

About me

Yaniv Mallet

Field CTO at Cylus

Last 3y at Cylus

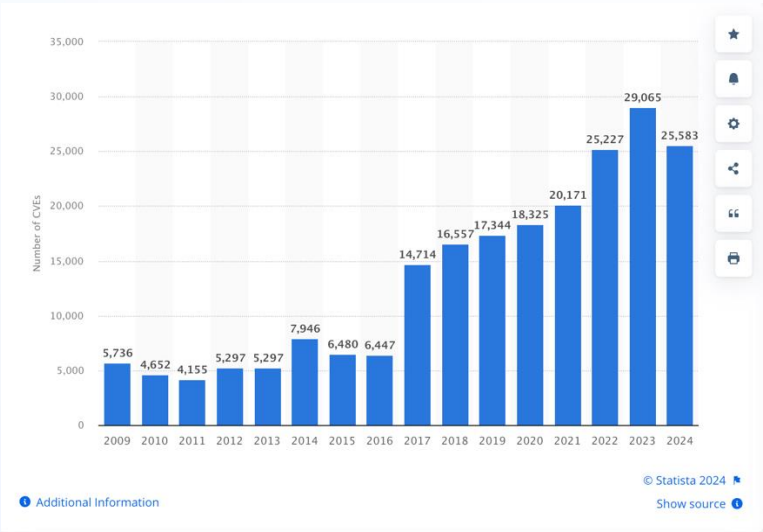
Before that: 24y+ for gov. agencies in cyber(security)

#Computer Science degrees, CISSP, ISSAP, GICSP,

Lego fan, Nintendo believer, FullTime DAD.

CYLUS

WHY – Railway Cybersecurity context



Digitalization

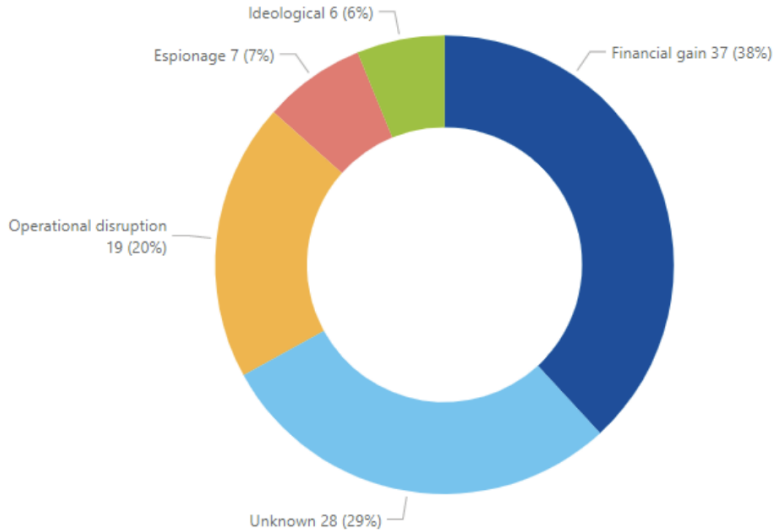
Wireless Communication

Advanced Services

CYLUS

WHY – Railway Cyber Threat Landscape

Figure 10: Motivation



ENISA Threat Landscape: Transport sector (March 2023)

Gaggero *et al. J Surveill Secur Saf* 2024;5:52-61 I http://dx.doi.org/10.20517/jsss.2023.35

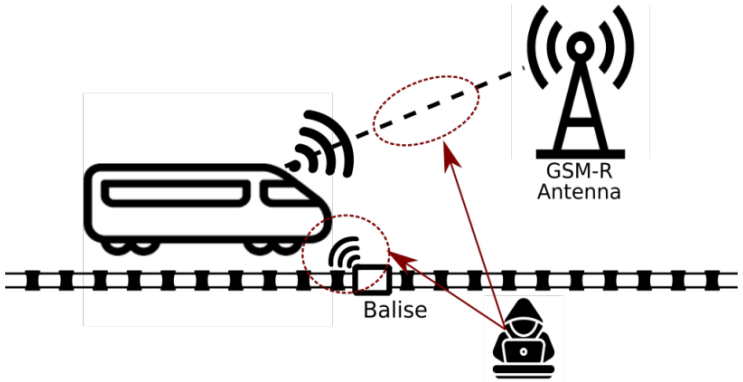


Figure 2. Attack surface.

WHY - Benefits

Security

Compliance

Resilience

WHEN – Railway Network Lifecycle

- Early testing during deployment to secure configurations.
- Validation of new technologies (e.g., FRMCS, IoT).
- INTEGRATIVE PT at testing

- Periodic PTs: Ensuring ongoing security amid evolving threats.
- Changes and variations (not only rail)
- New Interfaces
- Post-incident testing: Identifying gaps after a cyber event or suspicious activity.
- Compliance deadlines…

CYLUS

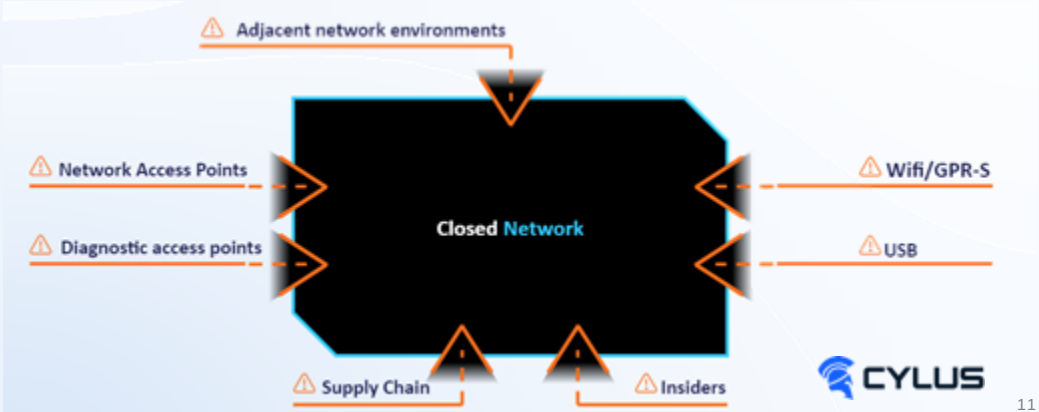
WHEN – Another major timing

WHAT – to test?

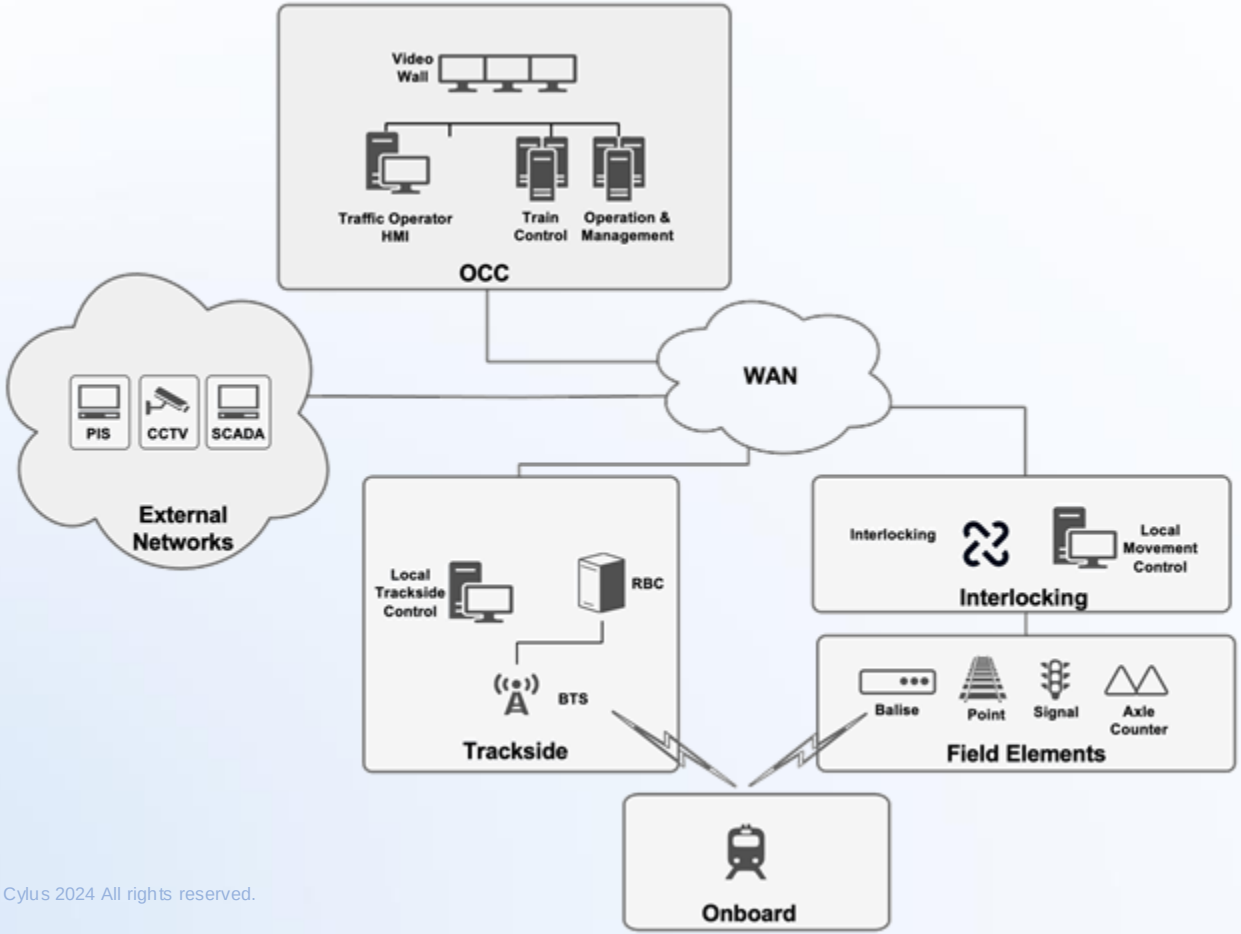
WHAT – we have the define it well

- Remember the SUC process in 62443?
- Legacy vs Modern ?
- Safety vs Security ?
- External facing or Closed Network ?

- What is the target that we require from the PT supplier?



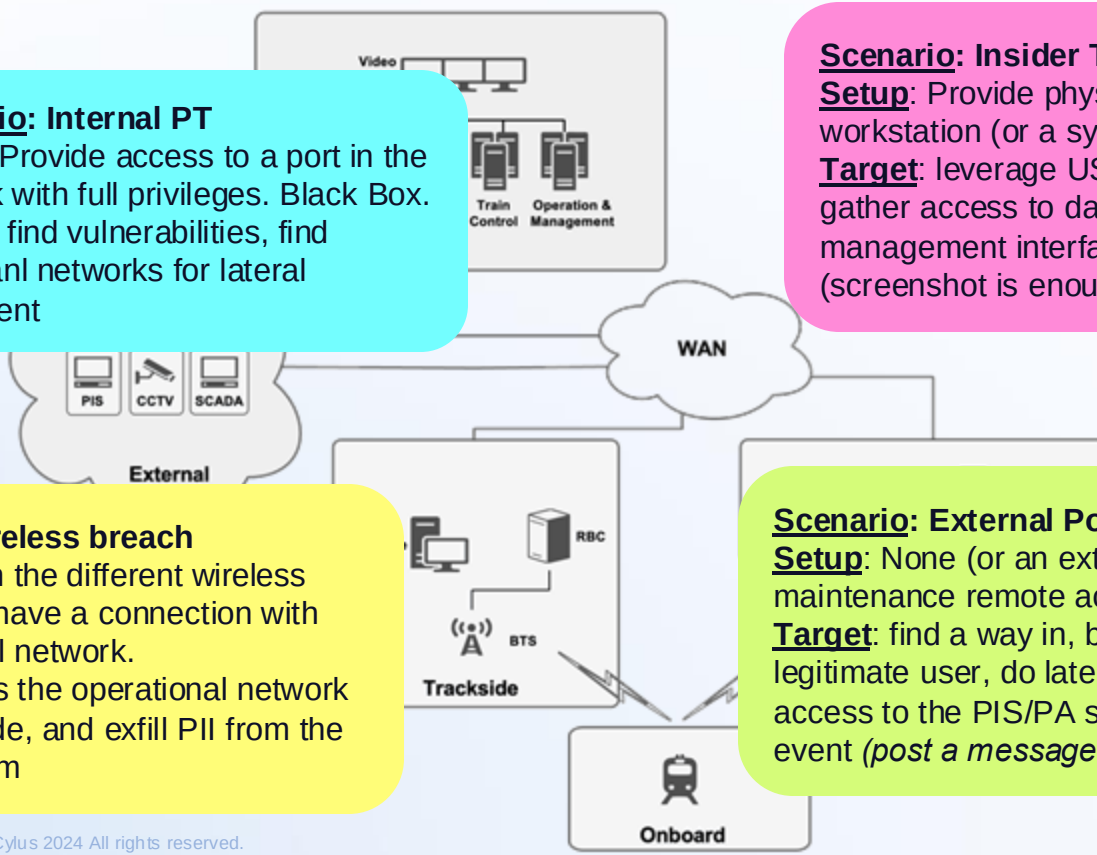
WHAT – to choose?



WHAT – examples of scenarios

Scenario: Internal PT
Setup: Provide access to a port in the network with full privileges. Black Box.
Target: find vulnerabilities, find additioanl networks for lateral movement

Scenario: Insider Threat
Setup: Provide physical access to an OCC workstation (or a systems room).
Target: leverage USB or network interfaces to gather access to data from one of the SCADA management interfaces and exfill this data (screenshot is enough)

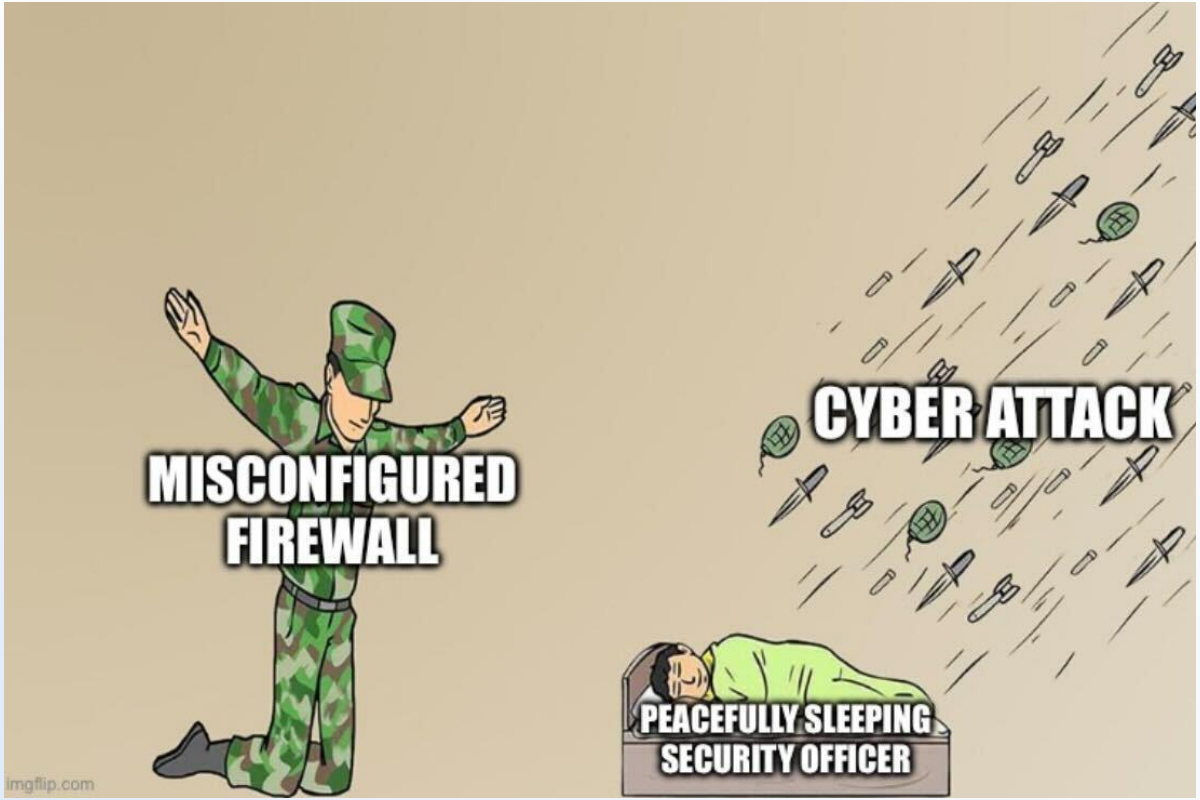


Scenario: Wireless breach
Setup: Explain the different wireless channels that have a connection with the operational network.
Target: access the operational network from the outside, and exfill PII from the ticketing system

Scenario: External Posture
Setup: None (or an external IP used for maintenance remote access)
Target: find a way in, by breaking in or abuse a legitimate user, do lateral movement and gather access to the PIS/PA system and create a panic event *(post a message on boards…)*

CYLUS

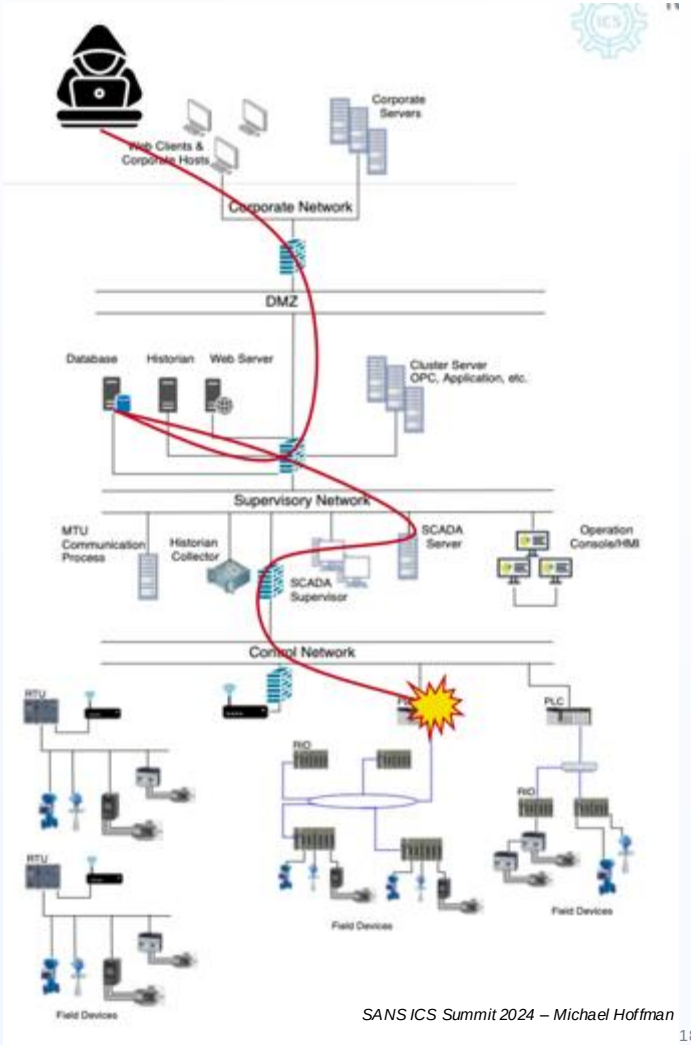
WHAT – Cyber controls are on the spot!



HOW

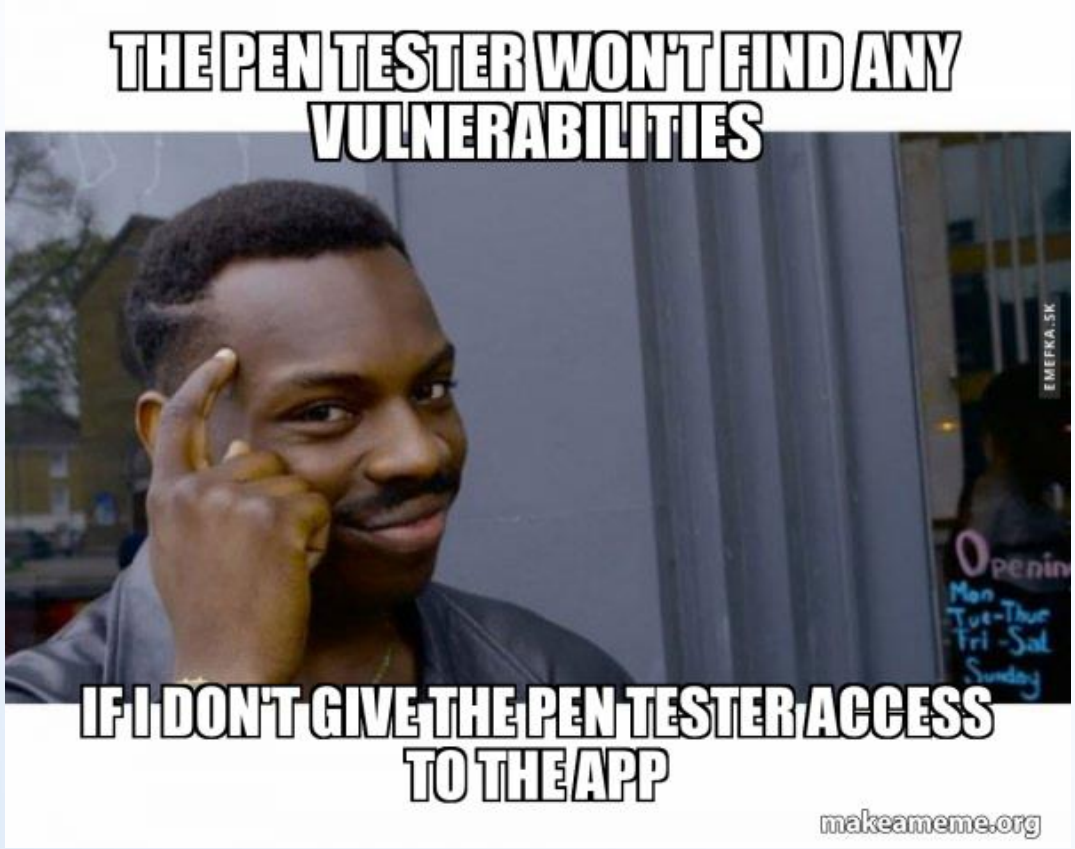
HOW – Prepare the what

- 🔍 Conducting a Security Architecture Review (SAR)
- 🔍 Defining scope: IT/OT boundaries, critical assets.

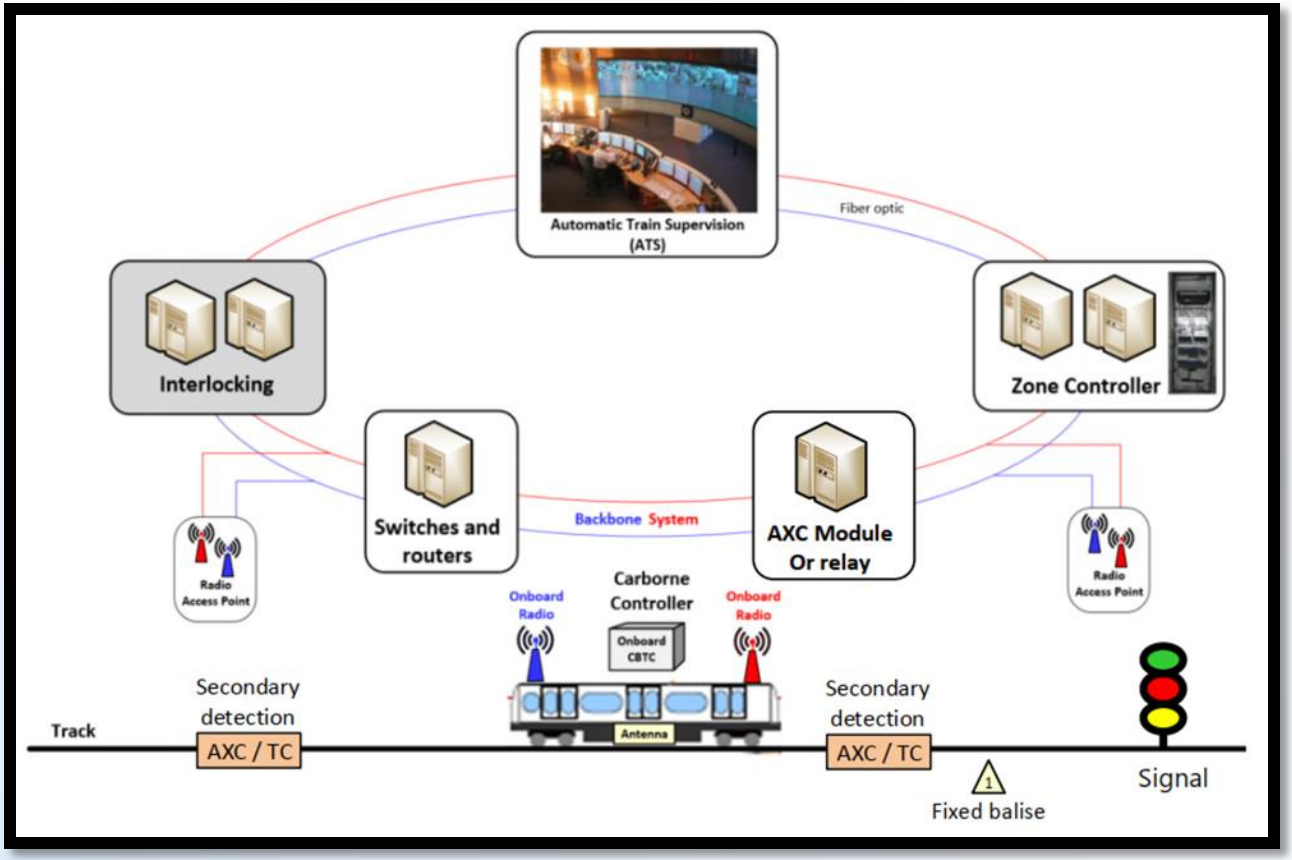


SANS ICS Summit 2024 – Michael Hoffman

HOW – manage the event



HOW – BlackBox, WhiteBox, GreyBox?



HOW – external exposure worth it

12

EUROPEAN UNION AGENCY FOR RAILWAYS

MFA for Access to ERA Resources

following Cybersecurity regulation (EU, Euratom) 2023/2841

- Redefines the cybersecurity landscape for institutions, bodies, offices, and agencies of the European Union (Union entities).
- It represents a proactive stand against the evolving spectrum of cyber threats that challenge the integrity, confidentiality, and availability of information systems of Union entities.

Article 6(8) requires the appointment of the **Local Cyber Security Officer** (LCSO). ERA has implemented this provision with:

- **Luca TRINCA** as Local Cyber Security Officer (LCSO)
- **Kleon KLEANTHOUS** as alternate Local Cyber Security Officer (LCSO) - Point of Contact (PoC)

CYLUS

HOW – the ICS specifics

⚠ The safety worry is **mostly around "active scanning" impact**

⚠ It has roots in multiple real events, and the behavior of ICS systems:

- **Vulnerability Scanner Incidents[13].** While a ping sweep was being performed on an active SCADA network that controlled 3 meter (9 foot) robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers. See Section 4.2.6 for additional guidance on ICS vulnerability assessments.
- **Penetration Testing Incident[14].** A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

HOW – the ICS specifics

⚠ ICS professionals understands (most of) the precautions.

⚠ Example with nmap:

- ⚙ Reduce the scanning speed to scan only one port at a time {*"--scan-delay=1"*}
- ⚙ Without ping, SYN or UDP scans, only TCP scans {*"nmap -sn -PR -n"*}
- ⚙ Do not use fingerprinting options, they will send a lot of extra packets to force the listener to respond with certain crafted packets.

⚠ Other example: use protocols that are designed to work on such a network….like SNMP.

HOW – the ICS specifics

⚠ We now see academic research on this topic .

⚠ A recommended one was at S4x24 **"PLCs: To Scan Or Not To Scan”**.

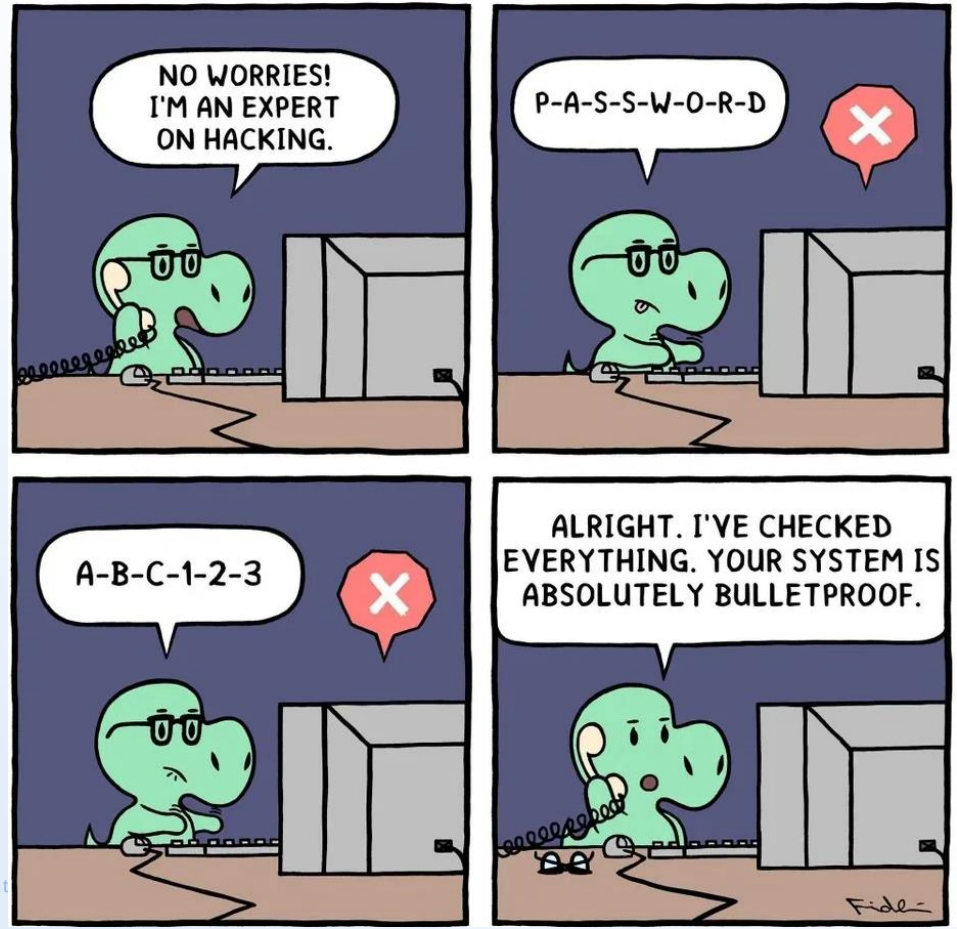
“PLCs: To Scan Or Not To Scan”

HOW – tools approach

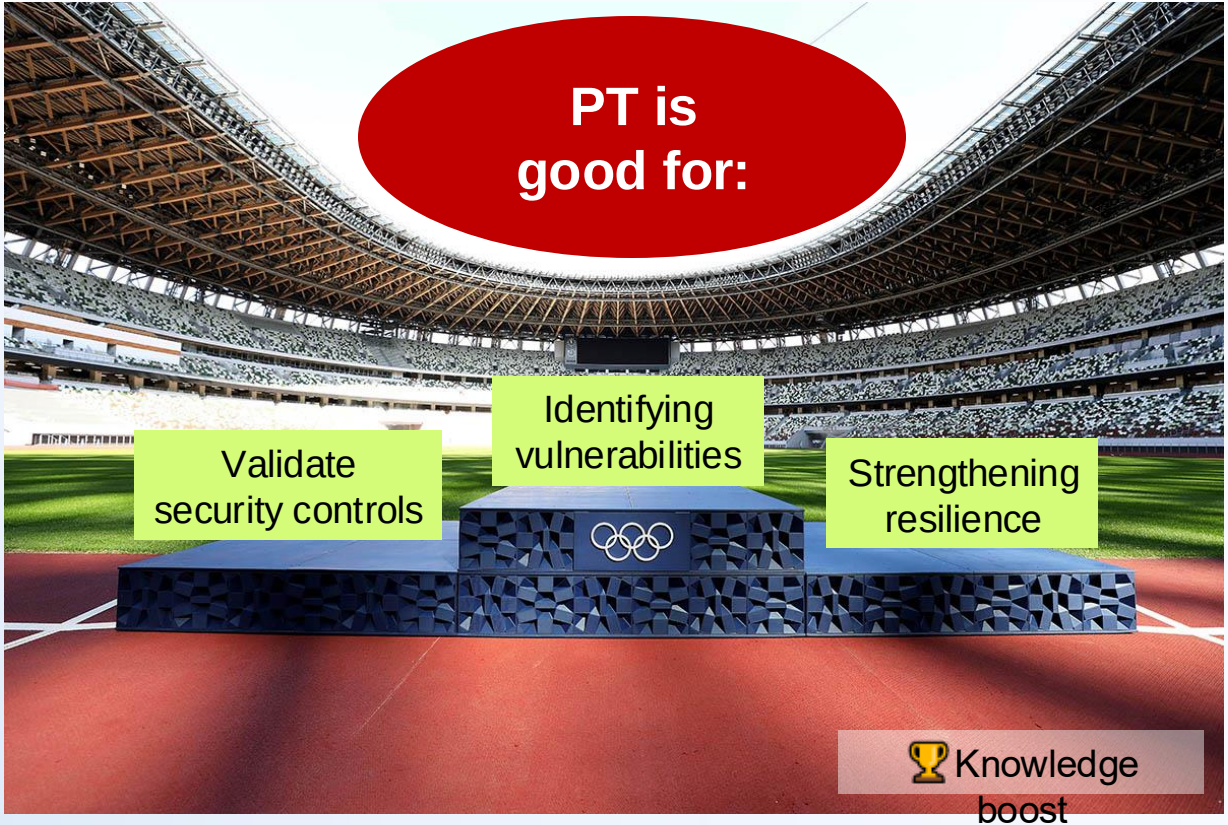
- ⚠ Passive techniques only: traffic analysis (e.g., Wireshark, Zeek)
- ⚠ Active Techniques: Controlled scans with Nmap, Snap7, PLCscan, ControlThings (maybe Py_PLC Honeypot...)
- ⚠ RF spoofing/jamming/hacking (Rogue BTS, Rogue AP, HackRF…)
- ⚠ Run a full replicate environment for testing

CYLUS

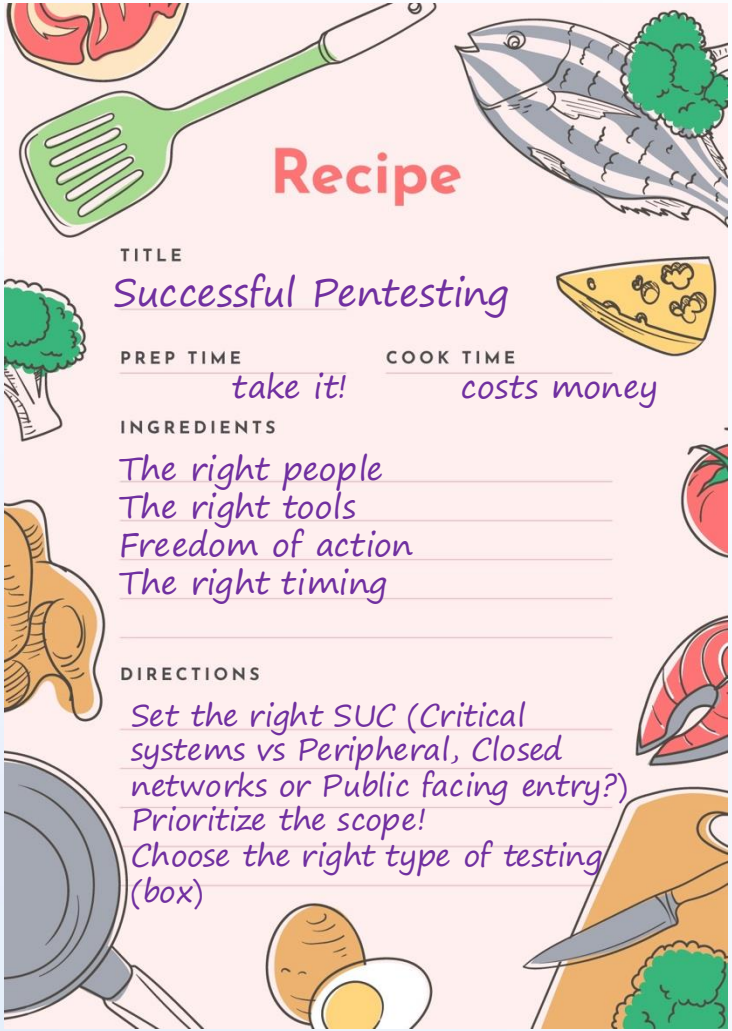
WHO – did we forgot the who?



Key Takeways



Key Takeways



designed by Freepik

Rail Tech Security Platform

CYLUSONE™

Providing 360-degree asset visibility and protection for all rail systems enabling real-time threat detection, advanced forensics, and mitigation

CylusOne Functions

- **Asset Visibility -** real time asset discovery, classification, and management.
- **Vulnerability Management** – continuous discovery, classification, and reporting.
- **Detection & Response** – threat and safety violations detection and mitigation playbooks powered by ML/AI.
- **Compliance** – meets rail frameworks and risk-reduction security directives.