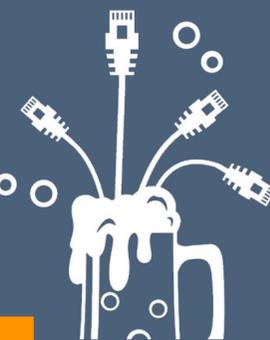


May 8-9 2025, Zürich

Unfold the OT Network Jungle

Martin Scheu

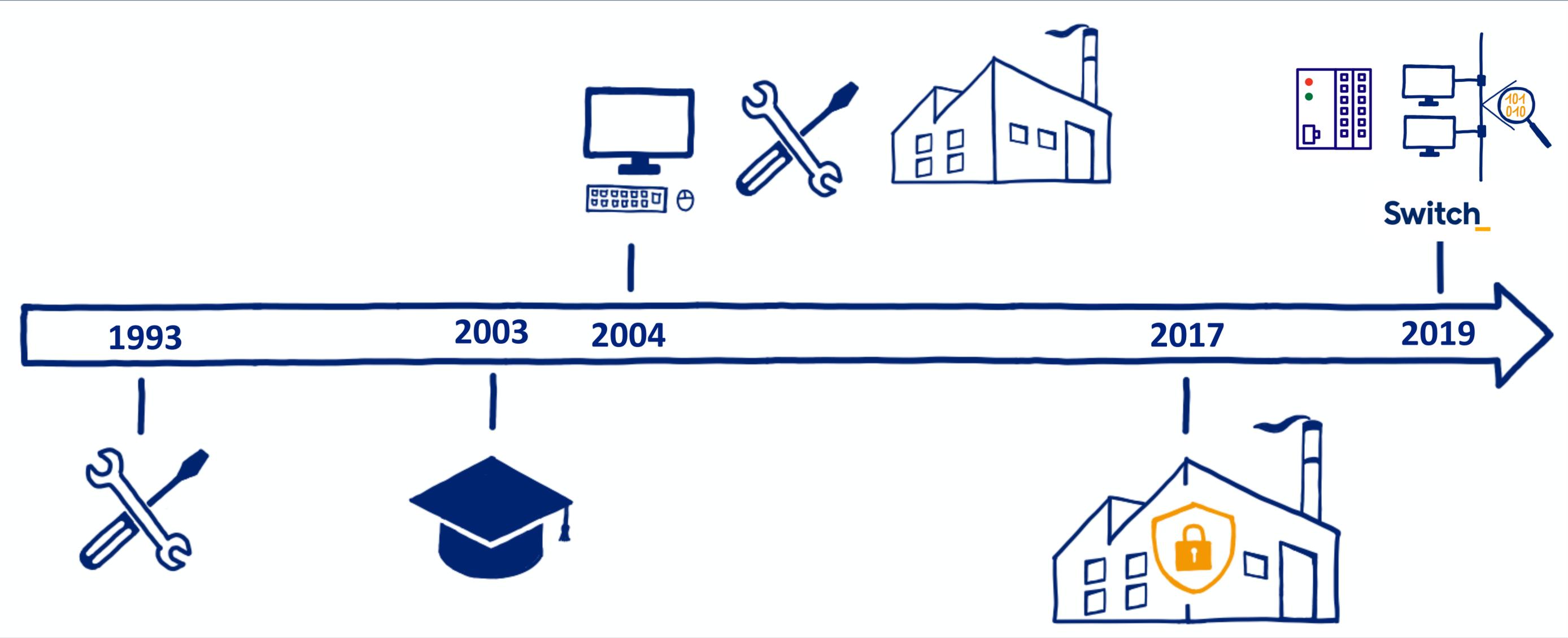
PacketFest'25



Agenda

- OT Network Overview
- Understanding your Network
- OT Network Examples
- Risk based Monitoring

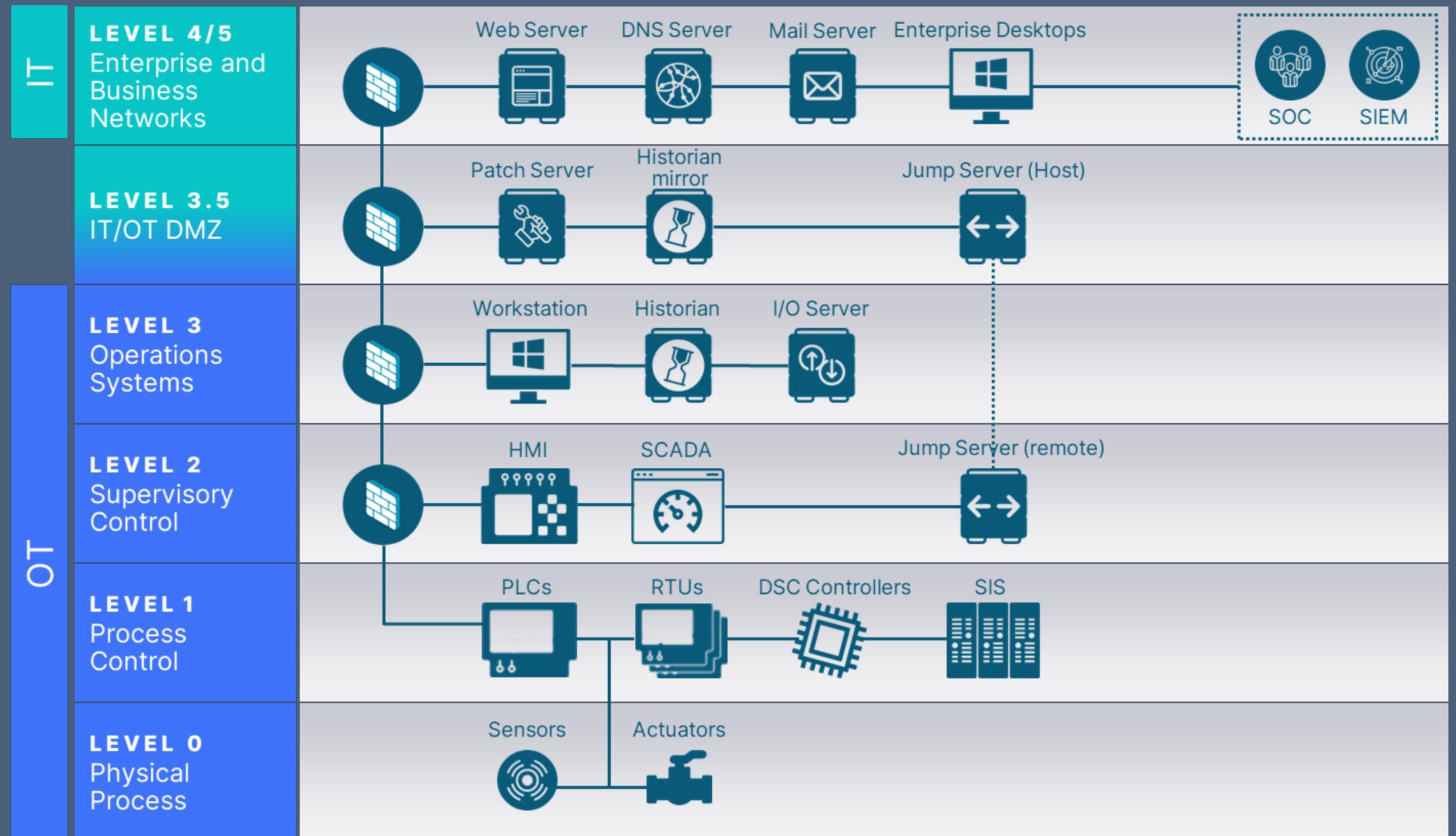
% whoami



OT Network Overview

OT Network in Theory

Purdue model

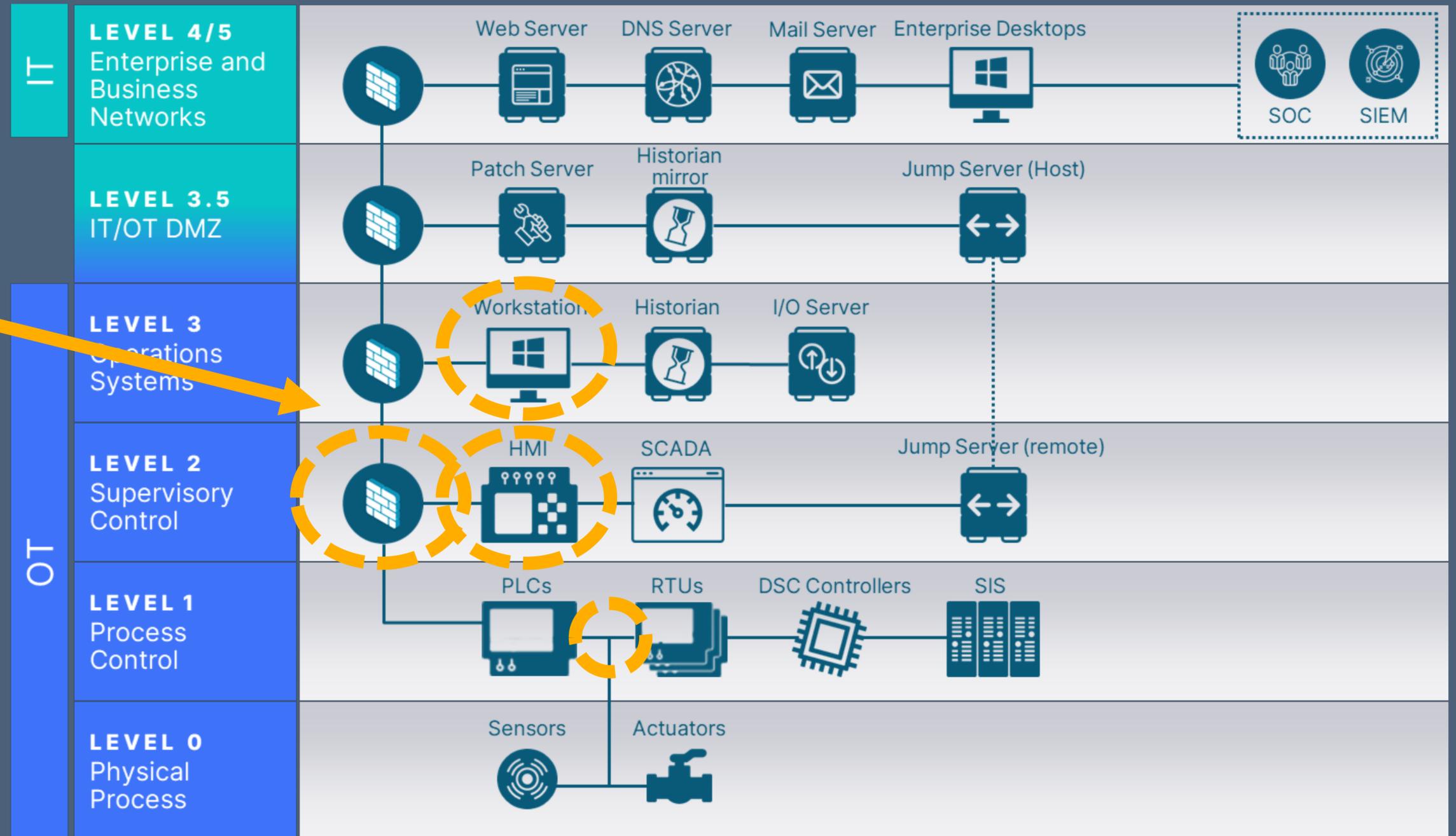


Source: <https://securityboulevard.com/2023/06/bringing-it-ot-security-together-part-2-bas-and-the-purdue-model/>

OT Network in real world

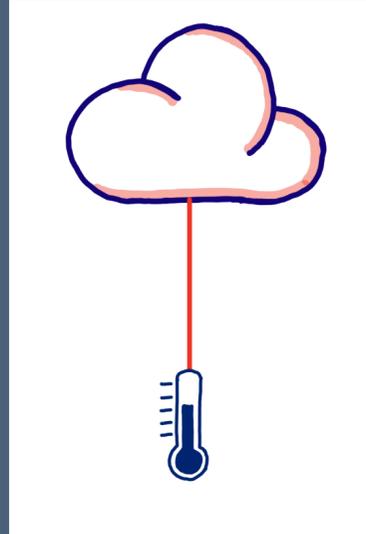
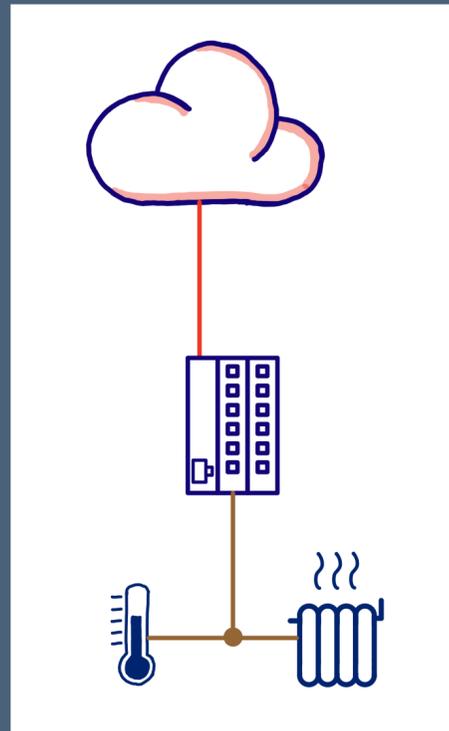
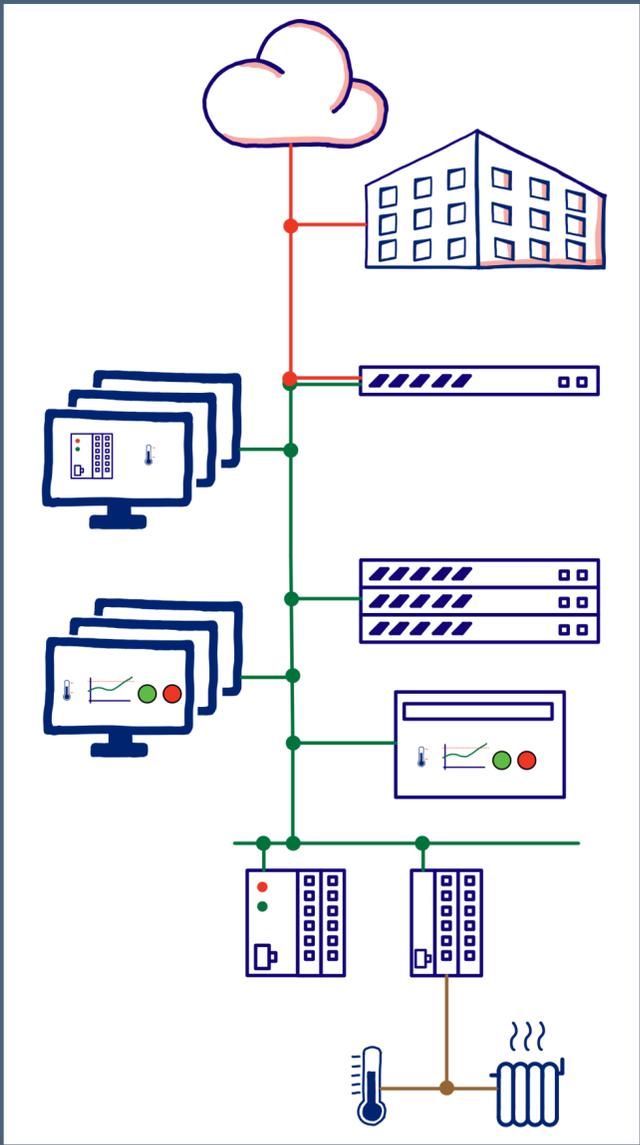
Purdue model

IT Equipment



Source: <https://securityboulevard.com/2023/06/bringing-it-ot-security-together-part-2-bas-and-the-purdue-model/>

Connectivity Evolution



Are OT Networks static?

- Common myth: OT networks are static .. ok, yes, if your network is 5 PLCs or so
- Reality:
 - Devices come and go
 - Increased IT-OT connectivity, e.g. because business needs data, Smart Meter
 - Remote access: suppliers, integrators or support engineers

Higher dynamic = higher risk → definitely need for visibility

OT Network Examples

Example 1 - Energy Sector

Foreign Devices – kind of Bring your own Device

- Solar Systems – residential ISP – cloud connection for data analysis
 - EV charging systems - billing
 - Smart Metering – billing – real time data
-
- And no, power outage in Spain/Portugal was not cyber related, also not low inertia (70% renewables), but most likely n-2 loss of power generation and RoCoF protection

Example 2 - Industrial Sector

- Preventive maintenance / maintenance contract: machine comes with own connectivity..
- Industrie 4.0: pay by use
- A mix of OT protocols
- “Old” protocols coming back, like ModbusTCP

Regulatory requirements

Germany - Attack detection system

- Logging and detection of security relevant events

Switzerland - Obligation to report an attack

- hence you need to be able to detect

IEC 62443-3-3:

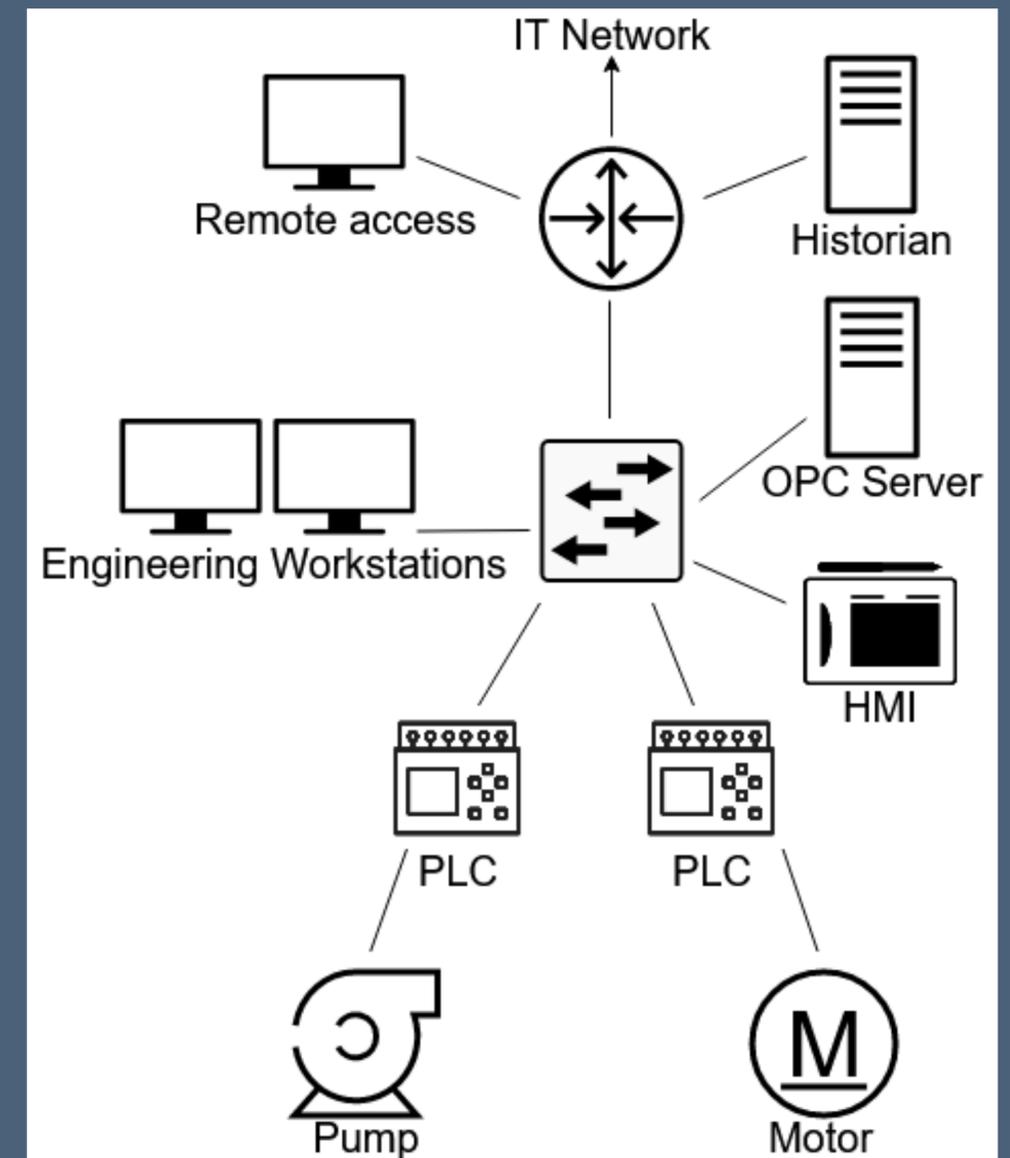
- SR 3.2: Detect malicious code (not just block it)
- SR 3.8: Network and security event logging

Understanding your Network

OT Network Ingress/Egress Traffic

Do you have visibility?

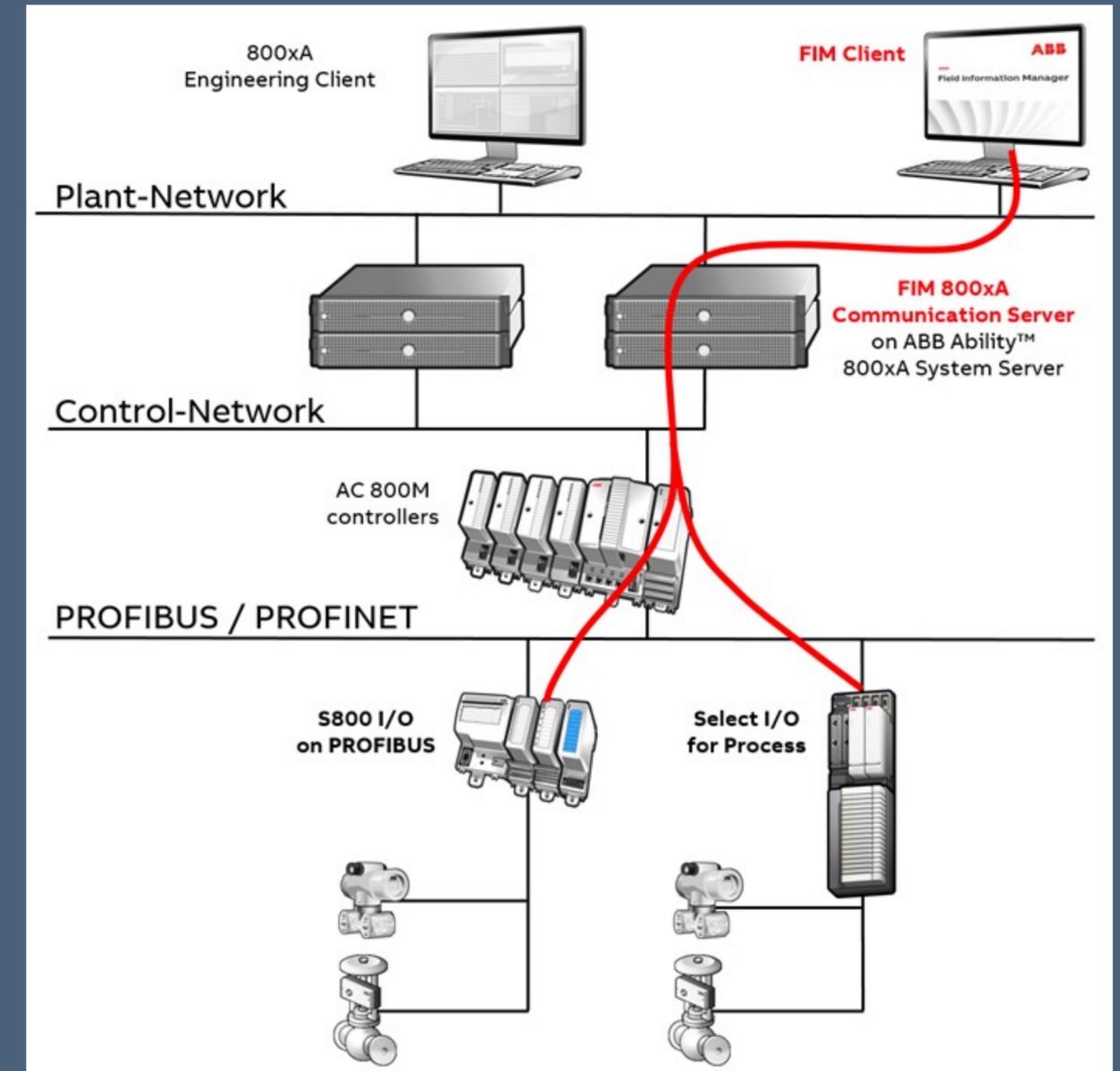
- Can OT devices reach the internet?
- What is permitted from the IT / office / engineering side to OT?
- Remote Access
Who, when / how long, from/to, what
- Remote Sites
- Do we really have everything?



Source: <https://craglem.com/>

Data flows

- Field devices
- Operator Station
- Engineeringstation
- Remote Sites
- Office
- Remote Access



<https://new.abb.com/control-systems/fieldbus-solutions/fim/connectivities/system800xa>

Risk based Monitoring

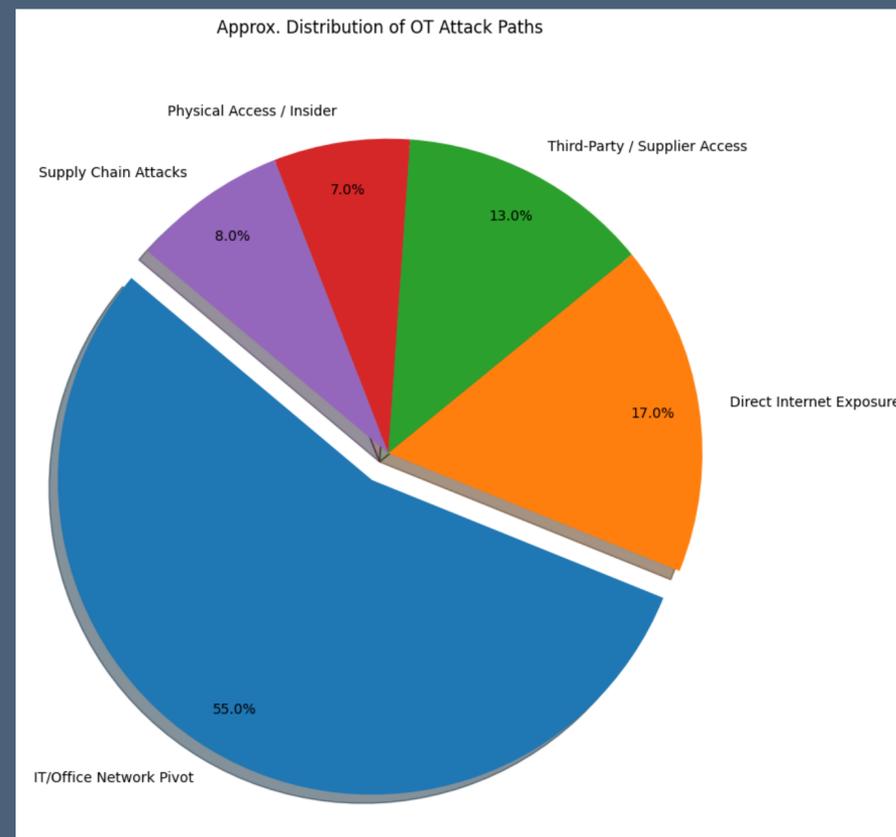
How do OT Attacks evolve

Reality Check

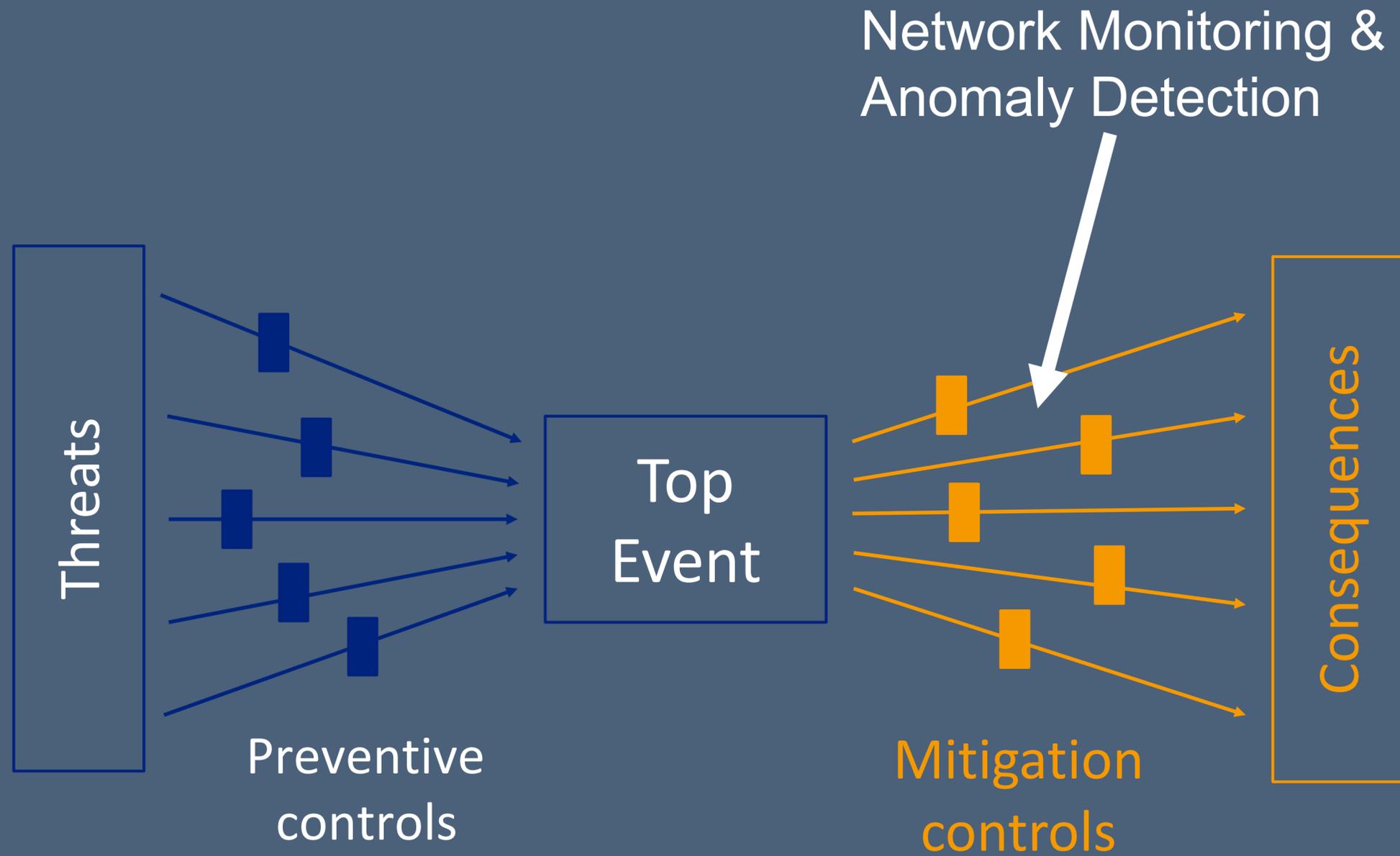
- Entering through the IT/office network and pivot into the OT environment
- Direct Internet Exposure
- Third-Party or Supplier Remote Access
- Physical Access or Insider Threat
- Supply Chain Attacks



The screenshot shows the header of the America's Cyber Defense Agency website. The logo on the left features an eagle and the text 'CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY' and 'CISA'. The main header text reads 'America's Cyber Defense Agency' and 'NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE'. A search bar is located on the right. The navigation menu includes 'Topics', 'Spotlight', 'Resources & Tools', 'News & Events', 'Careers', and 'About'. The breadcrumb trail is 'Home / News & Events / Cybersecurity Advisories / Alert / Unsophisticated Cyber Actor(s) Targeting Operational Technology'. The main content area displays an 'ALERT' titled 'Unsophisticated Cyber Actor(s) Targeting Operational Technology' with a release date of 'May 06, 2025'.



Keep in mind, that..



Open Source Monitoring

Monitoring Software

Open Source and/or with professional version, support (\$)

	Description	Installation, Production and Maintenance	ICS Protocol support
	All in one collection of open source tools, like zeek, suricata, arkime, netbox, opensearch and more	Docker only Rather complicated due the number of different components	Zeek scripts
 	All in one tool: - GUI - Alerting - Block-Lists and scripting	On Debian/Ubuntu easy to install	IEC-104, ModbusTCP
 SURICATA®	Network analysis and threat detection software File extraction	On Debian/Ubuntu moderate to install	S7
	Network “logging” software File extraction	On Debian/Ubuntu moderate to install	Many, scripts

Questions?

Thank you!

Stay safe and secure



FACTORY SECURED



martin@ics-cyber.ch



[martin-scheu](#)