

A dark blue banner with a network diagram overlay. The diagram consists of white nodes connected by thin white lines, forming a complex web. In the background, there are blurred images of server racks with glowing lights in green, yellow, and red.

Network Security Monitoring

Martin Scheu

26. Februar 2022

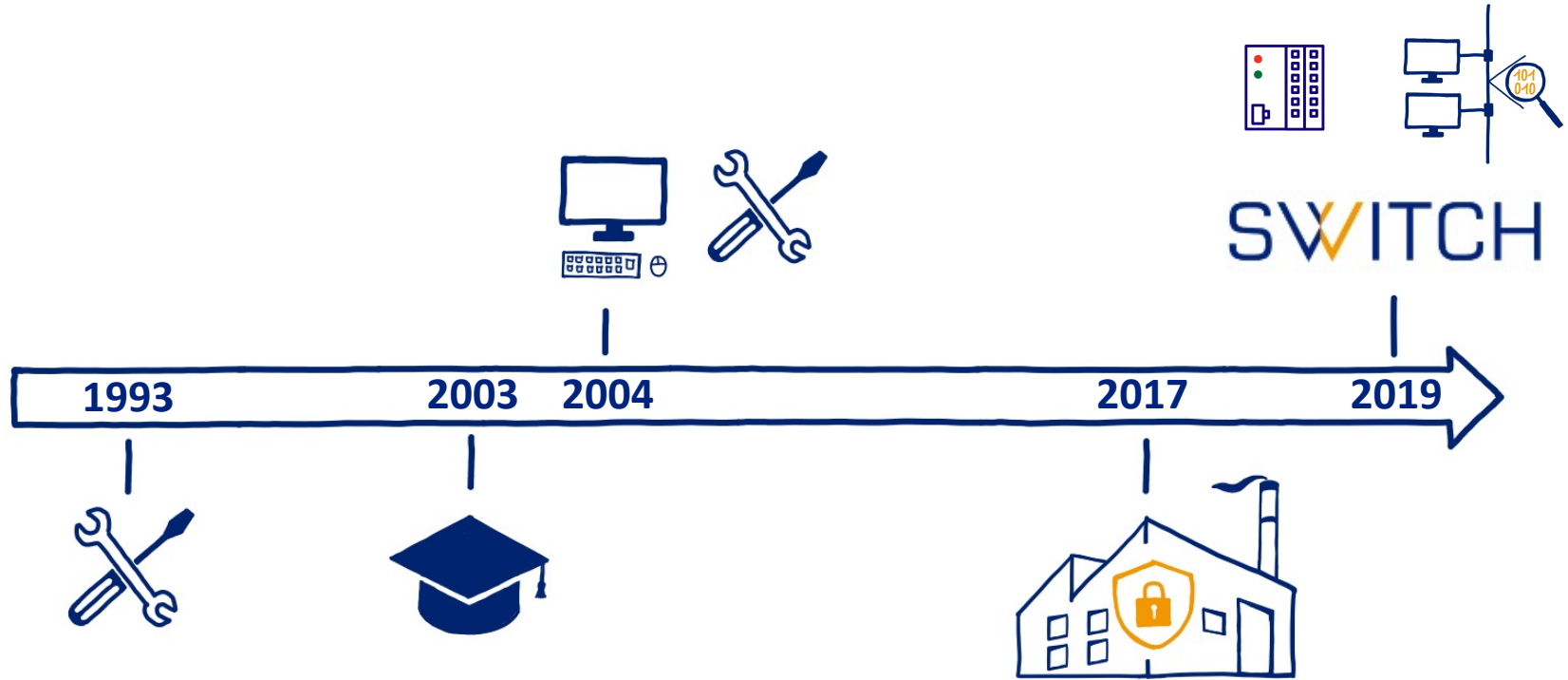
Agenda

Kommunikation und Pakete

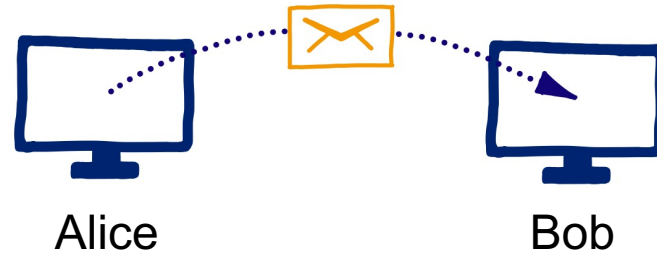
Umsetzung

Beispiele / Demo

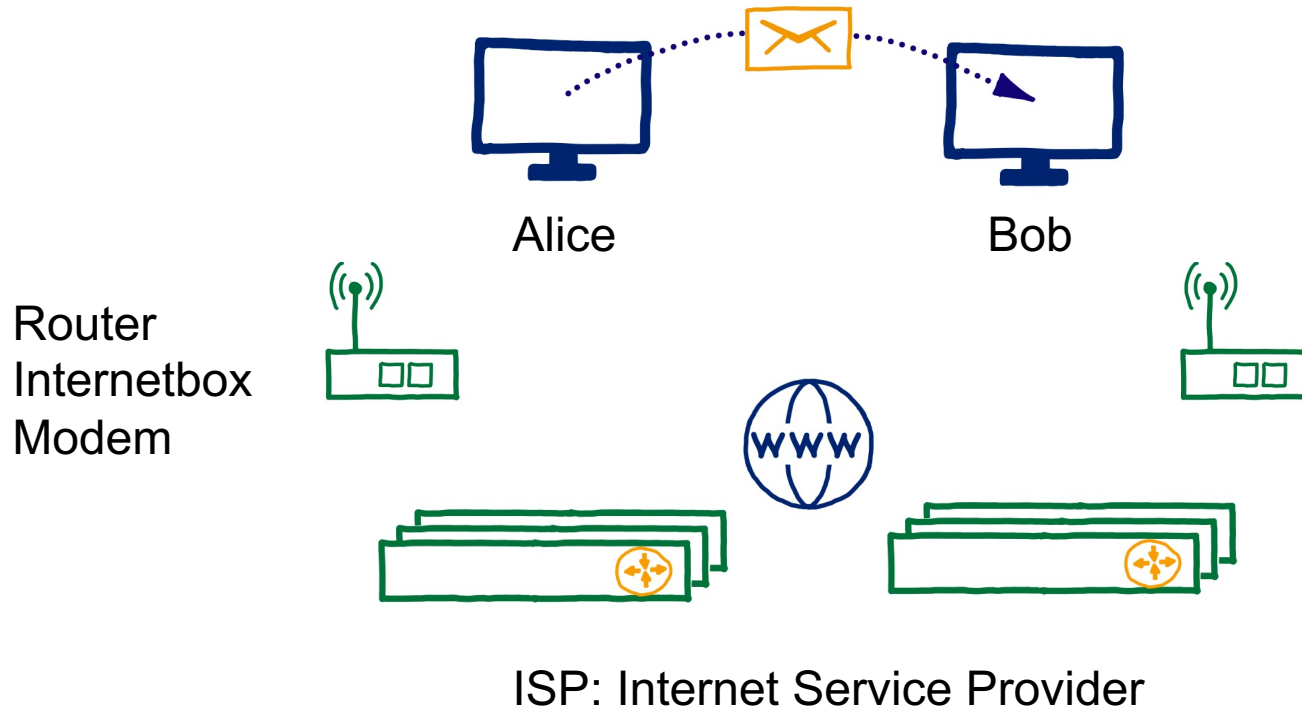
#whoami



Kommunikation



Kommunikation



Kommunikation

Geräteadressierung

MAC Adresse : 00-80-41-ae-fd-7e

Hersteller:

00-80-41

<https://maclookup.app/>

IP Adresse :

v4 192.168.1.1

Dienste rund ums
Netzwerk

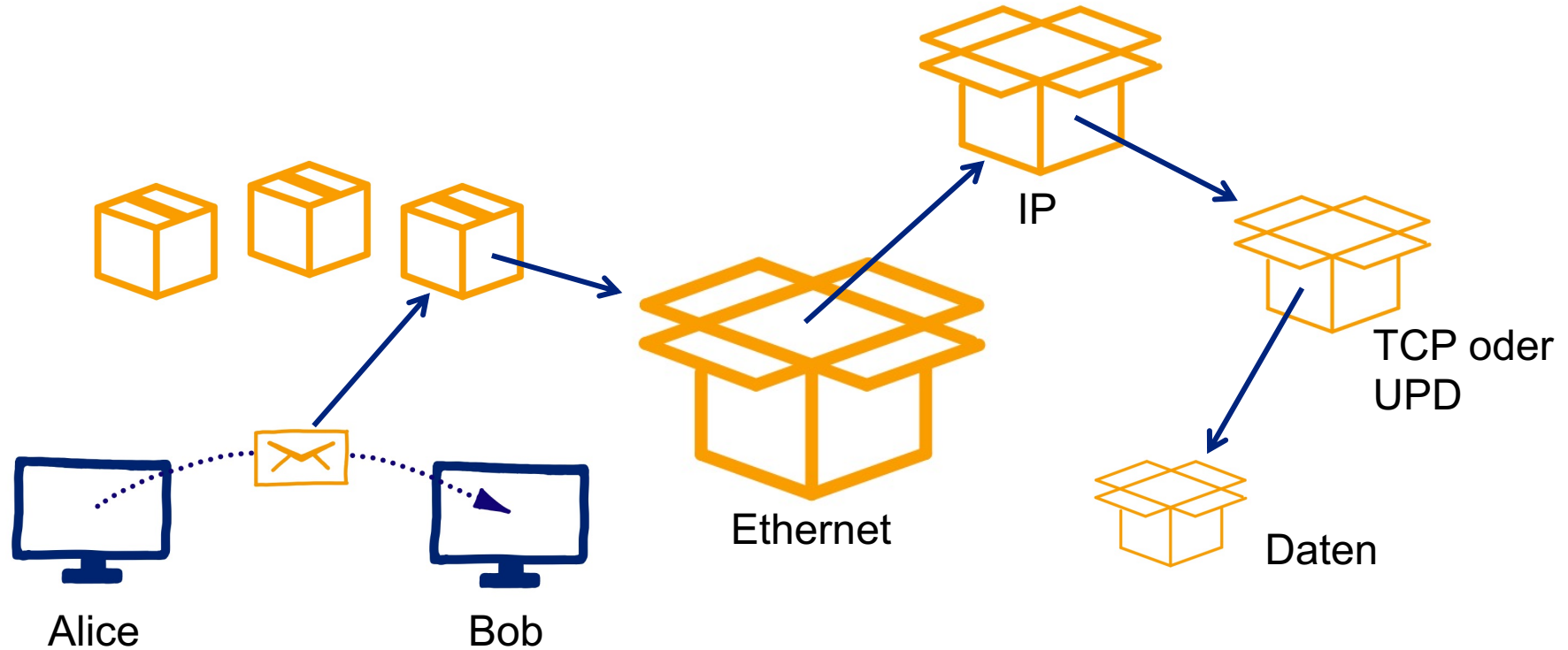
v6 fe80::1ff:fe23:4567:890a

DNS :

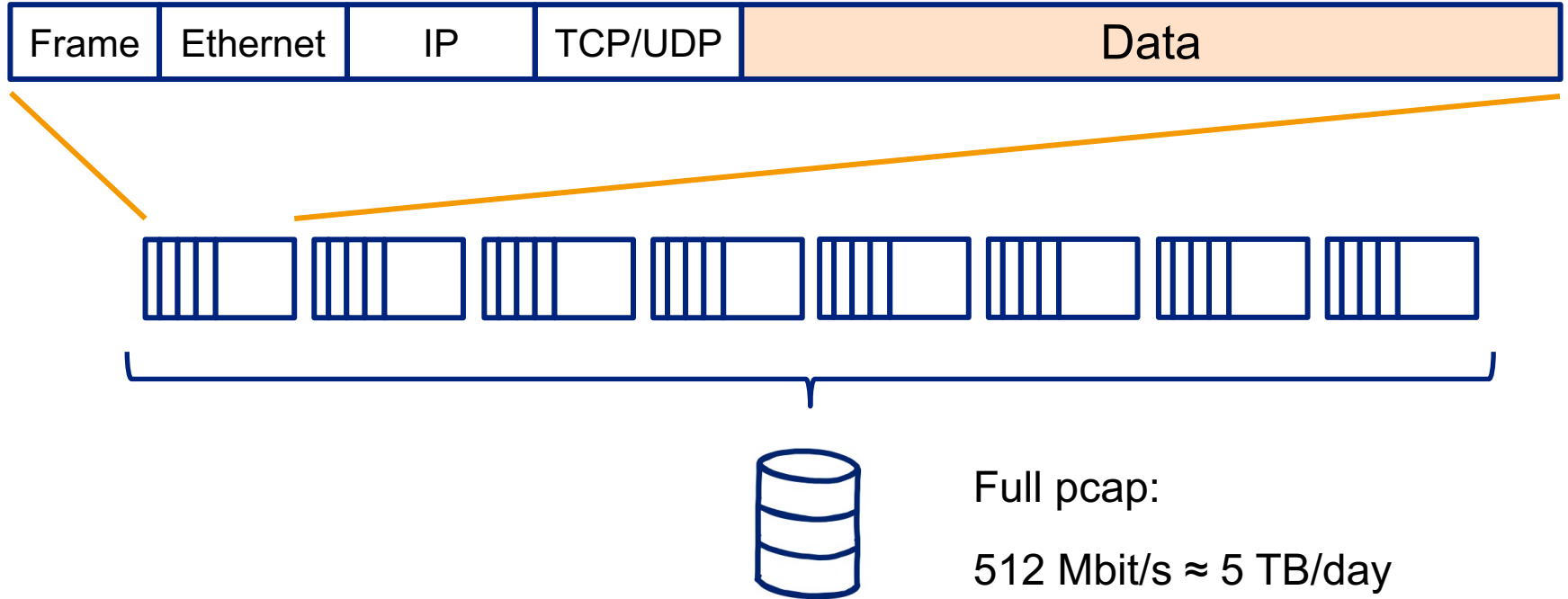
digiges.ch

DHCP, NTP, HTTP(S), SMB, SMTP, ...

Pakete - OSI Modell



Pakete aufzeichnen - full pcap



Pakete aufzeichnen - Flow

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

Src = Source / Ursprung

Dst = Destination / Ziel

Proto = Protokoll

Wireshark

The screenshot displays the Wireshark interface with a network capture of an Apple login process. The packet list pane shows a series of DNS queries and responses, followed by an application data packet (frame 13) which is an Apple login request. The packet details pane shows the structure of the TCP segment, including sequence numbers, acknowledgment numbers, and window size. The packet bytes pane shows the raw hex and ASCII data of the selected packet.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Flags	Info
3	2022-02-14 22:39:20.841177	192.168.7.51	59710	192.168.7.255	443	NBNS	92	0x010	33700 → 443 [ACK] Seq=117 Win=2048 Len=0 TSval=1591075251 TSecr=...
4	2022-02-14 22:39:21.965025	192.168.7.102	137	192.168.7.255	137	NBNS	92		Name query NB RASPBERRYPI<00>
4	2022-02-14 22:39:21.965051	192.168.7.102	5353	224.0.0.251	5353	MDNS	77		Standard query 0x0000 A raspberrypi.local, "QM" question
5	2022-02-14 22:39:21.965191	fe80::a952:7d...	5353	ff02::fb	5353	MDNS	97		Standard query 0x0000 A raspberrypi.local, "QM" question
6	2022-02-14 22:39:21.966155	192.168.7.102	5353	224.0.0.251	5353	MDNS	77		Standard query 0x0000 A raspberrypi.local, "QM" question
7	2022-02-14 22:39:21.966159	fe80::a952:7d...	5353	ff02::fb	5353	MDNS	97		Standard query 0x0000 A raspberrypi.local, "QM" question
8	2022-02-14 22:39:21.966538	192.168.7.42	5353	224.0.0.251	5353	MDNS	88		Standard query response 0x0000 A, cache flush 192.168.7.42
9	2022-02-14 22:39:21.966978	192.168.7.42	5353	224.0.0.251	5353	MDNS	88		Standard query response 0x0000 A, cache flush 192.168.7.42
10	2022-02-14 22:39:22.142485	192.168.7.51	59711	85.235.88.41	443	TLSv1...	897	0x018	Application Data
11	2022-02-14 22:39:22.142685	192.168.7.51	59711	85.235.88.41	443	TLSv1...	891	0x018	Application Data
12	2022-02-14 22:39:22.152617	85.235.88.41	443	192.168.7.51	59711	TCP	66	0x010	443 → 59711 [ACK] Seq=1 Ack=1657 Win=1263 Len=0 TSval=1114916083 TSecr=...
13	2022-02-14 22:39:22.164098	85.235.88.41	443	192.168.7.51	59711	TCP	1514	0x010	443 → 59711 [ACK] Seq=1 Ack=1657 Win=1263 Len=1448 TSval=1114916084 TSecr=...
14	2022-02-14 22:39:22.164172	192.168.7.51	59711	85.235.88.41	443	TCP	66	0x010	59711 → 443 [ACK] Seq=1657 Ack=1449 Win=2025 Len=0 TSval=255389305 TSecr=...

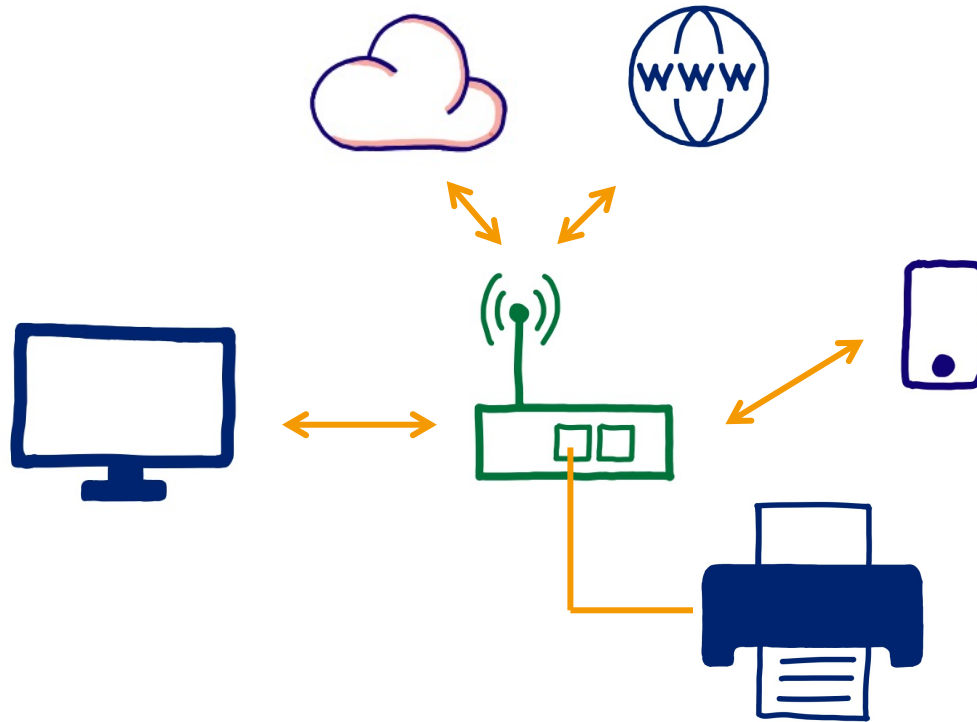
> Frame 13: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0

- Ethernet II, Src: Ubiquiti_45:6c:e3 (fc:ec:da:45:6c:e3), Dst: Apple_5f:82:d7 (a4:83:e7:5f:82:d7)
- Internet Protocol Version 4, Src: 85.235.88.41, Dst: 192.168.7.51
- Transmission Control Protocol, Src Port: 443, Dst Port: 59711, Seq: 1, Ack: 1657, Len: 1448
 - Source Port: 443
 - Destination Port: 59711
 - [Stream index: 1]
 - [Conversation completeness: Incomplete (12)]
 - [TCP Segment Len: 1448]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 2838588298
 - [Next Sequence Number: 1449 (relative sequence number)]
 - Acknowledgment Number: 1657 (relative ack number)
 - Acknowledgment number (raw): 4015802024
 - 1000 ... = Header Length: 32 bytes (8)
 - Flags: 0x010 (ACK)
 - Window: 1263
 - [Calculated window size: 1263]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0x406a [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [Timestamps]
 - [SEQ/ACK analysis]
 - TCP payload (1440 bytes)
 - [Reassembled PDU in frame: 15]
 - TCP segment data (1448 bytes)
- ntop
 - Application Latency RTT (msec): 21.6131

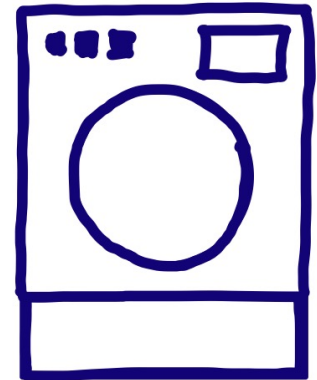
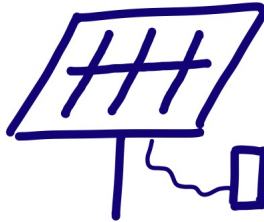
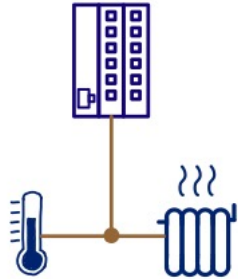
0000 b4 83 e7 5f 82 d7 fc ec da 45 6c e3 08 00 45 00E...E

Frame (frame), 1514 bytes Selected Packet: 13 - Packets: 1695 - Displayed: 1695 (100.0%) Profile: Default

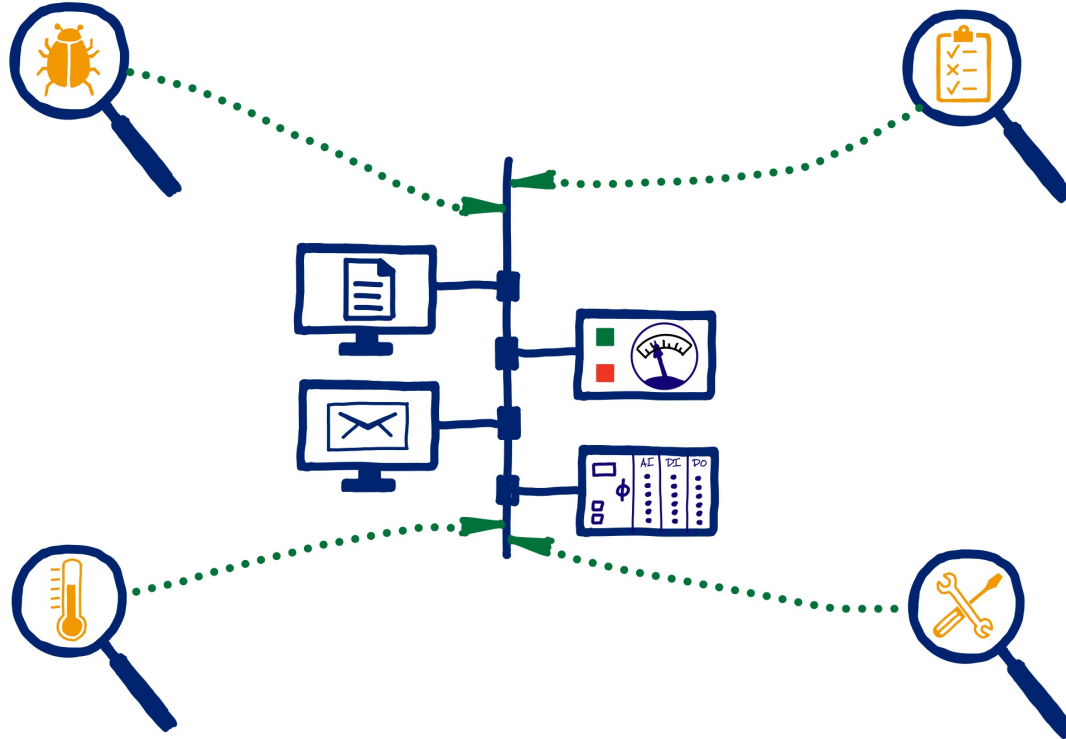
Geräte im Netzwerk



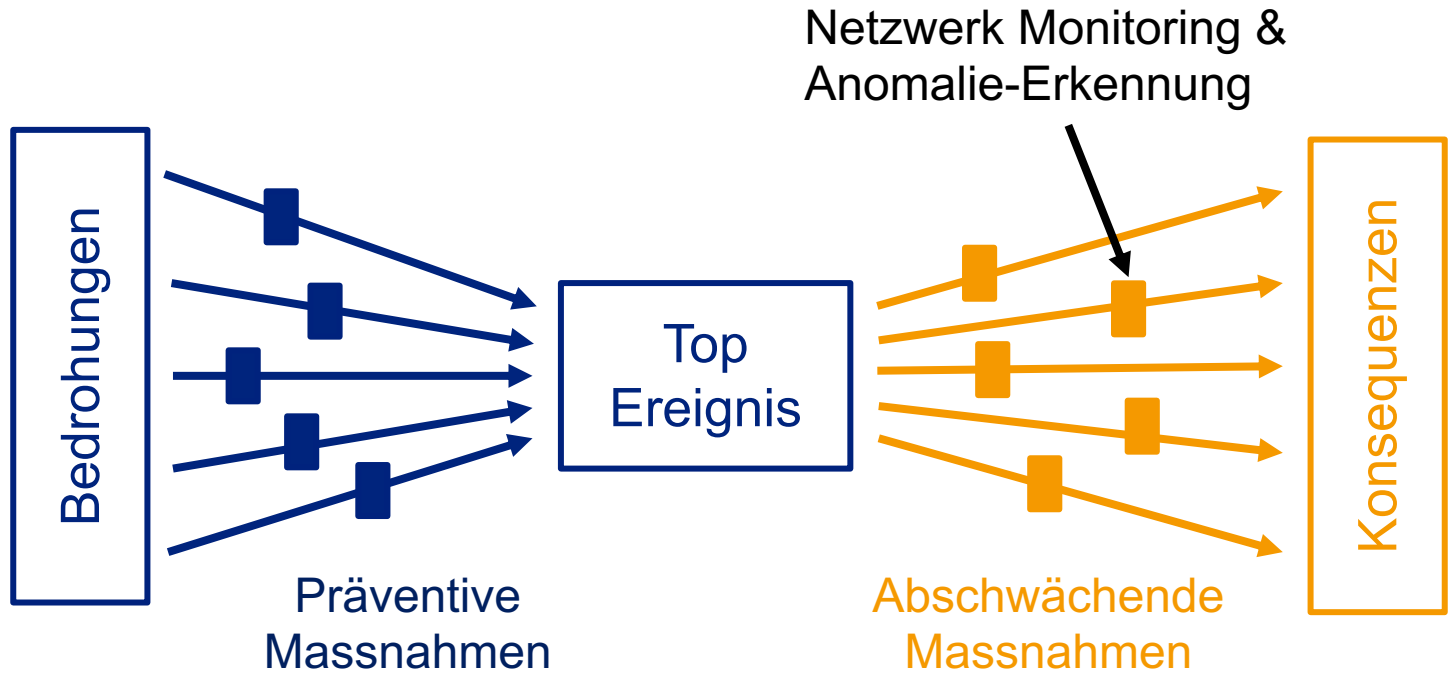
Geräte im Netzwerk



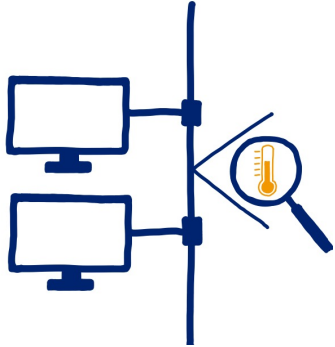
Netzwerk Security Monitoring



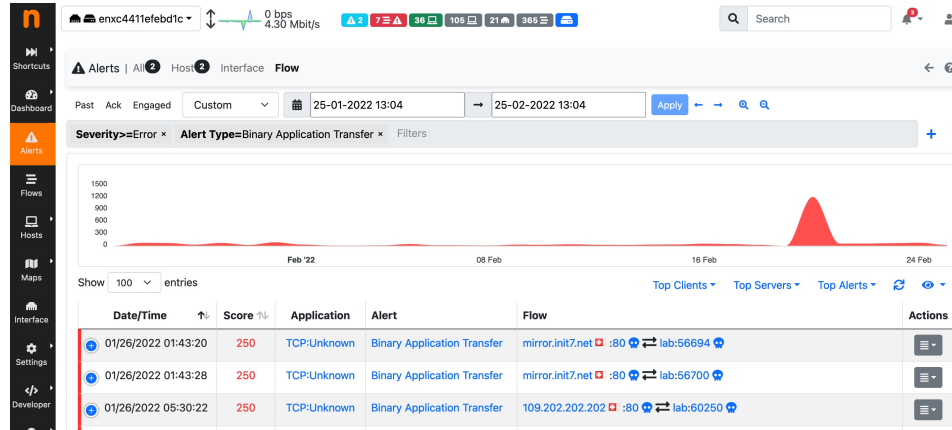
Ingenieurs -



Netzwerk Security Monitoring



Sensor









Anzeige und Administration
über Webbrowser

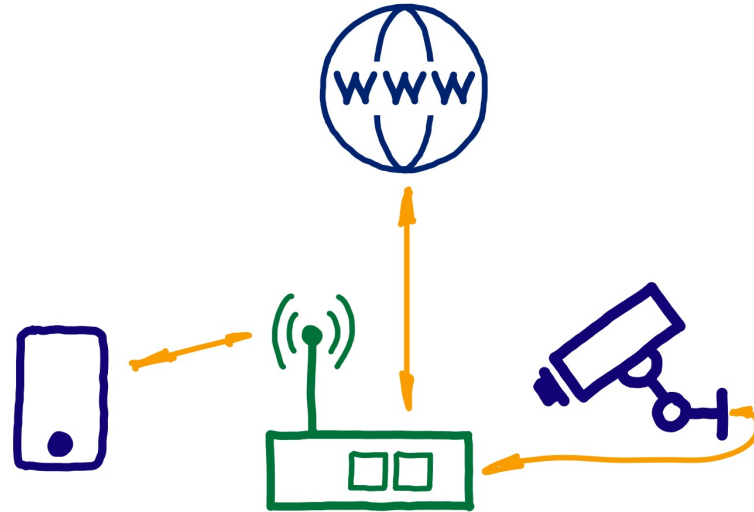
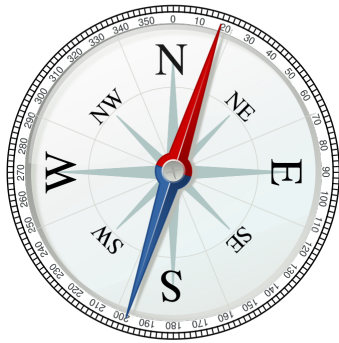


Alarmierung

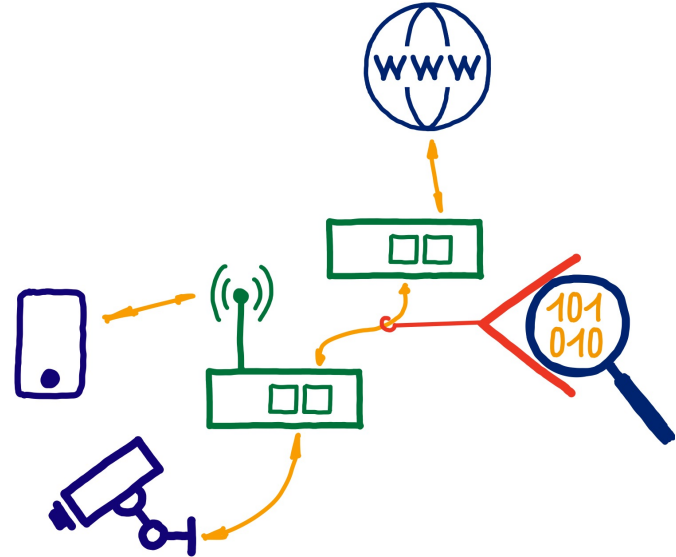
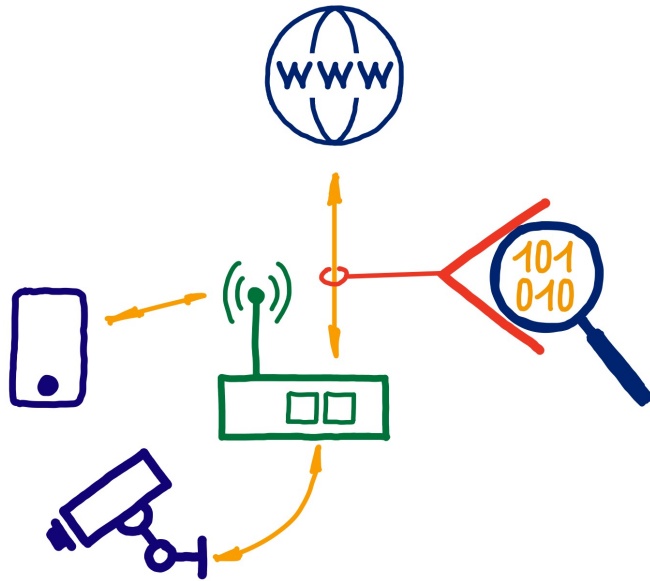
Open-source Netzwerk Security Monitoring

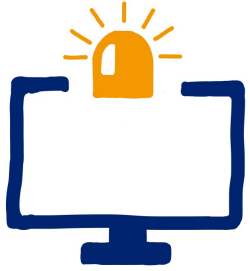
	Com- munity	Benutzer- freundlich	Resourcen Anforderung	Installation und Einrichten
	klein	nein	gross	kompliziert
	klein	ja	klein	einfach
	gross	nein	klein	kompliziert
	gross	nein	klein	kompliziert
	mittel	ja	mittel - viel	einfach - mittel
	gross	nein	klein	kompliziert

Sensor platzieren



Sensor platzieren





Beispiele / Demo

Beispiel I - komische Verbindung

→ 101-100-146-146.myrepublic.co.nz:

Flow	Protocol ↕	Application ↕	Score ↕	Pkts ↕	Bytes ↕	Thpt ↕	Begin ↕	End ↕
101-100-146-146.myrepublic.co.nz:123 ↔ valdivia.mscheu.ch:123	UDP	NTP	10	2 Pkts	110 Bytes	880 bit/s	12/29/21 23:13:08	12/29/21 23:13:08

Application ↕	Score ↕	Pkts ↕	Bytes ↕
NTP	10	2 Pkts	110 Bytes

Synchronize with NTP server

Server address:

pool.ntp.org

Update Now

Beispiel II - Klartext Passwörter

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

Beispiel III - GEO Fence in 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 (Alsycon 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 IV - Schadsoftware

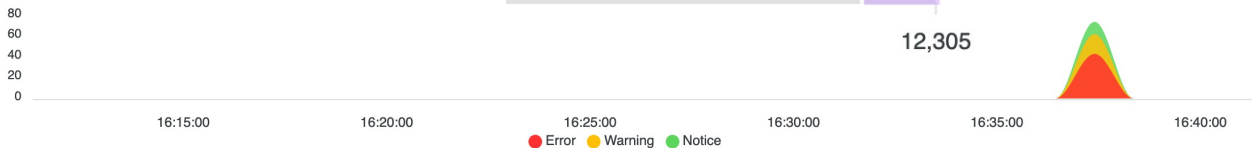
2021-09-10...rcise.pcap ▾

desktop-kkitb6q

Score as Attacker: 12,305

Score as Victim: 5

Hosts Map | 🏠



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 → simpsonsavings.com:80
Description Detected binary application transfer [simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjX/5uFG3Dz7yt/date1?BN... [Score: 250] [Method: GET] [Return Code: 200] [URL: simpsonsavings.com/bmdff/Bho...]				
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]				

Demo


Werkzeuge

 **BRIM** Desktop pcap Analyse

<https://www.brimdata.io/download/>

Pcaps mit Schadsoftware,
Anleitungen und Tutorials

<https://malware-traffic-analysis.net/>

 NetworkMiner, Desktop pcap Analyse

<https://www.netresec.com/?page=NetworkMiner>

TraceWrangler - Packet Capture Toolkit

<https://www.tracewrangler.com/>

 **WIRESHARK**

Pcap aufzeichnen
und analysieren

<https://www.wireshark.org/>

Dankeschön!



martin.scheu@switch.ch



[martin-scheu](https://www.linkedin.com/in/martin-scheu)



[@martin_scheu](https://twitter.com/martin_scheu)