

The background of the slide features a dark blue header with a network-themed graphic. It includes a complex web of white lines connecting circular nodes, overlaid on a blurred image of server racks with glowing yellow and red lights.

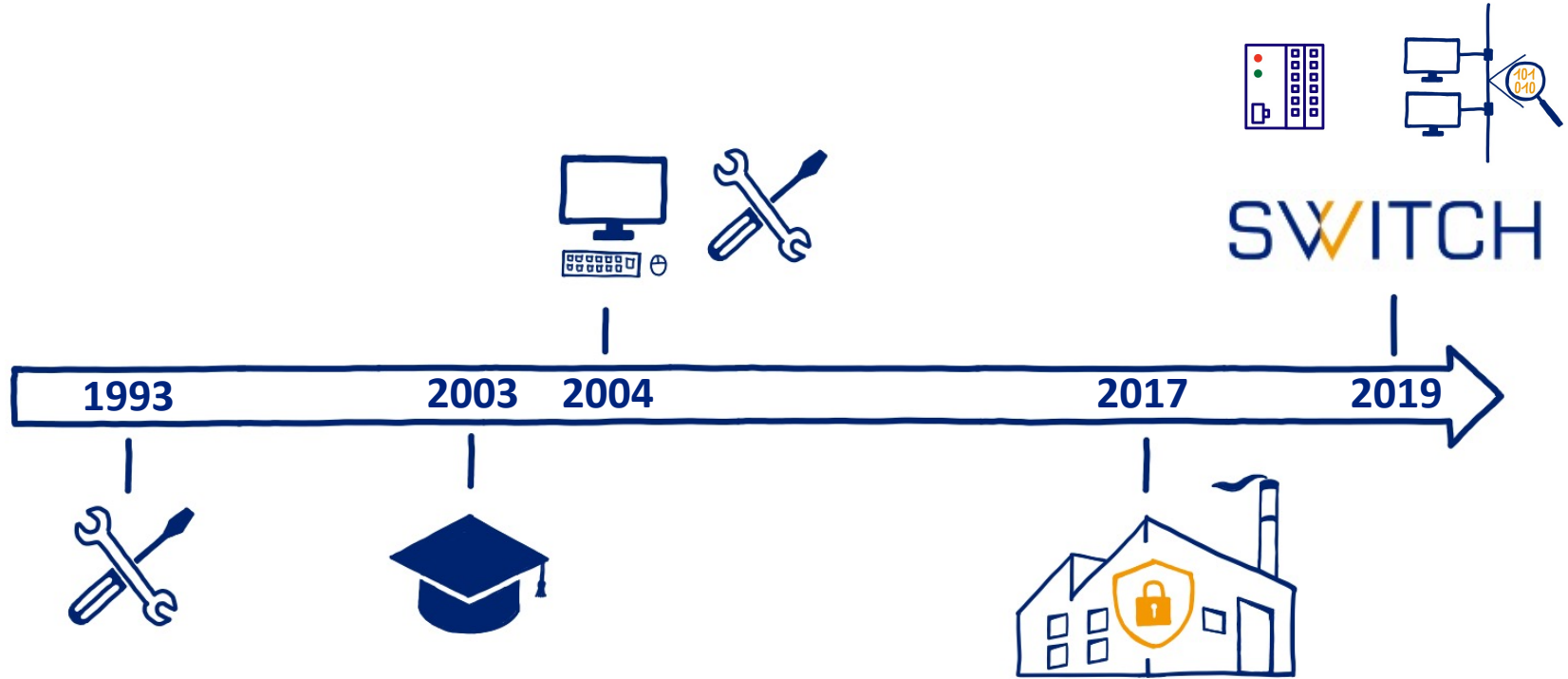
Network Security Monitoring in Critical Infrastructure

Martin Scheu

23. June 2022

ntopConf '22

#whoami



Agenda

What is Industrial Communication about

How to get started

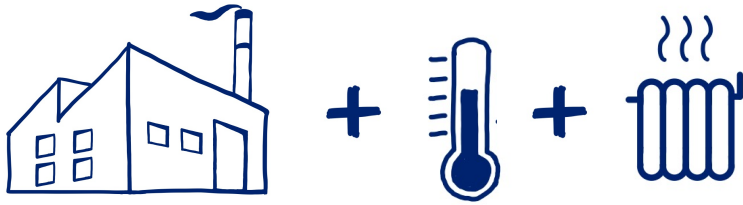
Monitoring Examples



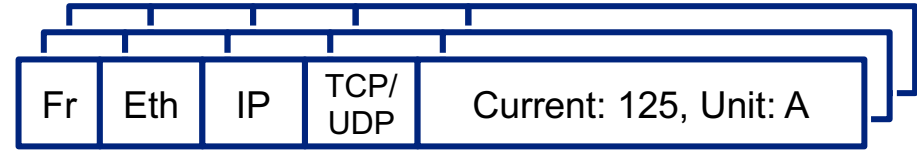
Industrial Communication

Environment

Industrial Control



Full pcap

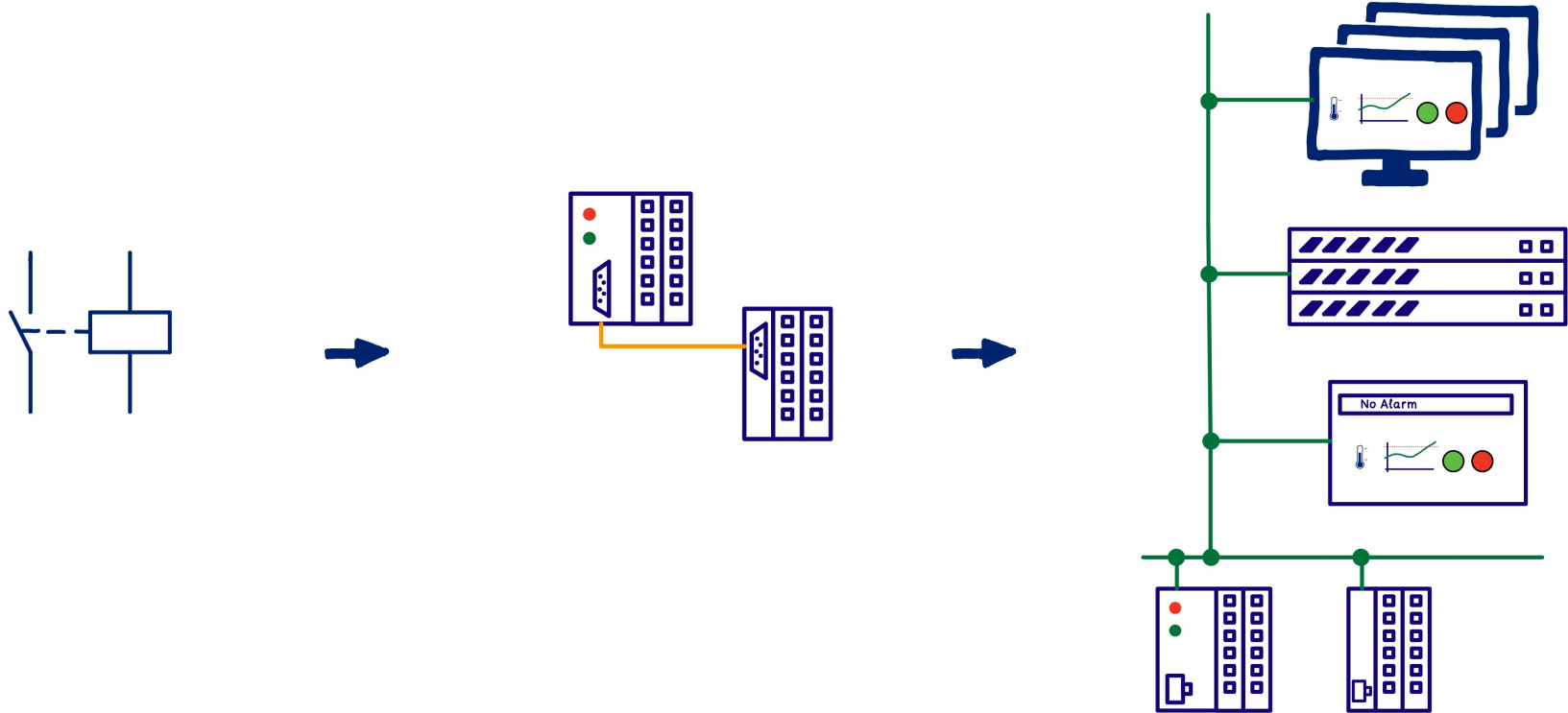


512 Mbit/s $\approx$ 5 TB/day

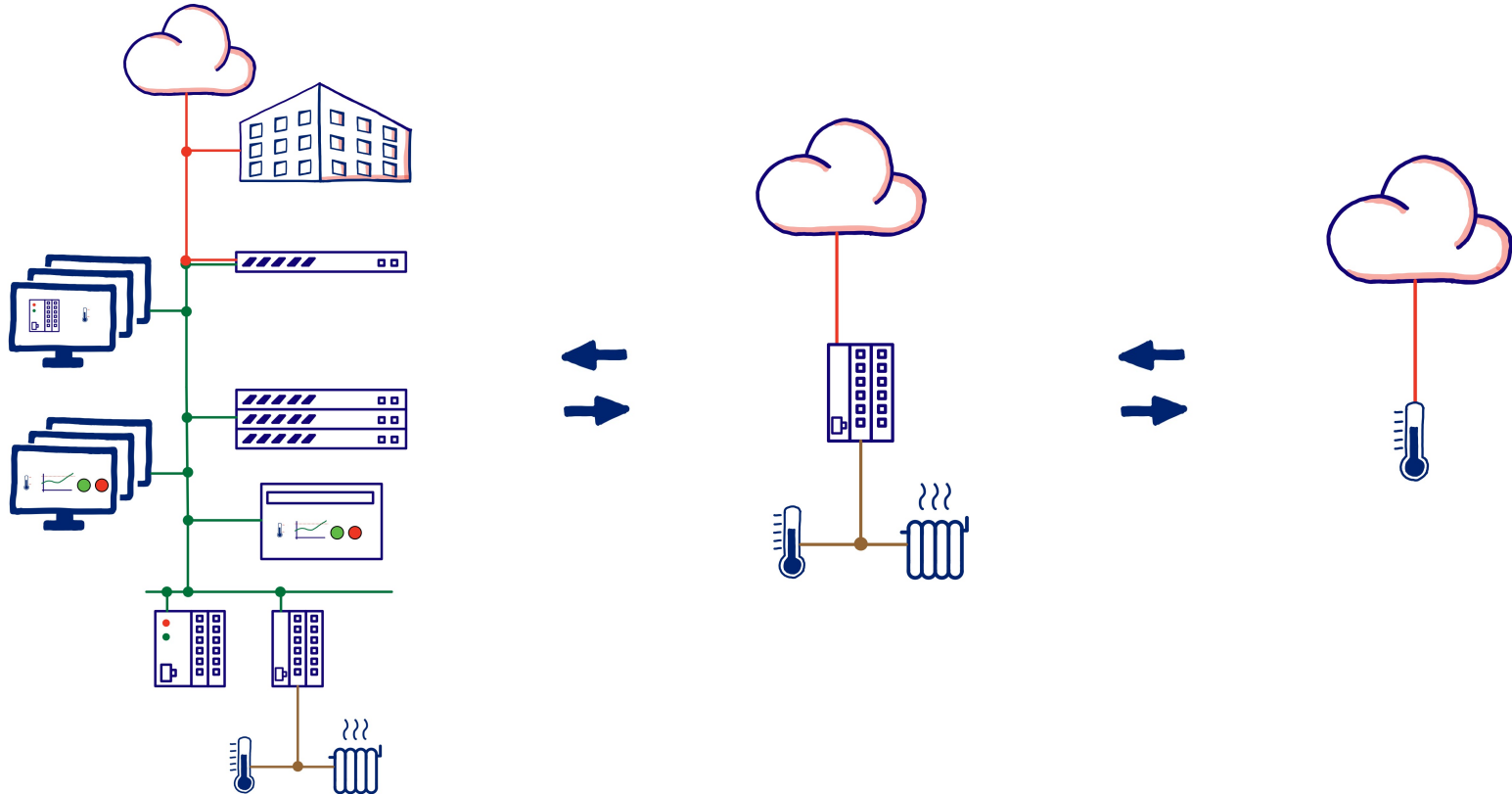
Flows

IP.Src	Src.Port	IP.Dst	Dst.Port	Proto
172.16.2.11	58336	172.16.2.1	53	DNS
172.16.2.1	45771	9.9.9.9	53	DNS

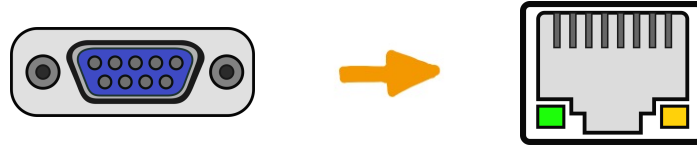
Connectivity Evolution I



Connectivity Evolution II



Industrial Protocol Characteristics



Data exchange Flow



Connection check / Keep a live Flows



Frame	Ethernet	IP	TCP/UDP	Current: 125, Unit: A
-------	----------	----	---------	-----------------------

Protocols

2 - wire

CAN
HART
IEC 60870
IO-Link
Modbus
PROFIBUS

Ethernet based

	PROFINET			OPC UA	IEC 60870-5-104
	IO	DGP/ RPC	CBA		
Application - 7		RPC	DCOM	UA	IEC 104
Presentation - 6					
Session - 5					
Transport - 4		UDP	TCP	TCP	TCP
Network - 3		IP	IP	IP	IP
Data Link - 2	TSN	C/C	C/C	C/C	C/C
Physical - 1	Eth	Eth	Eth	Eth	Eth

TSN

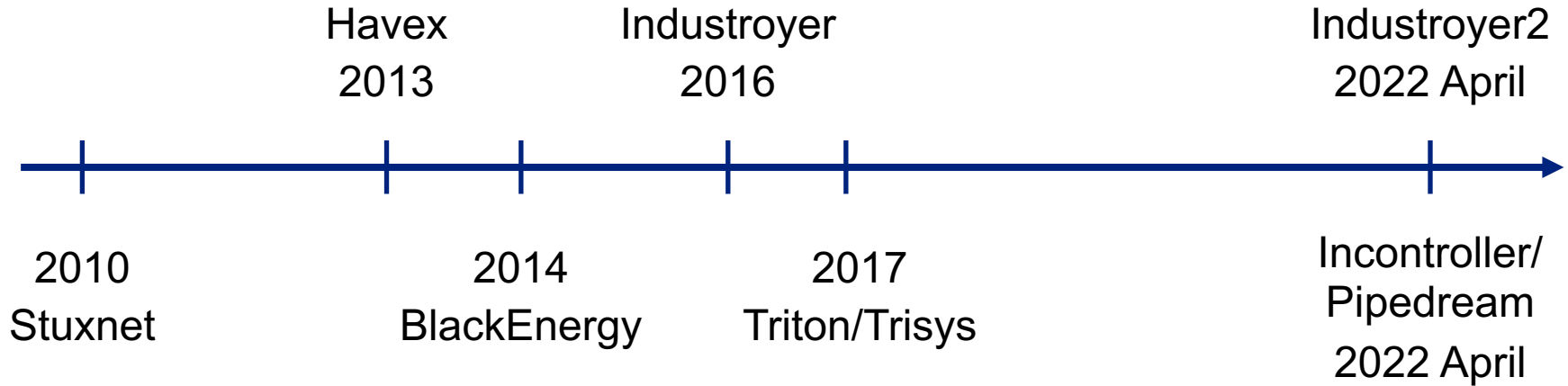
Safety

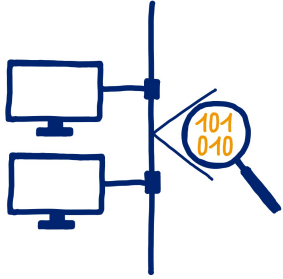
ProfiSAFE
IO-Link Safety
CIP Safety

Implemented as
“black channel”
on top of a
Protocol

TSN: Time sensitive network

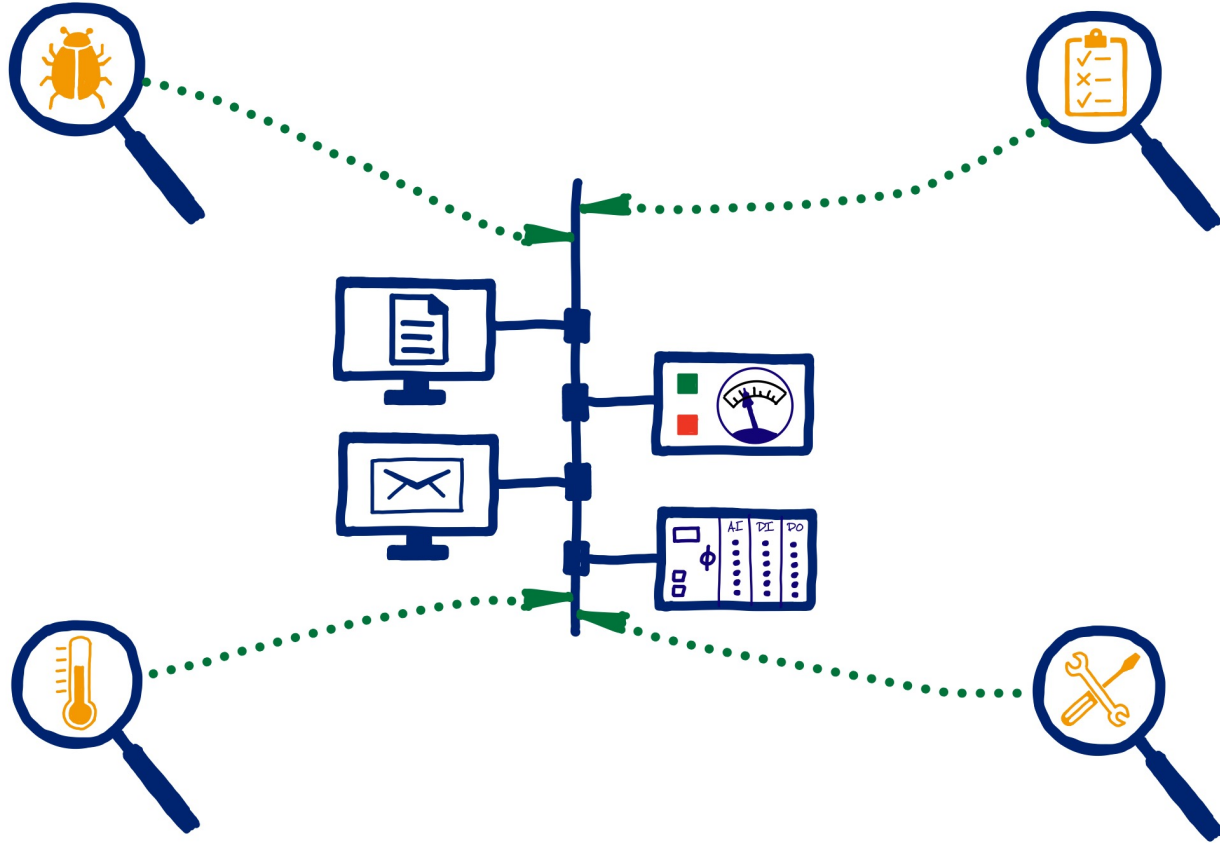
OT Malware



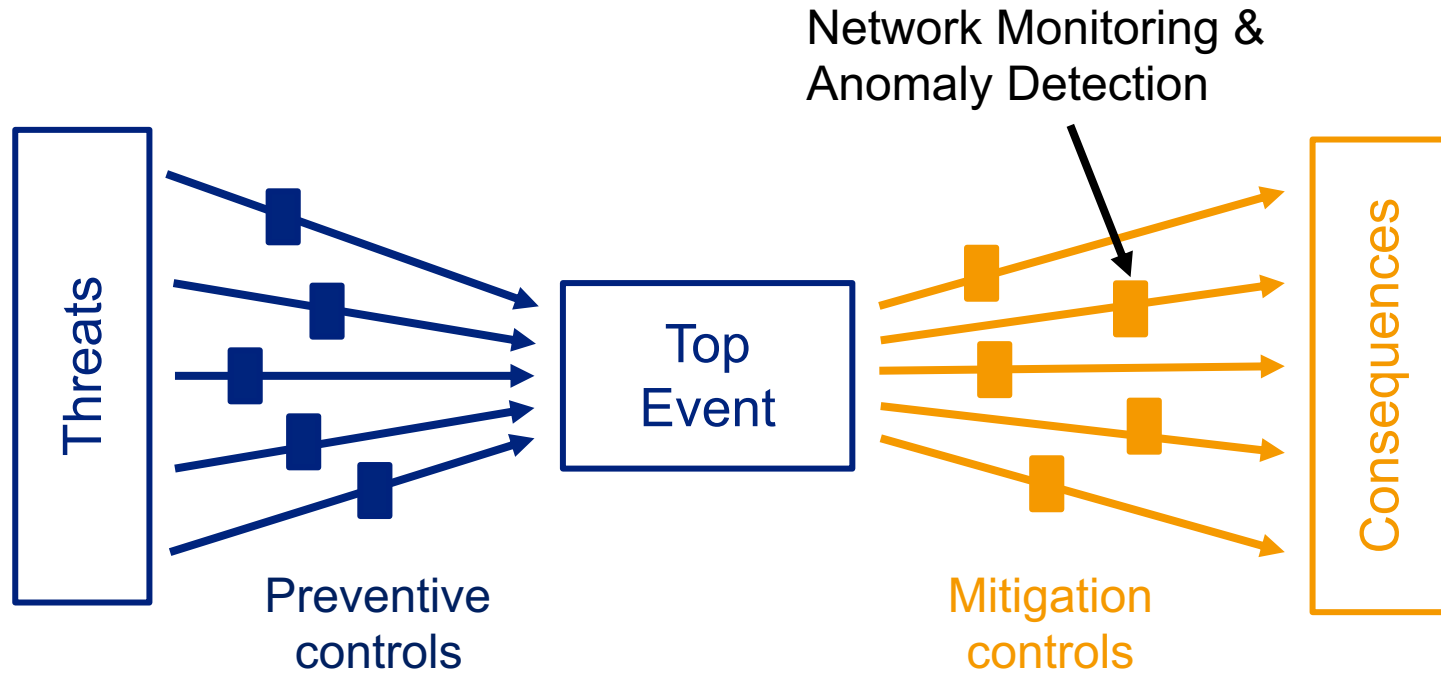


Industrial Network Security Monitoring

Why?



Engineering bow-tie



Commercial Products

CLAROTY



Asset discovery

passive
active

Asset management

Network monitoring

Anomaly detection

Vulnerability management

Threat intelligence feed

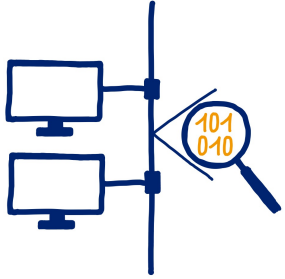
Version control of user software, e.g. PLC program

Open-source

	IEC 104	Script language	Ease of use	Resource requirements	Setup and installation
	no	zeek script	-	huge	very complicated
	yes	Lua	+	minimal	easy
	no	Lua	-	minimal	complicated
	yes	snort rules	-	minimal	complicated
	no	n/a	+	depends	easy - medium
	PoC available	zeek script	-	minimal	complicated

Toolitis





Where to start

Choose a tool



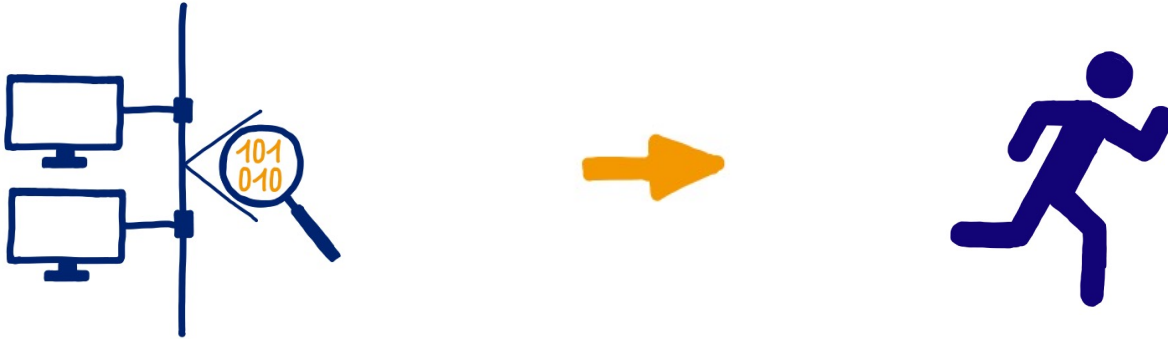
ntopng

One GUI for Alerts and Configuration.

Easy to use for not-field experts.

Use of Risk score for flows and hosts.

Choose a Use Case - Playbook



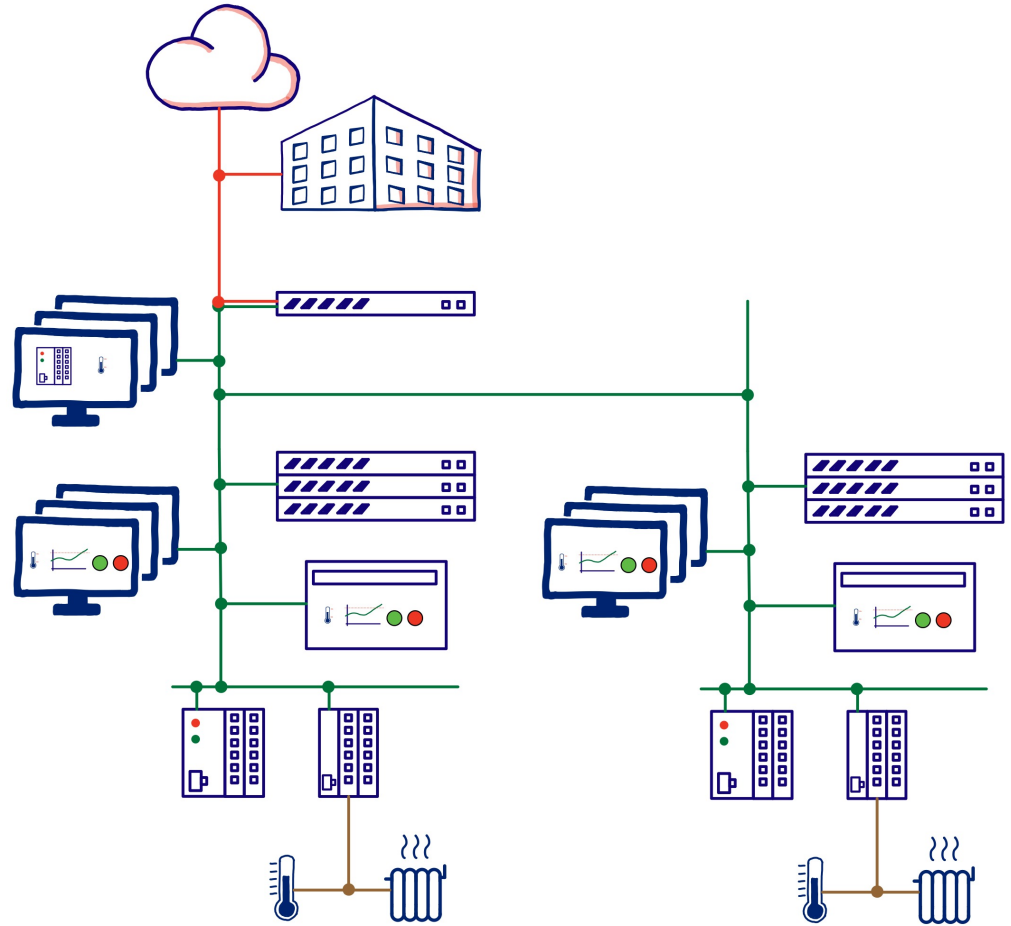
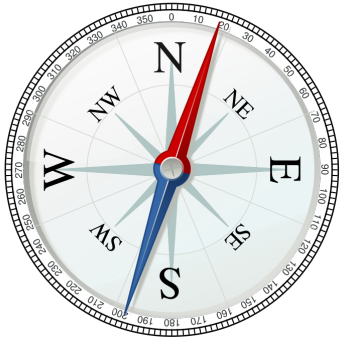
General Use Cases

- ☐ Unusual or exceptional activities in a network
- ☐ Connection of a new device, disconnection of a device
- ☐ Rogue DHCP, DNS, SMTP or NTP server
- ☐ Data packets from an unknown device
- ☐ Data transmission between devices that have not previously communicated
- ☐ Data transmission via a protocol / port that has not been used before
- ☐ Data transmission via an unusual protocol or one not intended for the purpose at hand
- ☐ Events that occur at unusual times
- ☐ Use of unexpected addresses (public IP addresses, etc.)
- ☐ Generally noteworthy events such as address or port scans
- ☐ Changes in network quality, including high broadband usage, increased round-trip times and smaller TCP window sizes

ICS Use Cases

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

Place the Sensor



Best practice

Select Use Cases together with OT Colleagues.

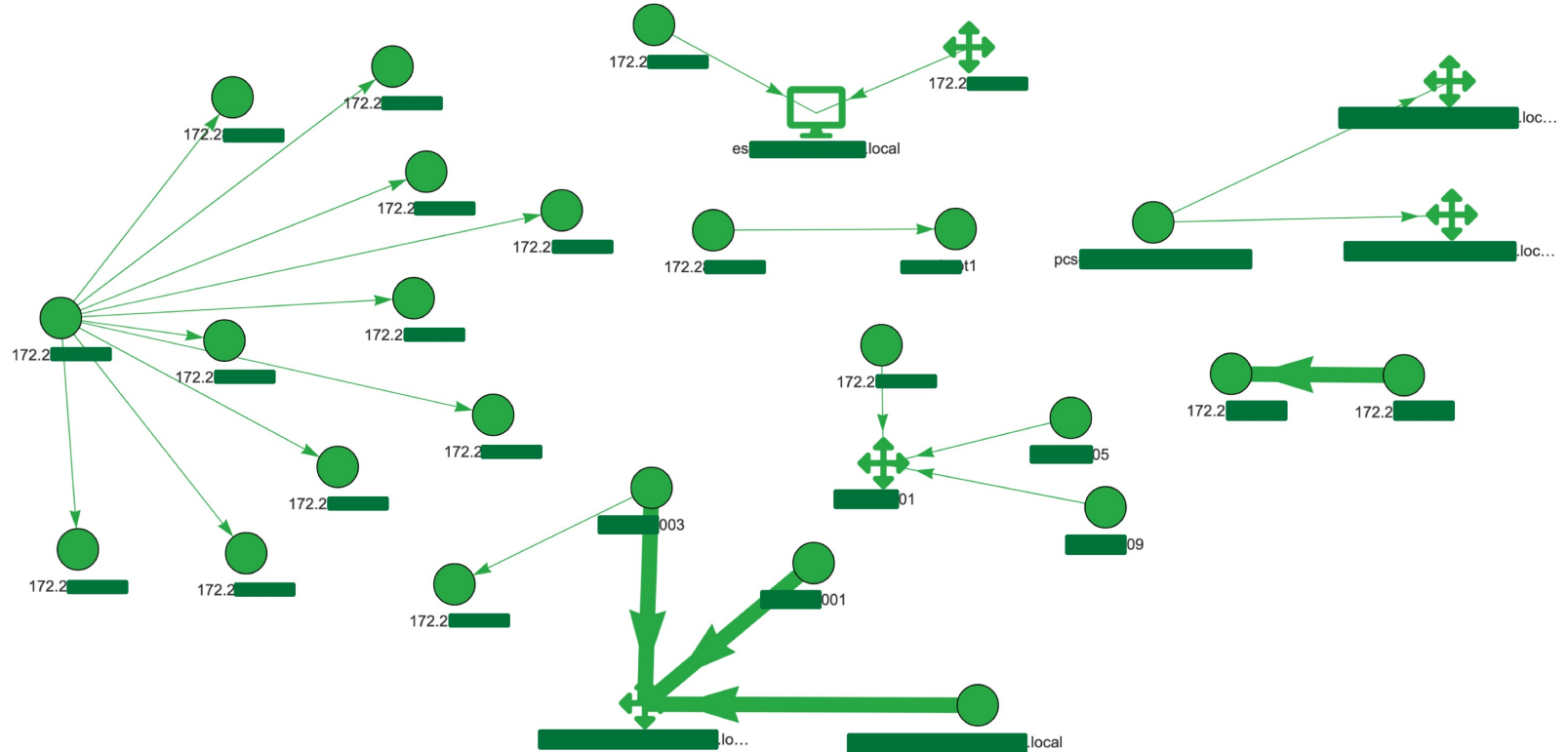
Besides the use case, define the alerting and playbook as well.

Have regular “Monitoring” meetings.



Examples

Example I - Remote Support



Example II - GEO Fence on Firewalls

Date/Time	Score	Application	Alert	Flow	De:
09/11/2021 10:13:26	200	TCP:HTTP	Blacklisted Flow	45.134.144.42@3654:44588	Bl...

Other Issues Remote to Local Insecure Protocol [Score: 100] [Predominant Traffic: Srv → Cli]

7
/ 90

7 security vendors flagged this IP address as malicious

45.134.144.42 (45.134.144.0/24)
AS 49870 (Alsyon B.V.)

DE

DETECTION	DETAILS	RELATIONS	COMMUNITY
Certego	Malicious	Comodo Valkyrie Verdict	Malicious
CRDF	Malicious	CyRadar	Malicious
GreenSnow	Malicious	IPsum	Malicious
Spamhaus	Malicious	Abusix	Clean

v4.whois.cymru.com

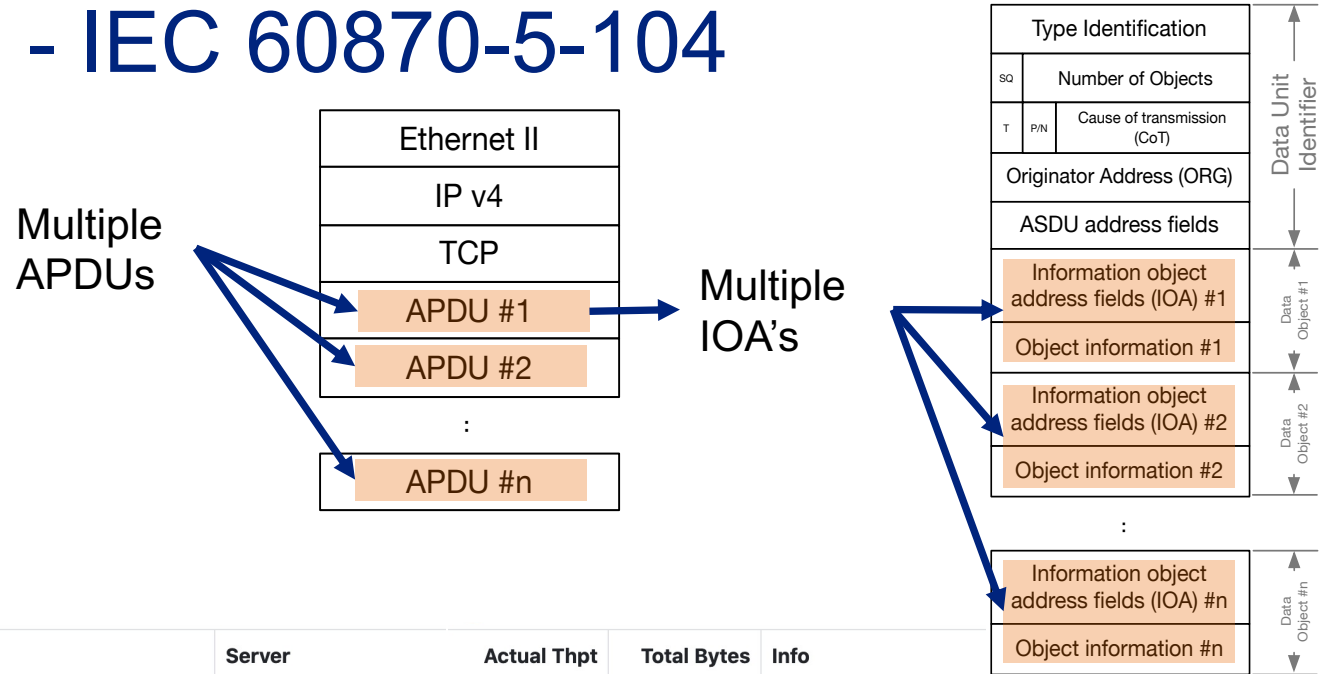
The server returned 2 line(s).

AS | IP
49870 | 45.134.144.42

CC
HK

AS Name
AS49870-BV, NL

Example III - IEC 60870-5-104

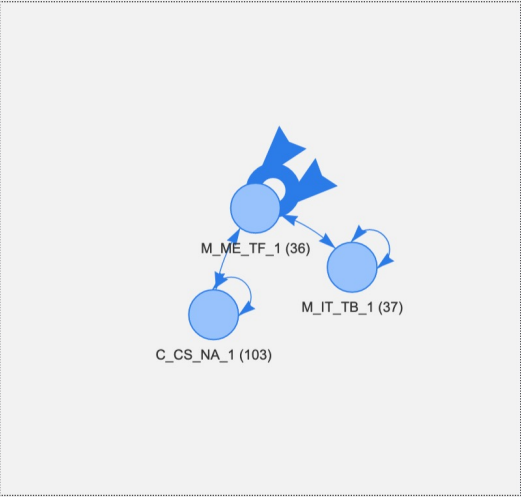


Application	Protocol	VLAN	Client	Server	Actual Thpt	Total Bytes	Info
IEC60870 🍌	TCP	21	🔴:2404	🔴👤:44404	0 bps —	100.48 KB ↑	<- S, RX 21582
IEC60870 🍌	TCP	21	🔴...:2404	🔴👤:59749	0 bps —	53.31 KB ↑	-> I, RX 65, TX 28985
IEC60870 🍌	🚩 TCP	21	🔴👤:58463	🔴:2404	0 bps —	8.44 KB —	<- S, RX 14
IEC60870 🍌	TCP	21	🔴👤:54827	🔴:2404	0 bps —	12.1 KB ↑	-> U (TESTFR con)

Example III - IEC 60870-5-104

Alarm Type	Score	Applikation	Beschreibung	Actions
! Invalid IEC Transition	50	IEC60870 👍	Invalid transition detected [M_ME_NB_1 (11) -> C_CS_NA_1 (103)] [Flow: Lokaler Host :2404 ⇄ Lokaler Host :22525] [TCP] [Applikation: IEC60870] [Info: IEC60870] ⚙️	 

Type ID Transitions



M_ME_TB_1 (36) ⇄ M_ME_TB_1 (36)	98.651 %
M_IT_TB_1 (37) ⇄ M_IT_TB_1 (37)	1.000 %
M_ME_TB_1 (36) → M_IT_TB_1 (37)	0.116 %
M_IT_TB_1 (37) → M_ME_TB_1 (36)	0.116 %
C_CS_NA_1 (103) → M_ME_TB_1 (36)	0.047 %
M_ME_TB_1 (36) → C_CS_NA_1 (103)	0.047 %
C_CS_NA_1 (103) ⇄ C_CS_NA_1 (103)	0.023 %

Transitions	normal operations traffic	malware
M_ to M_	> 1000	0
M_ to C_ or C_ to M_	> 0 && < 10	0
C_ to C_	0	> 10

Type I-S Ack Latency (Average / Std Dev)	0.160 ms (0.474 msec)
Messages Breakdown	83.9% 16.1%
Messages Lost / Retransmissions	← 0, → 18 / 1 Retransmitted

Example IV - Clear Text Passwords

Alert Type ☐ Clear-text credentials × Filters



Top Hosts

- [REDACTED] (50.0%)
- [REDACTED]@32 (50.0%)
- [REDACTED]!...@32 (50.0%)

Show entries

Date/Time	Score	Application	Alert	Flow
10:01:26	100	TCP:HTTP	Clear-text credentials	[REDACTED]:32:50985 ⇄ calendar.uefa.com@32:80
10:05:02	100	TCP:HTTP	Clear-text credentials	[REDACTED]@32:60413 ⇄ [REDACTED]!...:80

Example V - Malware Traffic

2021-09-10...rcise.pcap ▼

Hosts Map | 🏠

desktop-kkitb6q

Score as Attacker: 12,305

Score as Victim: 5

12,305

Top Hosts

- desktop-kkitb6q (98.6%)
- 94.158.245.52 (44.6%)
- 10.9.10.9 (12.2%)

Top Alerts

- Missing TLS SNI (29.7%)
- Too Long TLS Certificate... (23.0%)
- TLS Certificate Self-sig... (16.2%)

Show 200 entries

Date/Time	Score	Application	Alert	Flow
16:37:25	250	TCP:HTTP	Binary Application Trans...	desktop-kkitb6q:58131 → simpsonssavings.com:80
Description Detected binary application transfer [simpsonssavings.com/bmdff/BhoHsCtZ/MLdmpfjX/5uFG3Dz7yt/date1?BN... [Score: 250] [Method: GET] [Return Code: 200] [URL: simpsonssavings.com/bmdff/BhoHsCtZ/MLdmpfjX/5uFG3Dz7yt/date1?BN...]				
Other Issues				
16:37:25	210	TCP:TLS	TLS Certificate Self-sig...	desktop-kkitb6q:58132 → 167.172.37.9:443
Description TLS Certificate Self-signed [Issuer: C=UK, ST=London, L=London, O=LL EST, OU=UK System, CN=londonareloeli.uk][Subject: C=UK, ST=London, L=London, O=LL EST, OU=UK System, CN=londonareloeli.uk]				
Other Issues Missing TLS SNI [Score: 100] [Main Direction: Cli → Svr], Possibly Client Malicious JA3 Signature [Score: 100] [Main Direction: Cli → Svr], TLS not carrying HTTPS [Score: 100] [Main Direction: Cli → Svr]				



LOOKS LIKE LOT OF WORK

imgflip.com



Thank you!



martin.scheu@switch.ch



[martin-scheu](#)



[@martin_scheu](#)