May 7th, 2025, Zürich

OT Network Monitoring with Open Source SW

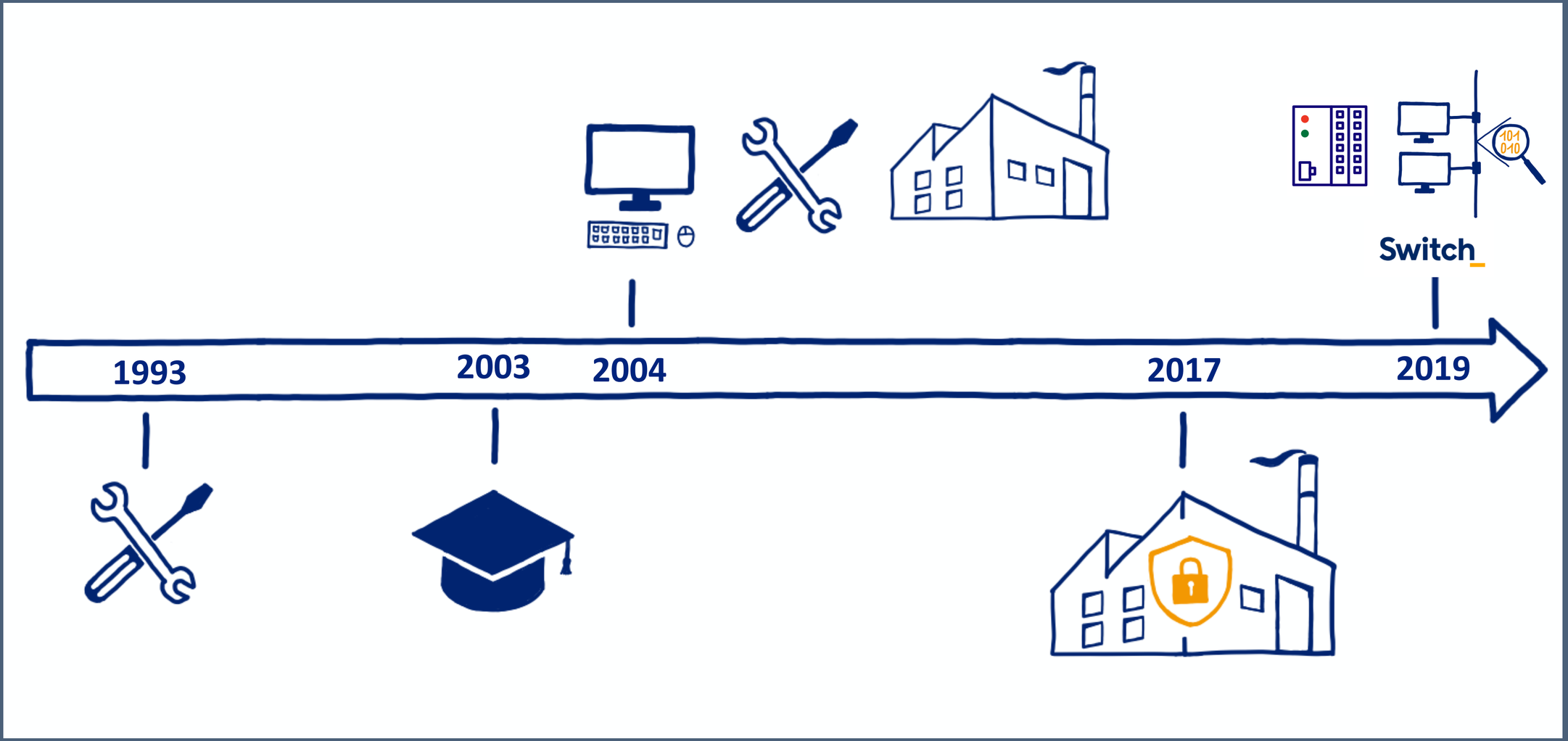
Martin Scheu

PacketFest'25

Agenda

- OT Networks today
- Tool overview
- Use of ntopng and ntap

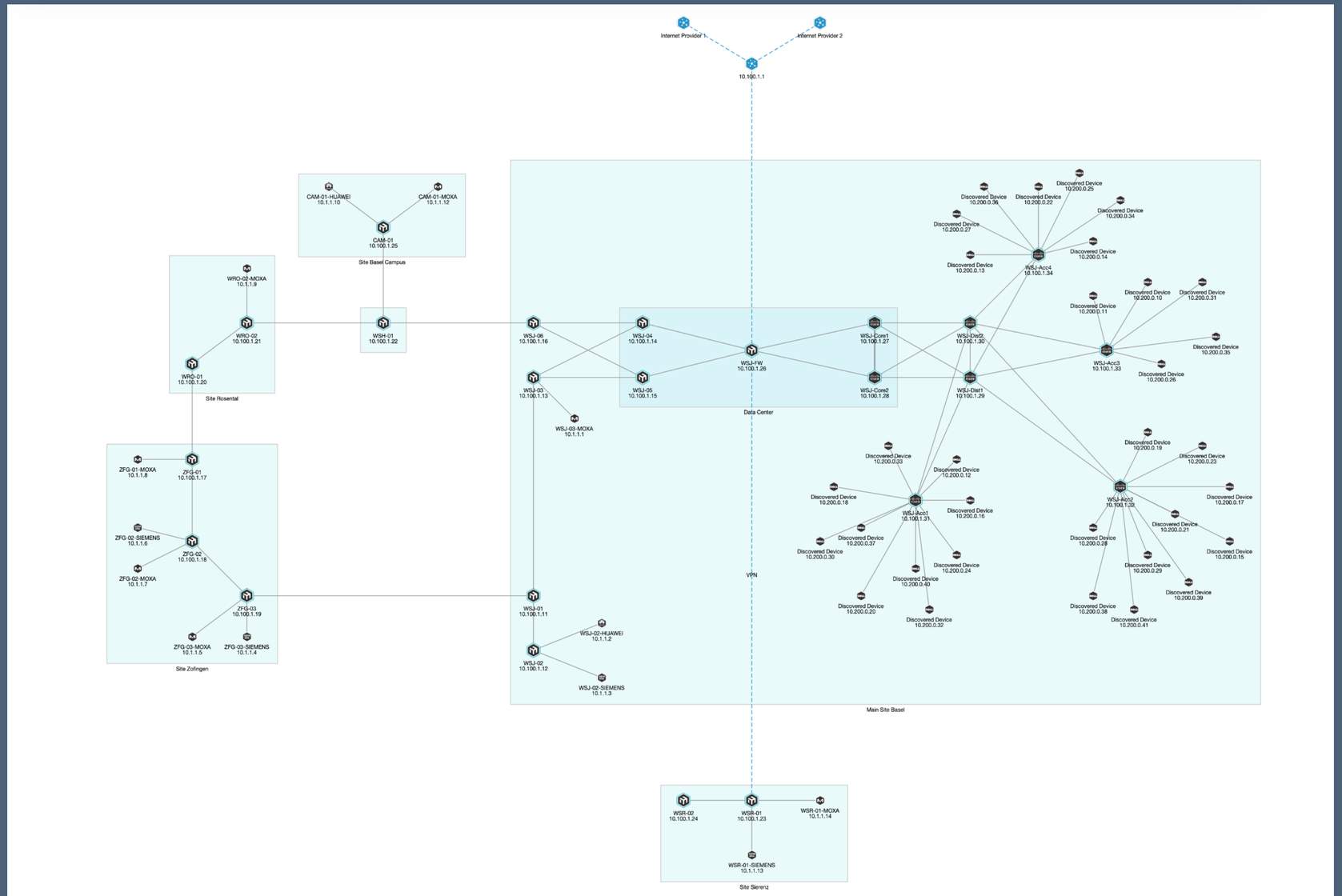
% whoami



OT Networks today

OT Network

- Ring structure
- OT DC
- One uplink
- Multi site architecture

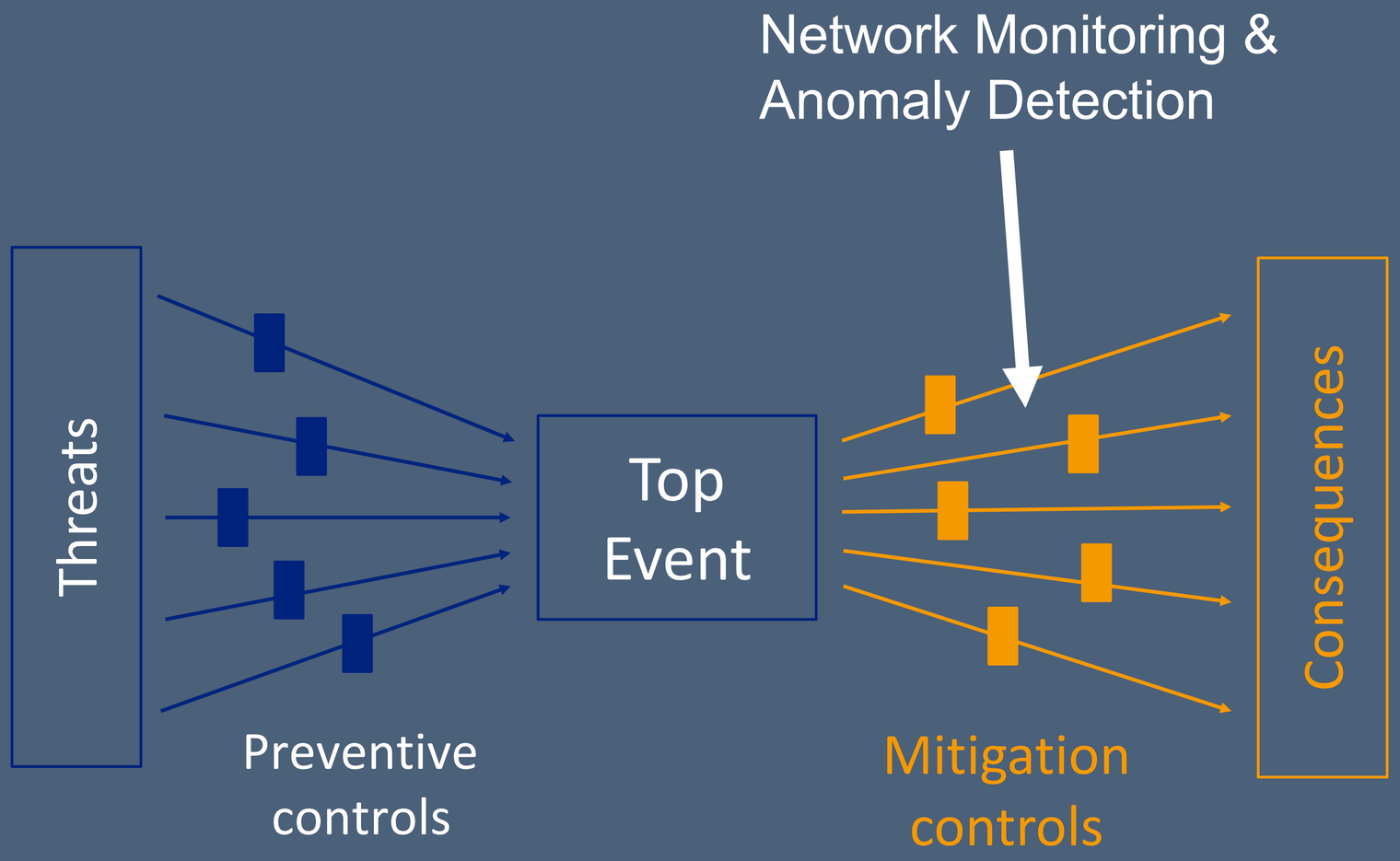


Why?

Its not only about cyber security..

- Configuration errors, e.g. Firewall port configuration, NTP configuration
- Technical issues, like OT protocol redundancy creating lots of traffic
- Having a “log book”
- Asset management
- And of course, cyber. Like non permitted remote access tool, device desperately trying to connect to the internet

Keep in mind, that..



Tooling

Monitoring Software

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

	Description	Installation, Production and Maintenance	ICS Protocol support
Malcolm	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
ntop	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
zeek®	Network “logging” software File extraction	On Debian/Ubuntu moderate to install	Many, scripts

PCAP Analysis

	Description	Installation, Production and Maintenance	ICS support
WIRESHARK	Check the bits and bytes	All major OS supported	Amazing!
Network Miner	One level ”above” wireshark File extraction, e.g. IEC-104	Windows only	Good
Zed (Brim)	Local “data lake”, working with json or Zeek log files	All major OS supported	Not by default
jupyter **Jupyter Lab**	Fast visualisation, like x over time	On Debian/Ubuntu moderate to install	n/a
gravwell	Ingest, Detect, Investigate, Monitor, and Visualize	Linux (Docker)	Good

How to

What to monitor?

Core Concepts of OT Network Monitoring

- What are we looking for?
- Asset visibility
- Protocol anomalies
- Unusual communication patterns
- Indicators of compromise (IoCs)
- Block lists

Where to monitor?

Placing sensors, using span ports, software taps

- Risk based approach. How does OT get attacked?
- We need to have visibility:
  - OT network in/out of OT network (north / south)
  - Internet in- / egress (I’d place it between firewall / internet)
  - Remote sites, internal traffic only

Use Cases

General

- ❑Connection of a new device, disconnection of a device
- ❑Rogue DHCP, DNS, SMTP or NTP server
- ❑Data packets, protocol / port from an unknown device or not intended protocol
- ❑Data transmission between devices that have not previously communicated
- ❑Events that occur at unusual times
- ❑Use of unexpected addresses (public IP addresses, etc.)
- ❑Generally noteworthy events such as address or port scans

Use Cases

OT Specific

- ❑ Unusual error messages
- ❑ Unsupported function calls, unknown function codes or function calls that have not been used before
- ❑ Flawed data packets
- ❑ Abnormal protocol behaviour
- ❑ Unexpected transition from one protocol to another
- ❑ Values outside of defined ranges
- ❑ Changes in frequency / periodicity or in cycle times
- ❑ Changing variance within certain periods of time

ntop

ntopng

- Proper setup:
  - Policies / Network Configuration:
    Unexpected DNS/NTP/DHCP/SMTP/Gateway Server Checks
    OT Protocol Checks
  - Add your Applications under Settings/Applications and Categories
    e.g. tcp:5510 for Synology Backup NAS – NAS
  - Historical Flows is a must
  - n2disk, very handy to have

ntap

Data diode functionality, runs as Docker Container

- Can run on modern PLCs (often network_mode: host is permitted ..)
- Make use of the filter: only capture and forward what is not normal
  e.g. known traffic between two PLCs does not forcingly be monitored.
  But traffic of a PLC towards the network switch management interface yes

Alerting

Make use of the multiple alerting options

- Even with proper baselining, depending the size of network and type of traffic, you will have alerts.
- Start with one or two use cases and try to tweak them right
- Try to setup regular “Threat Hunting” where you spend like 2h for figuring out why an alert was triggered and how you can mitigate it

Motivation

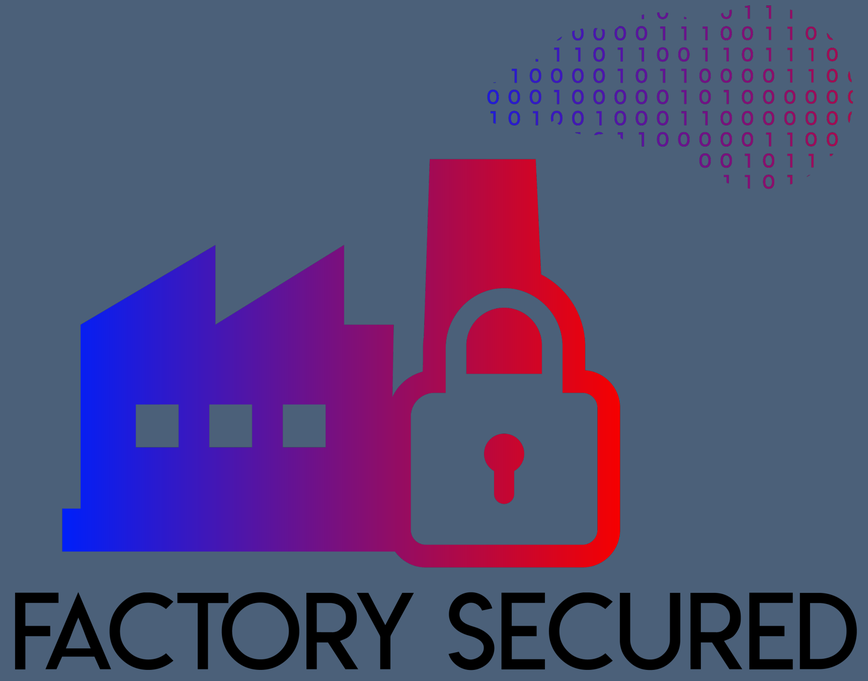
Working with Alerts is tedious

- Figure out how you stay motivated to get rid of false positives
- Involve OT engineers, you will see how they start to understand what is happening on the network level
- Do CTFs, there are great resources online

Questions?

Thank you!

Stay safe and secure



martin@ics-cyber.ch

martin-scheu