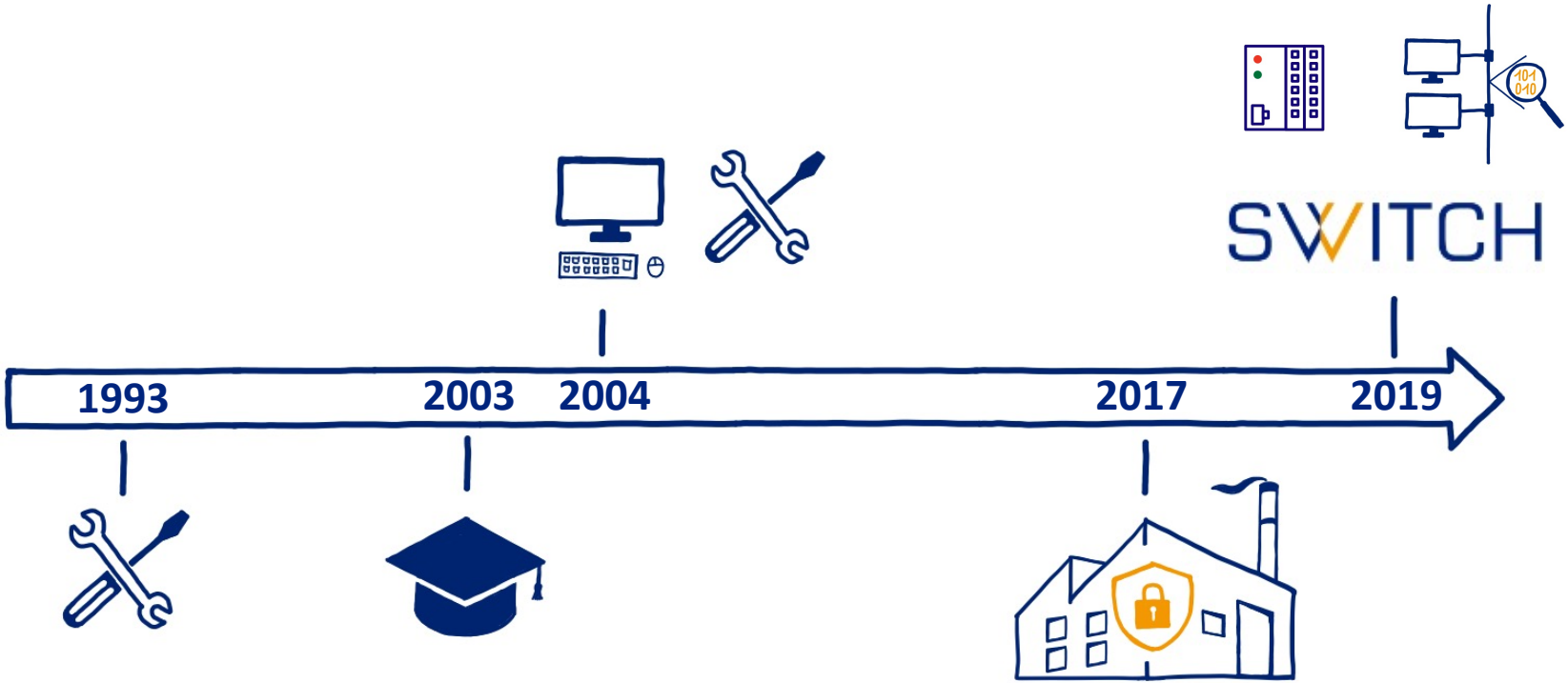
Network Security Monitoring in Critical Infrastructure

Martin Scheu

23. June 2022

ntopConf '22

#whoami



Agenda

What is Industrial Communication about

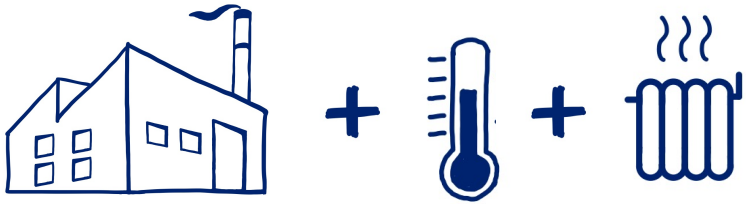
How to get started

Monitoring Examples

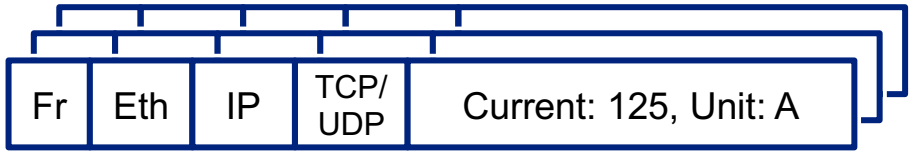
Industrial Communication

Environment

Industrial Control



Full pcap

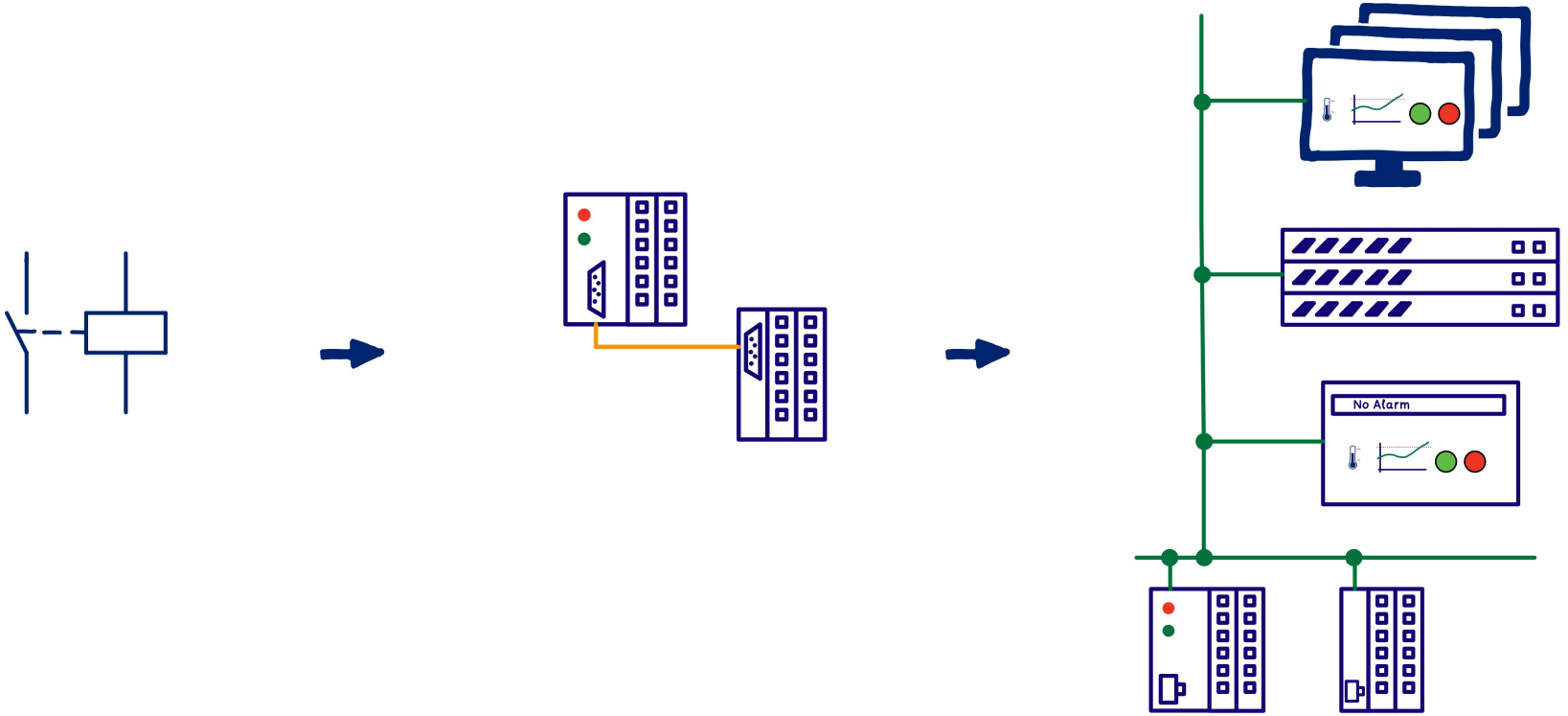


512 Mbit/s ≈ 5 TB/day

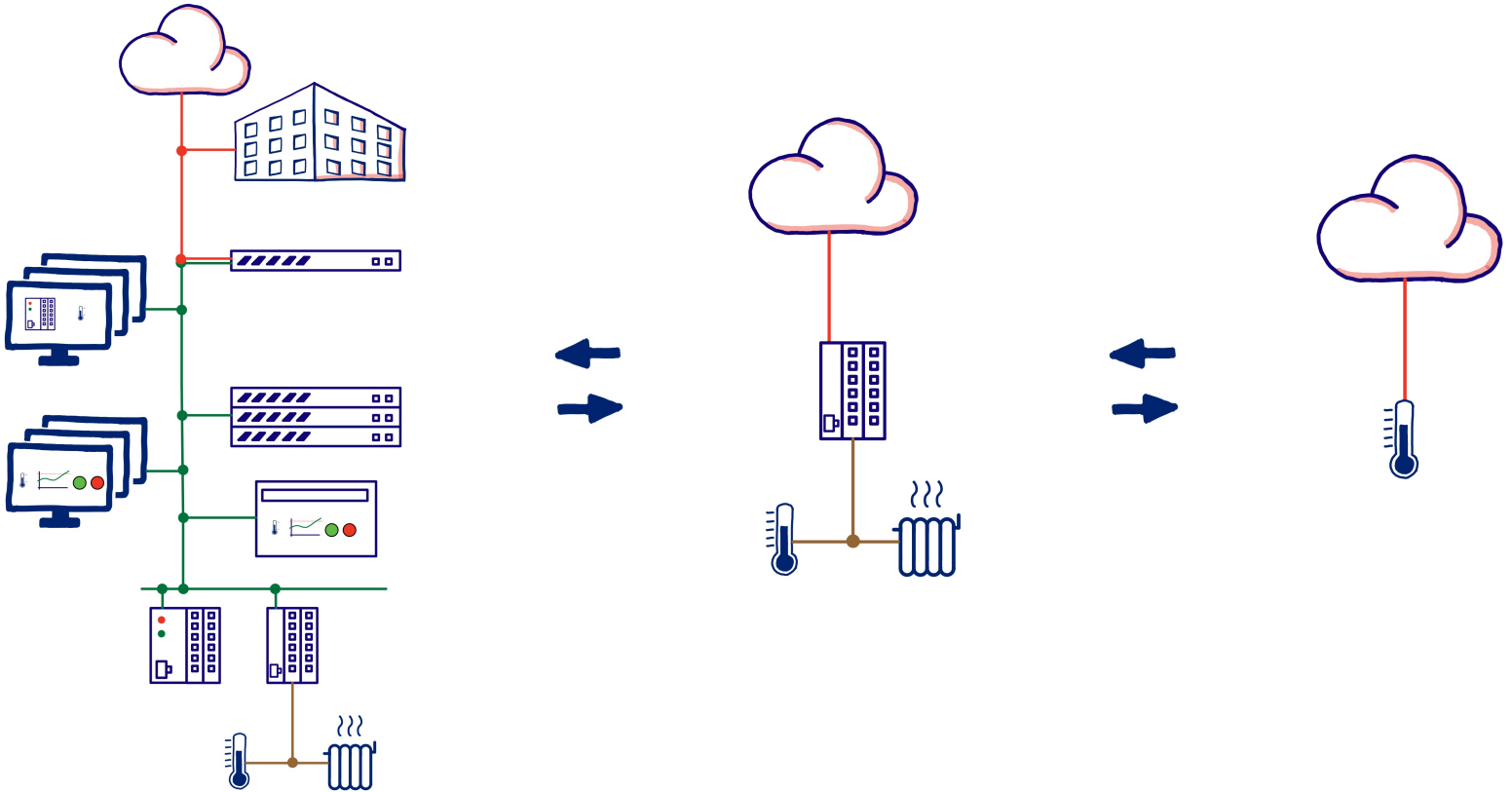
Flows

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

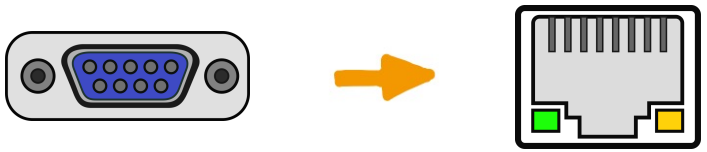
Connectivity Evolution I



Connectivity Evolution II



Industrial Protocol Characteristics



Data exchange Flow

Connection check / Keep a live Flows

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

Source symbols: https://openclipart.org

Protocols

2 - wire

CAN

HART

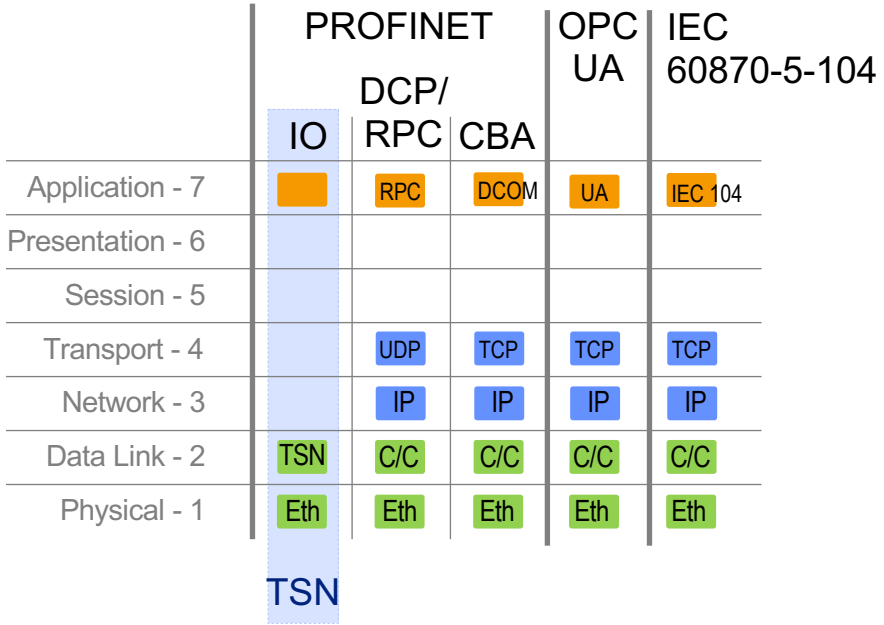
IEC 60870

IO-Link

Modbus

PROFIBUS

Ethernet based



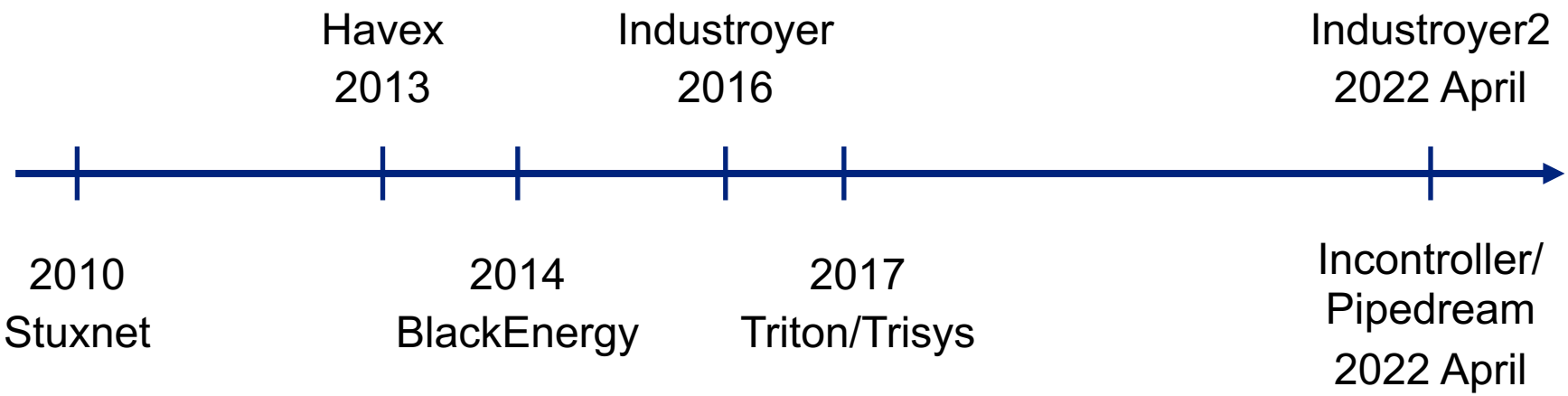
TSN: Time sensitive network

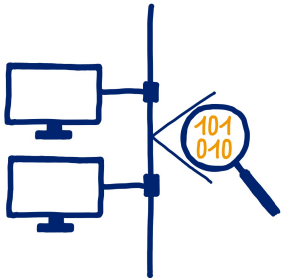
Safety

ProfiSAFE
IO-Link Safety
CIP Safety

Implemented as “black channel” on top of a Protocol

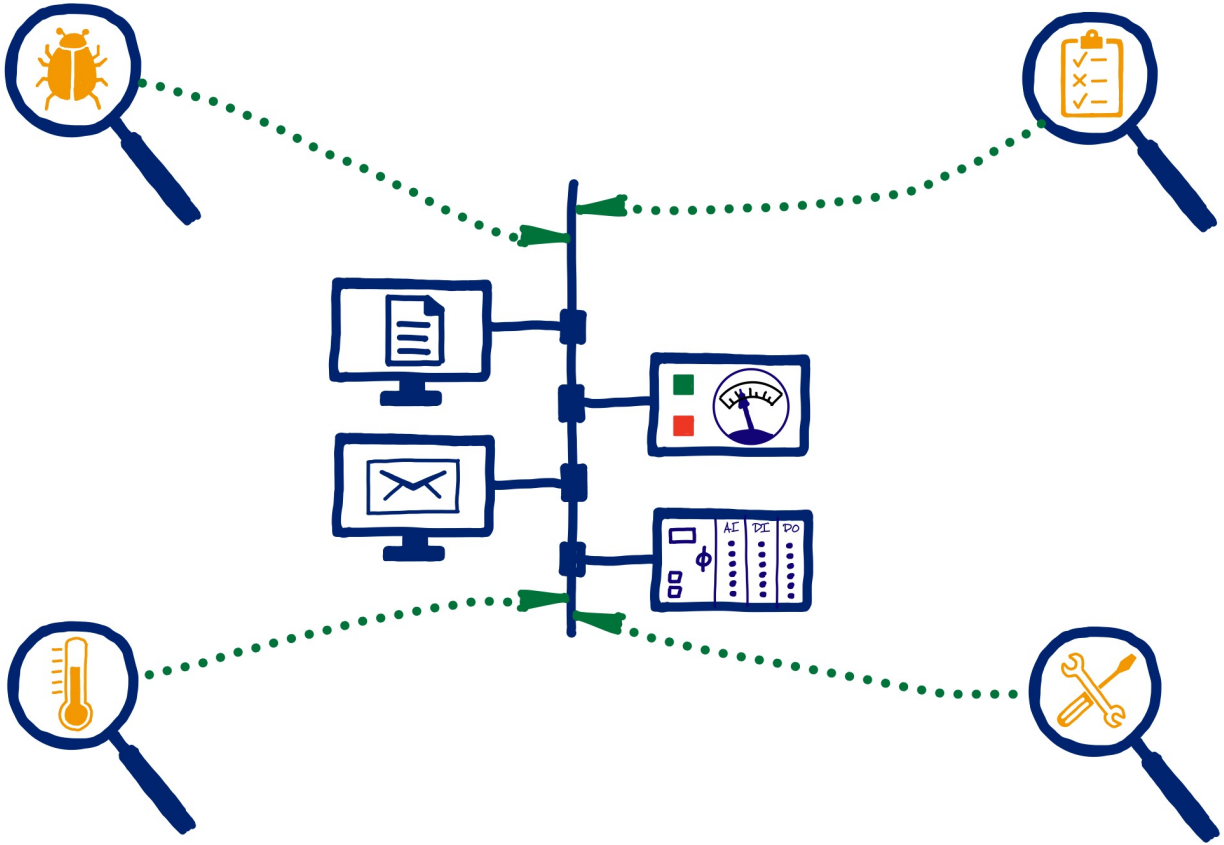
OT Malware


Havex
2013
Industroyer
2016
Industroyer2
2022 April
2010
Stuxnet
2014
BlackEnergy
2017
Triton/Trisys
Incontroller/
Pipedream
2022 April

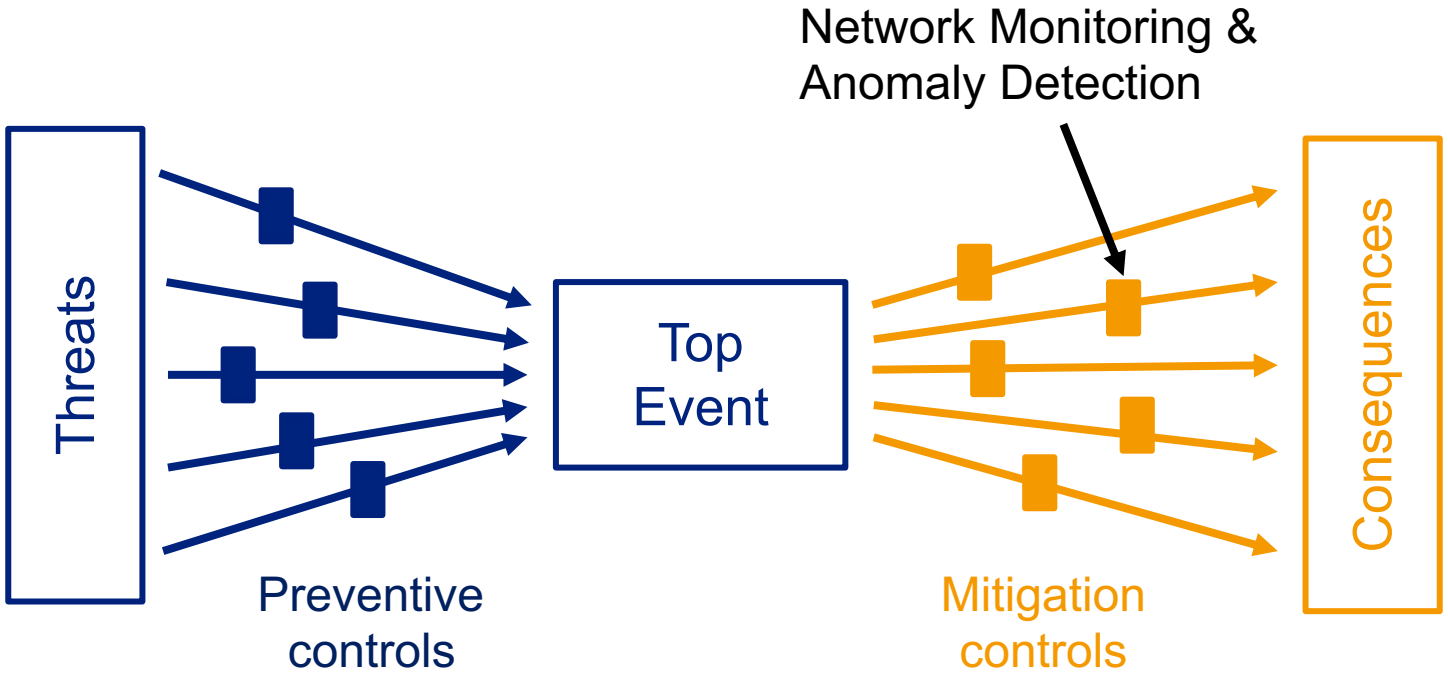


Industrial Network Security Monitoring

Why?



Engineering bow-tie



Source: #S4x20, Shiny Object Syndrome, Rebekah Mohr

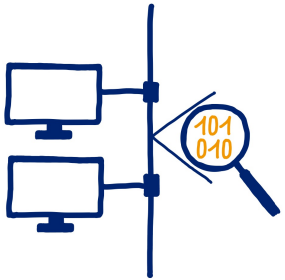
Commercial Products

- 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
Malcolm	no	zeek script	-	huge	very complicated
ntop	yes	Lua	+	minimal	easy
Suricata Open Source IDS / IPS /	no	Lua	-	minimal	complicated
SNORT	yes	snort rules	-	minimal	complicated
SOS	no	n/a	+	depends	easy - medium
zeek	PoC available	zeek script	-	minimal	complicated

Toolitis



Where to start

Choose a tool

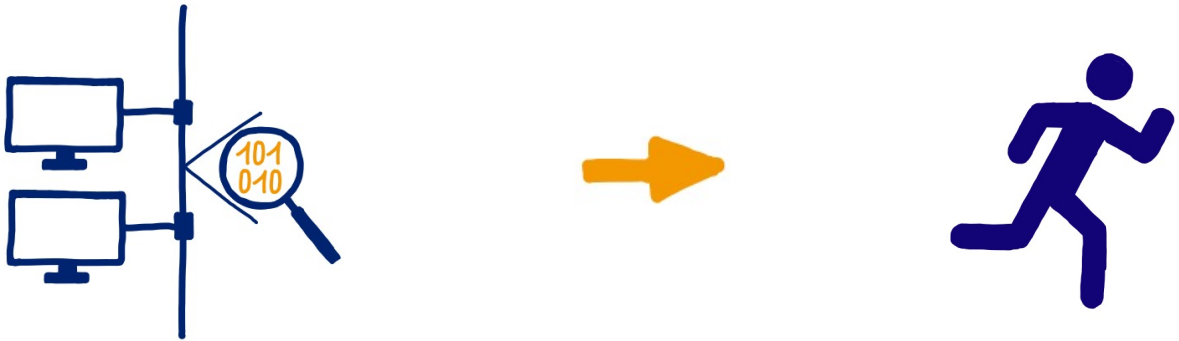
ntopng

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

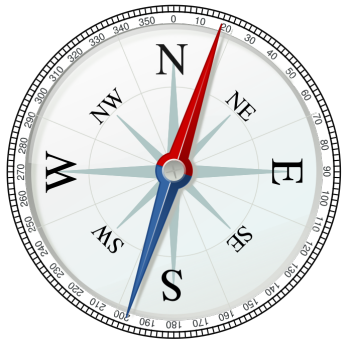
Source: allianz-fuer-cybersicherheit.de

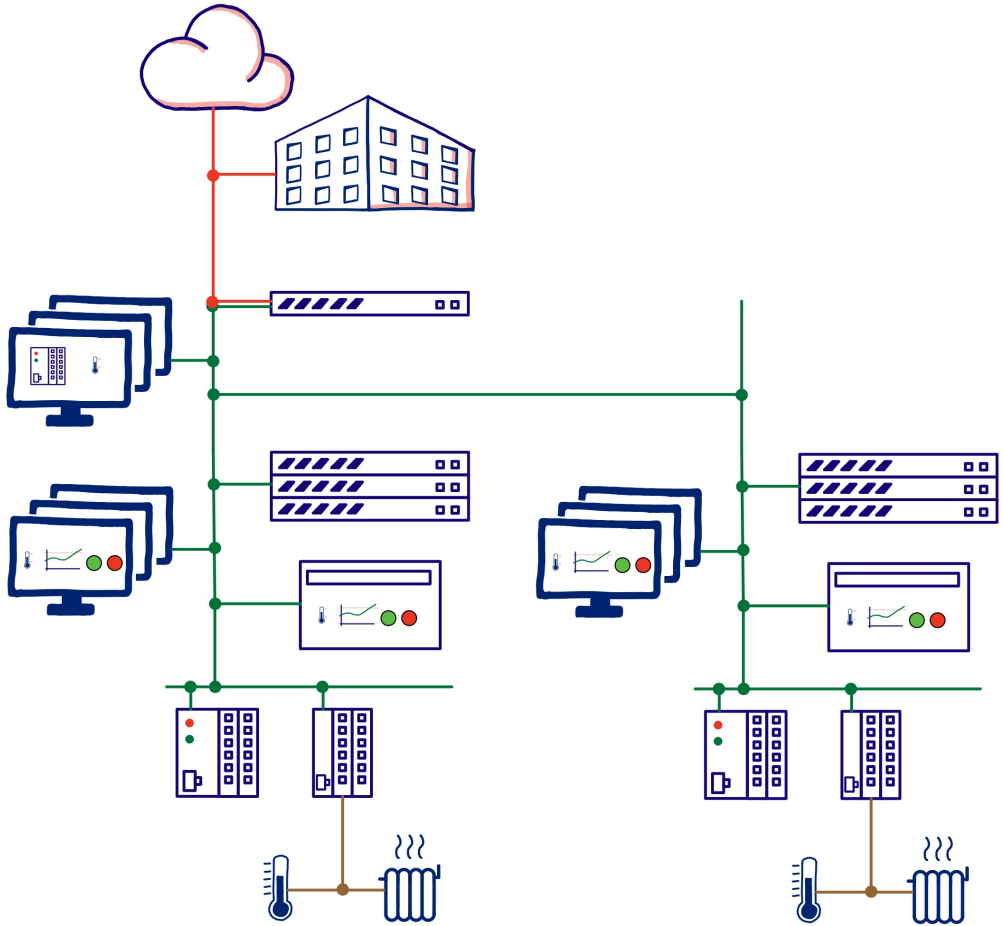
ICS Use Cases

- ❑ 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

Source: allianz-fuer-cybersicherheit.de

Place the Sensor





Source symbol: https://openclipart.org

Best practice

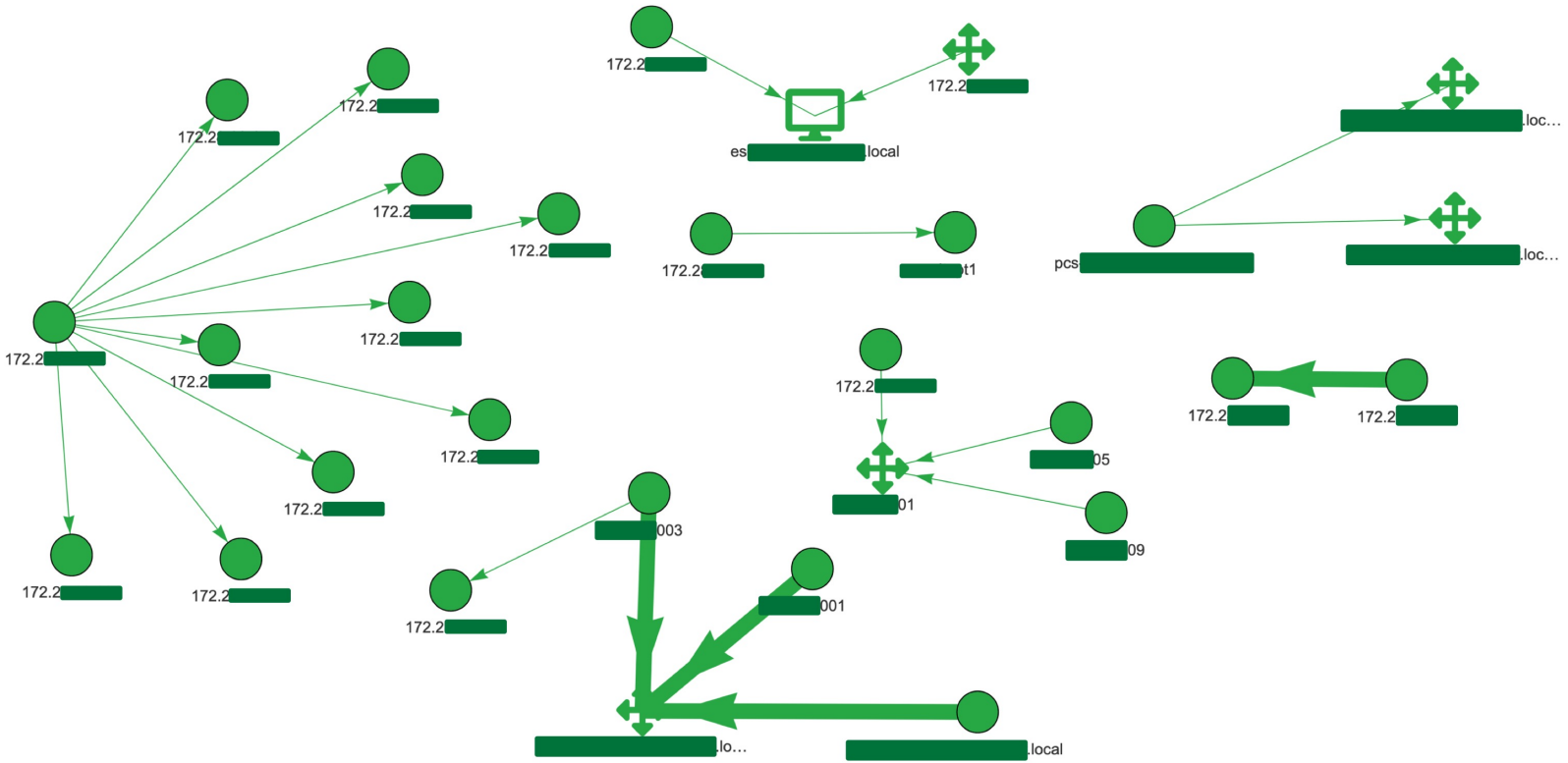
Select Use Cases together with OT Colleagues.

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

Have regular “Monitoring” meetings.

Examples

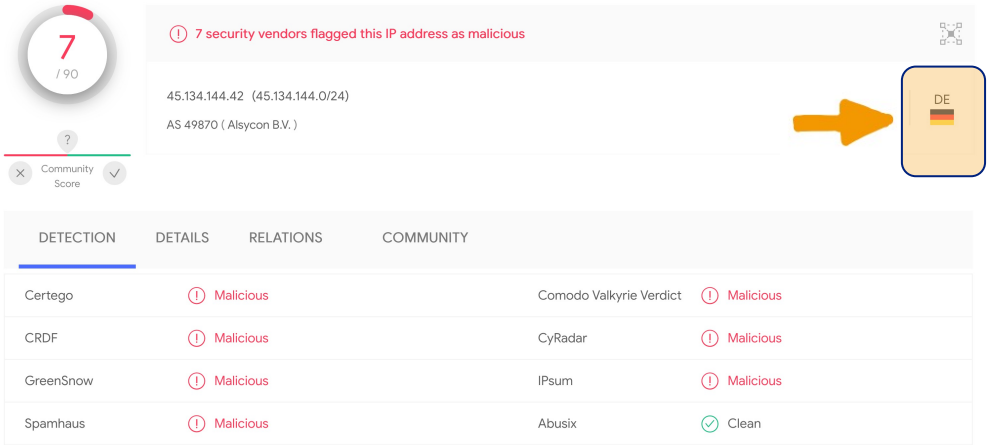
Example I - Remote Support

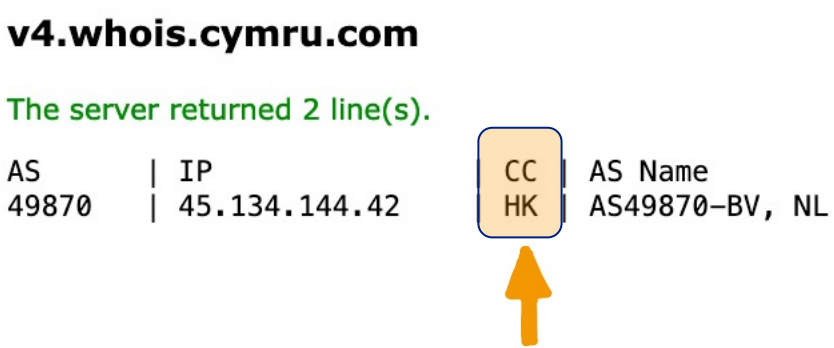


Example II - GEO Fence on Firewalls

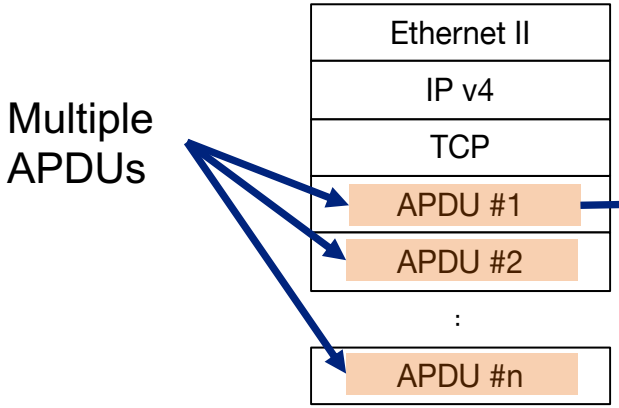
Date/Time	Score	Application	Alert	Flow	Des
09/11/2021 10:13:26	200	TCP:HTTP	Blacklisted Flow	45.134.144.42@3654:44588 [redacted]l...:80	Bla

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

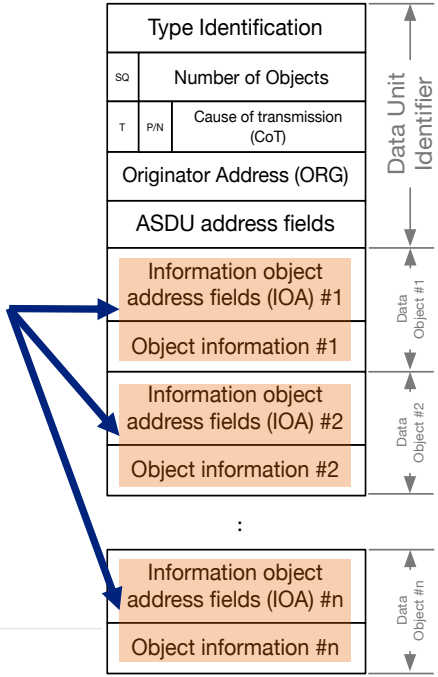




Example III - IEC 60870-5-104



Multiple
IOA's

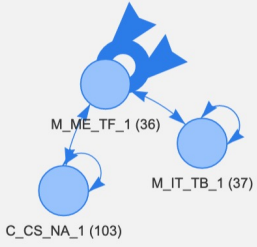


Application	Protocol	VLAN	Client	Server	Actual Thpt	Total Bytes	Info
IEC60870	TCP	21	[redacted]:2404	[redacted]:44404	0 bps	100.48 KB	<- S, RX 21582
IEC60870	TCP	21	[redacted]:2404	[redacted]:59749	0 bps	53.31 KB	-> I, RX 65, TX 28985
IEC60870	TCP	21	[redacted]:58463	[redacted]:2404	0 bps	8.44 KB	<-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

Example III - IEC 60870-5-104

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

Type ID Transitions

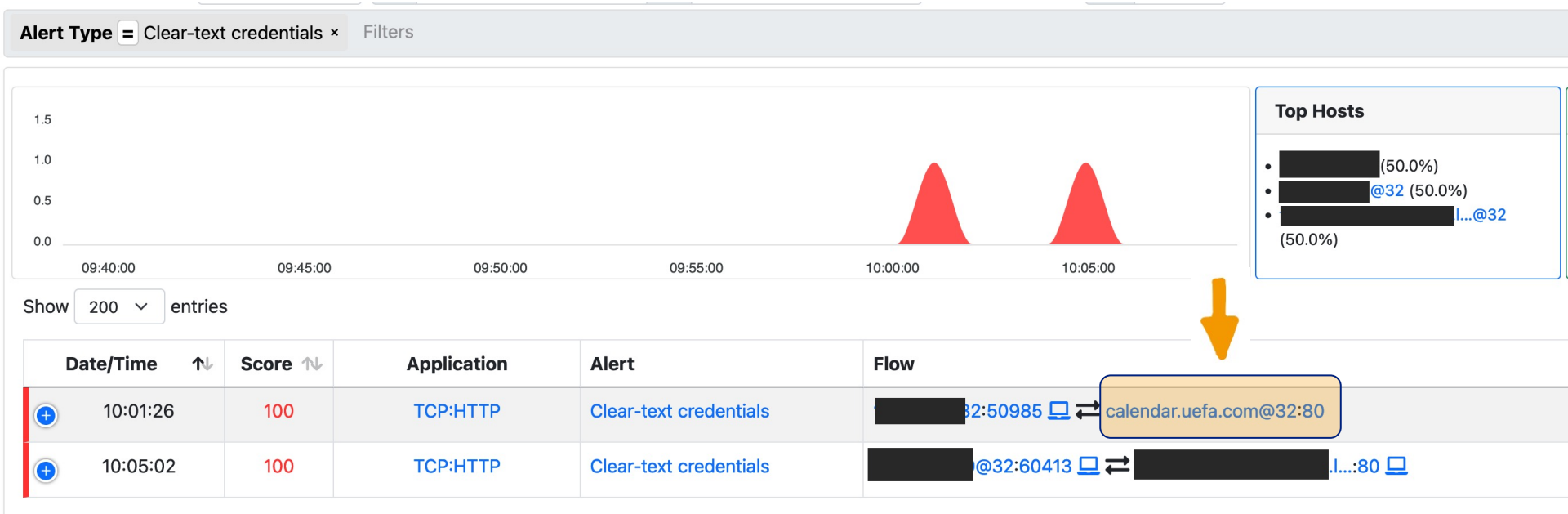


M_ME_TF_1 (36) ⇄ M_ME_TF_1 (36)	98.651 %
M_IT_TB_1 (37) ⇄ M_IT_TB_1 (37)	1.000 %
M_ME_TF_1 (36) → M_IT_TB_1 (37)	0.116 %
M_IT_TB_1 (37) → M_ME_TF_1 (36)	0.116 %
C_CS_NA_1 (103) → M_ME_TF_1 (36)	0.047 %
M_ME_TF_1 (36) → C_CS_NA_1 (103)	0.047 %
C_CS_NA_1 (103) ⇄ C_CS_NA_1 (103)	0.023 %

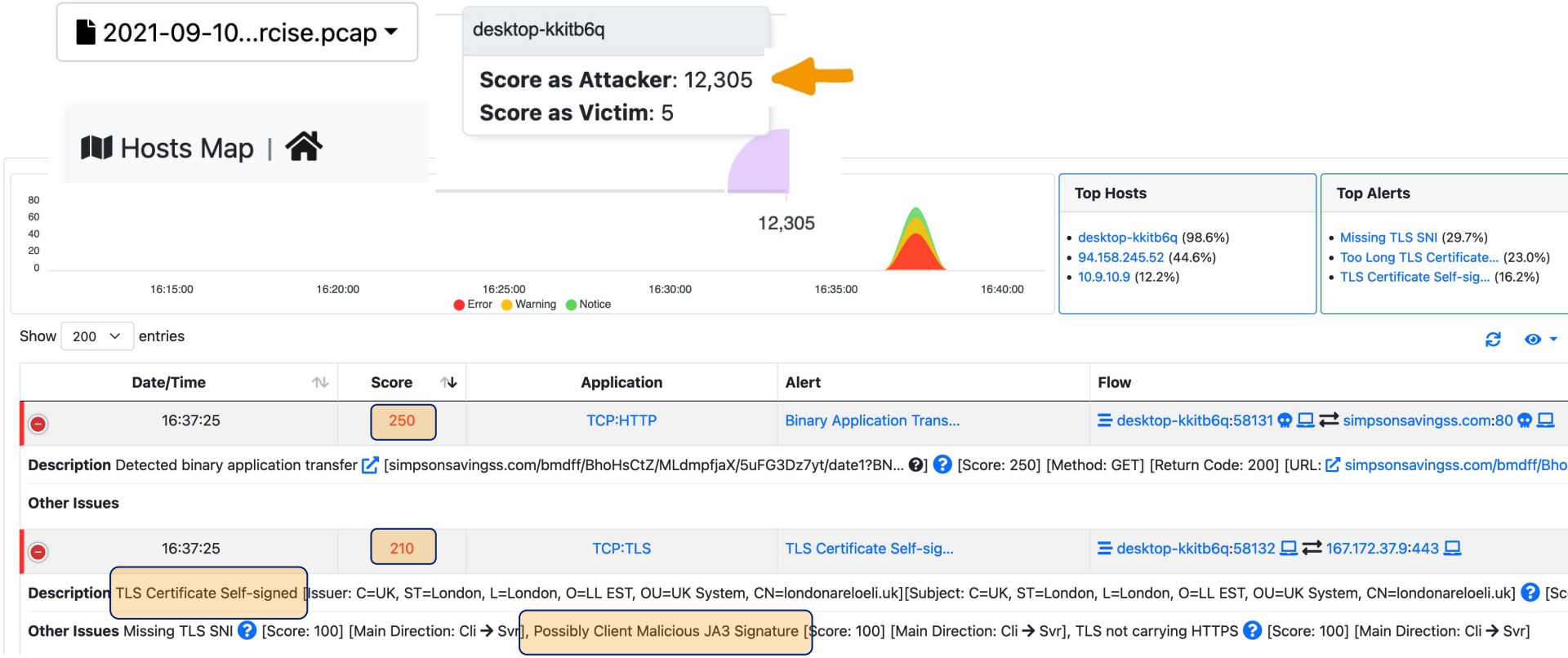
Type I-S Ack Latency (Average / Std Dev)	0.160 ms (0.474 msec)
Messages Breakdown	83.9% / 16.1%
Messages Lost / Retransmissions	← 0, → 18 / 1 Retransmitted

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

Example IV - Clear Text Passwords



Example V - Malware Traffic



Source sample: https://www.malware-traffic-analysis.net/2021/09/10/index.html


LOOKS LIKE LOT OF WORK
imgflip.com

Thank you!

martin.scheu@switch.ch

martin-scheu

@martin_scheu