Industrial Security in der Praxis

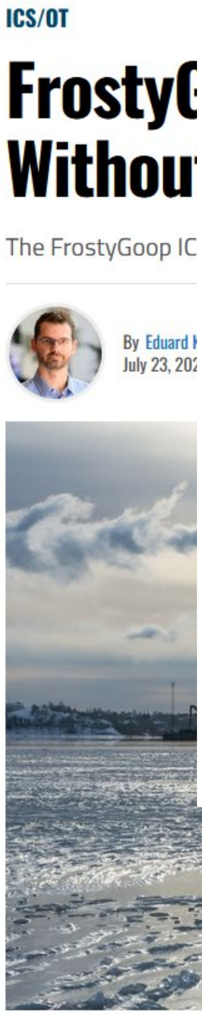
First steps, IDS & Honeypots

managed.defense

IT vs. OT

LED
INFORMATION TECHNOLOGY
PCB
PGC
NETWORK
RGB
RGB
ACHTUNG!
MACHINE IN
KECHOT!

Possible impact

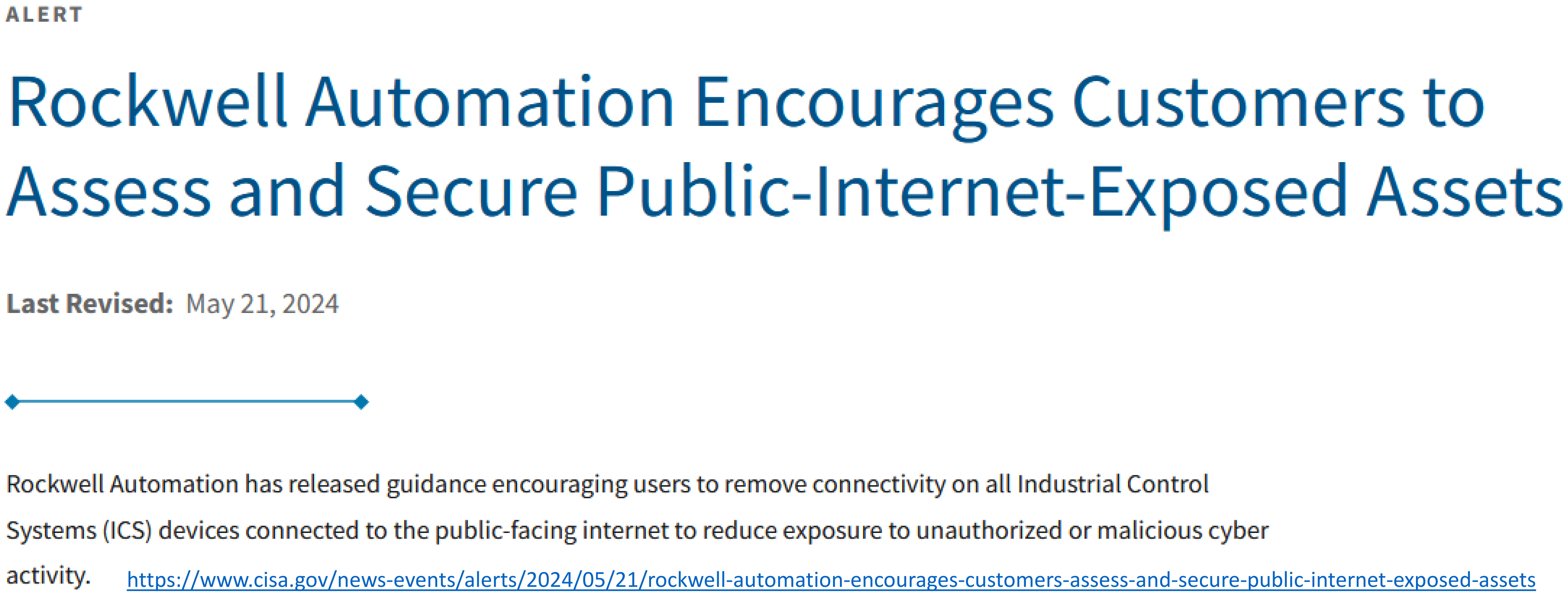


ICS/OT

FrostyG
Withou

The FrostyGoop IC

By Eduard K
July 23, 202



ALERT

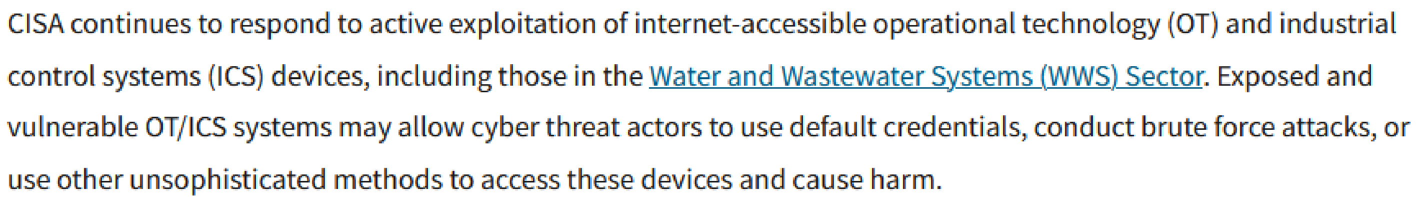
Rockwell Automation Encourages Customers to Assess and Secure Public-Internet-Exposed Assets

Last Revised: May 21, 2024

Rockwell Automation has released guidance encouraging users to remove connectivity on all Industrial Control Systems (ICS) devices connected to the public-facing internet to reduce exposure to unauthorized or malicious cyber activity.

https://www.cisa.gov/news-events/alerts/2024/05/21/rockwell-automation-encourages-customers-assess-and-secure-public-internet-exposed-assets

https://www.securityweek.com/frostygoop-ics



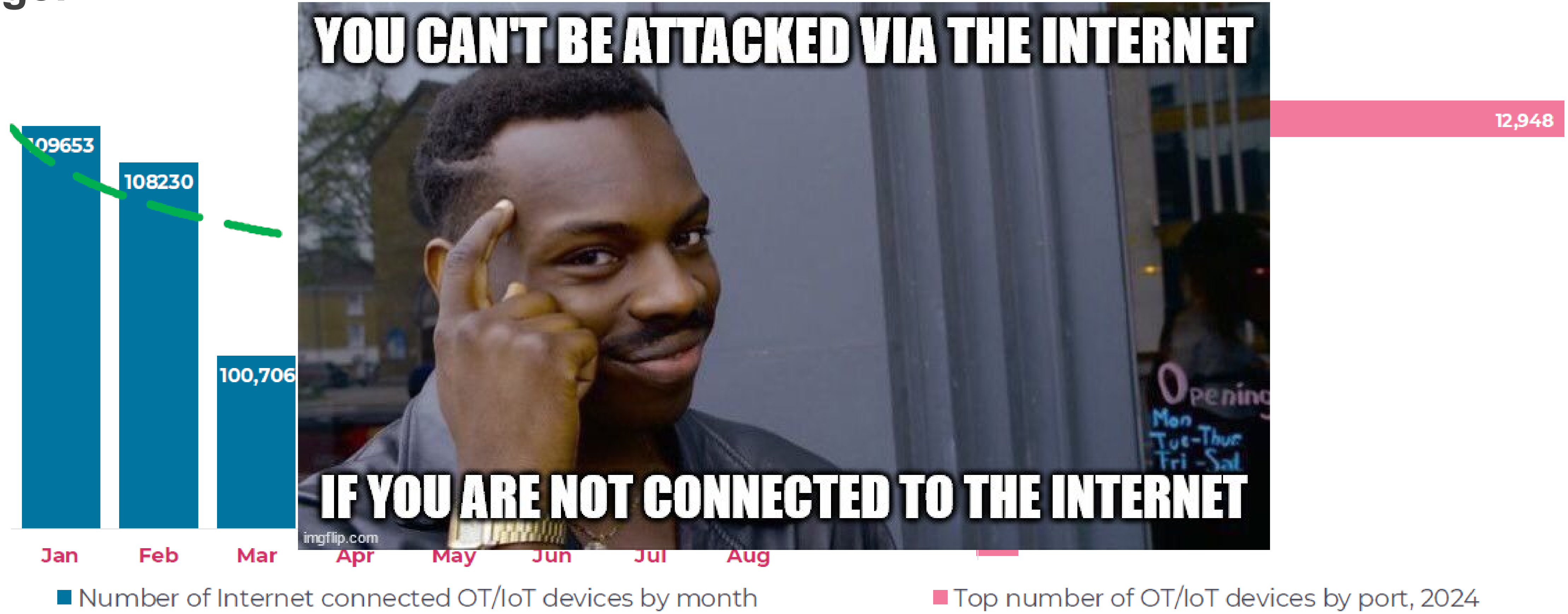
CISA continues to respond to active exploitation of internet-accessible operational technology (OT) and industrial control systems (ICS) devices, including those in the Water and Wastewater Systems (WWS) Sector. Exposed and vulnerable OT/ICS systems may allow cyber threat actors to use default credentials, conduct brute force attacks, or use other unsophisticated methods to access these devices and cause harm.

https://www.cisa.gov/news-events/alerts/2024/09/25/threat-actors-continue-exploit-otics-through-unsophisticated-means

OT Internet Exposure, H1 2024

IKARUS
security software

Lage:



Learn more: https://trends.shodan.io

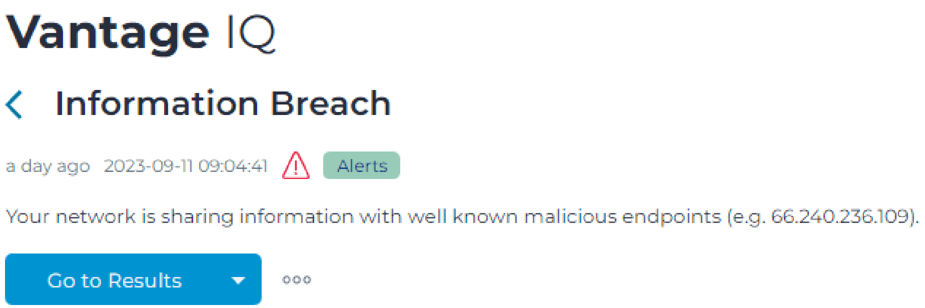
OT (Security) in the wild

1. Zuständigkeiten für OT Security („Darum kümmert sich die IT“).

WANTED
DEAD OR ALIVE
Shopfloor (OT) Security Officer (m/w/d)
OT-Security Engineer m/w/d
REWARD
165974813

OT (Security) in the wild

2. Port Forwarding zu internen Netzen.

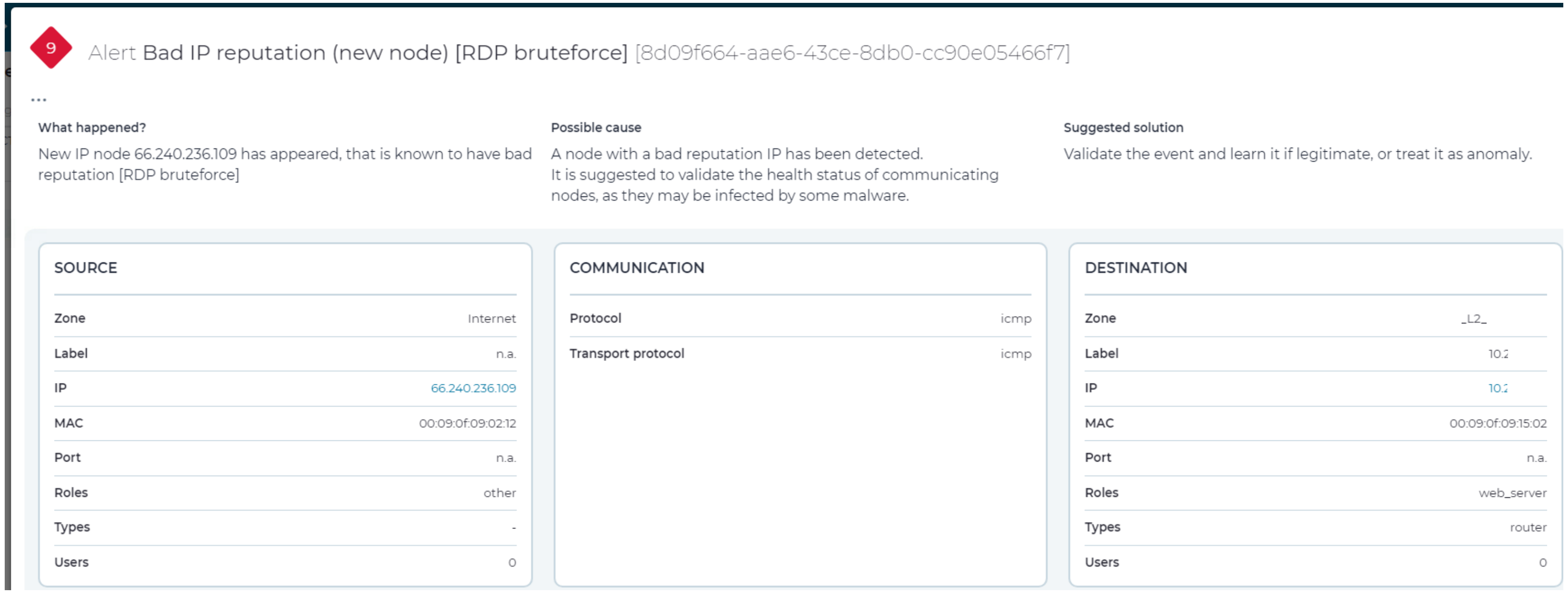


Vantage IQ

Information Breach

a day ago 2023-09-11 09:04:41 ⚠ Alerts

Your network is sharing information with well known malicious endpoints (e.g. 66.240.236.109).



9 Alert Bad IP reputation (new node) [RDP bruteforce] [8d09f664-aae6-43ce-8db0-cc90e05466f7]

What happened?
New IP node 66.240.236.109 has appeared, that is known to have bad reputation [RDP bruteforce]

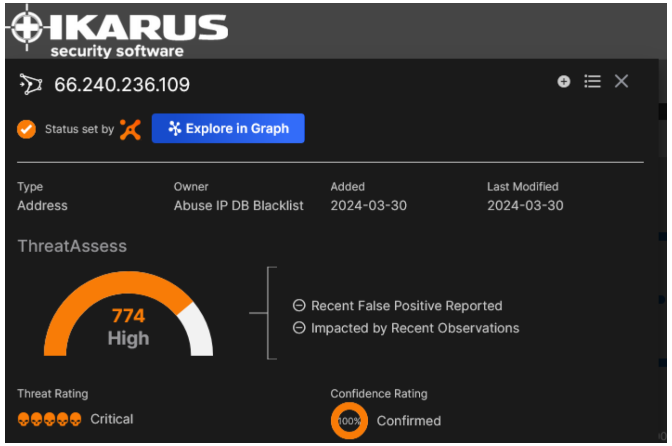
Possible cause
A node with a bad reputation IP has been detected.
It is suggested to validate the health status of communicating nodes, as they may be infected by some malware.

Suggested solution
Validate the event and learn it if legitimate, or treat it as anomaly.

SOURCE	
Zone	Internet
Label	n.a.
IP	66.240.236.109
MAC	00:09:0f:09:02:12
Port	n.a.
Roles	other
Types	-
Users	0

COMMUNICATION	
Protocol	icmp
Transport protocol	icmp

DESTINATION	
Zone	_L2_
Label	10.2
IP	10.2
MAC	00:09:0f:09:15:02
Port	n.a.
Roles	web_server
Types	router
Users	0



IKARUS security software

66.240.236.109

Status set by

Type	Owner	Added	Last Modified
Address	Abuse IP DB Blacklist	2024-03-30	2024-03-30

ThreatAssess

774 High

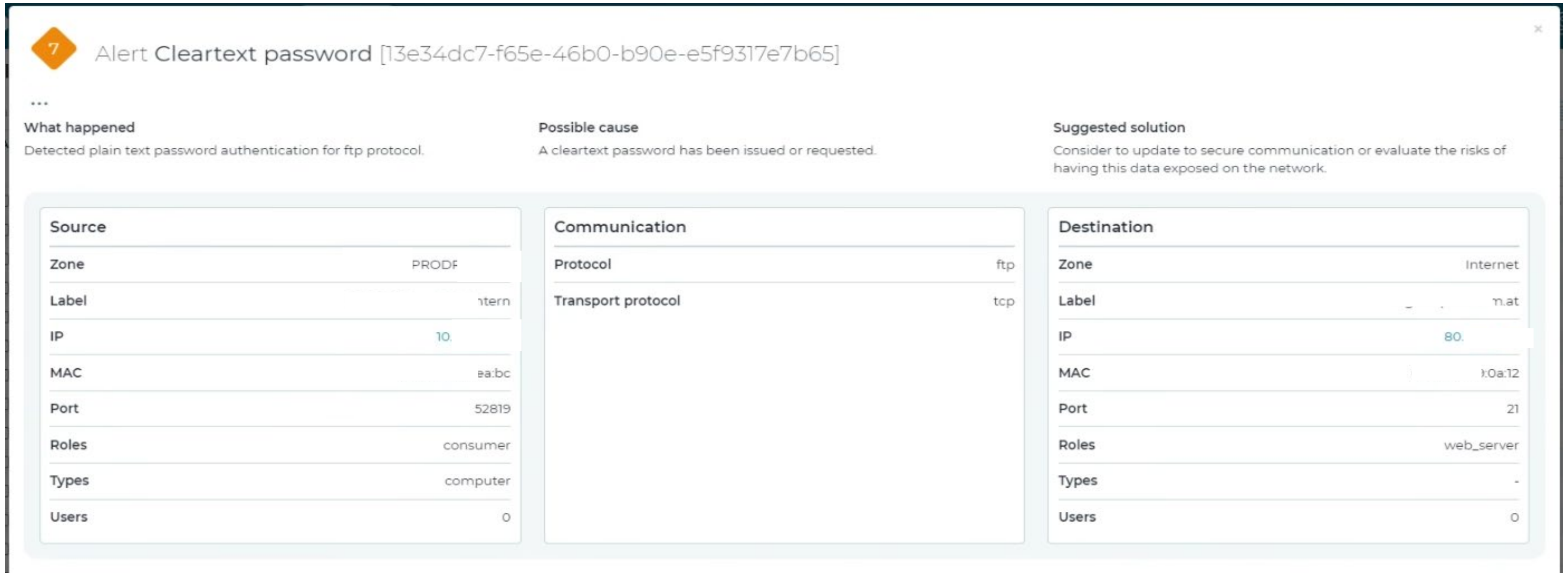
⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating: Critical

Confidence Rating: 100% Confirmed

OT (Security) in the wild

3. Unverschlüsselte Kommunikation (intern/extern) + großteils schwache PWs.



Alert Cleartext password [13e34dc7-f65e-46b0-b90e-e5f9317e7b65]

What happened
Detected plain text password authentication for ftp protocol.

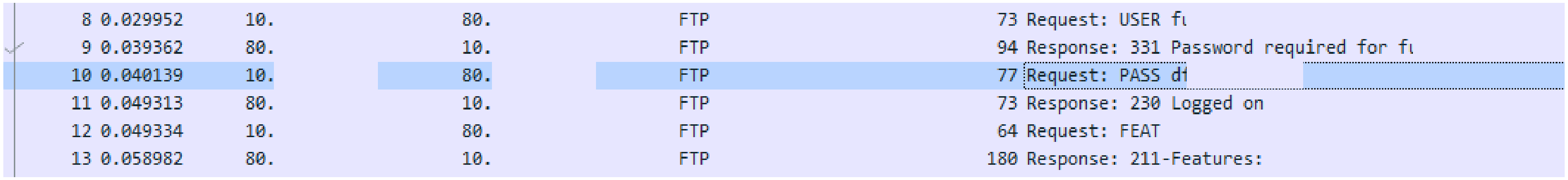
Possible cause
A cleartext password has been issued or requested.

Suggested solution
Consider to update to secure communication or evaluate the risks of having this data exposed on the network.

Source	
Zone	PRODF
Label	ıtern
IP	10.
MAC	ea:bc
Port	52819
Roles	consumer
Types	computer
Users	0

Communication	
Protocol	ftp
Transport protocol	tcp

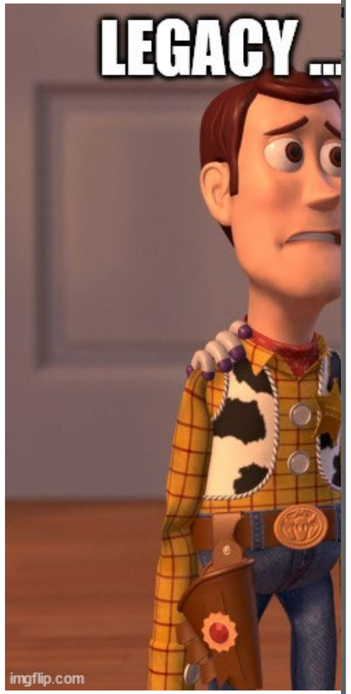
Destination	
Zone	Internet
Label	n.at
IP	80.
MAC	:0a:12
Port	21
Roles	web_server
Types	-
Users	0

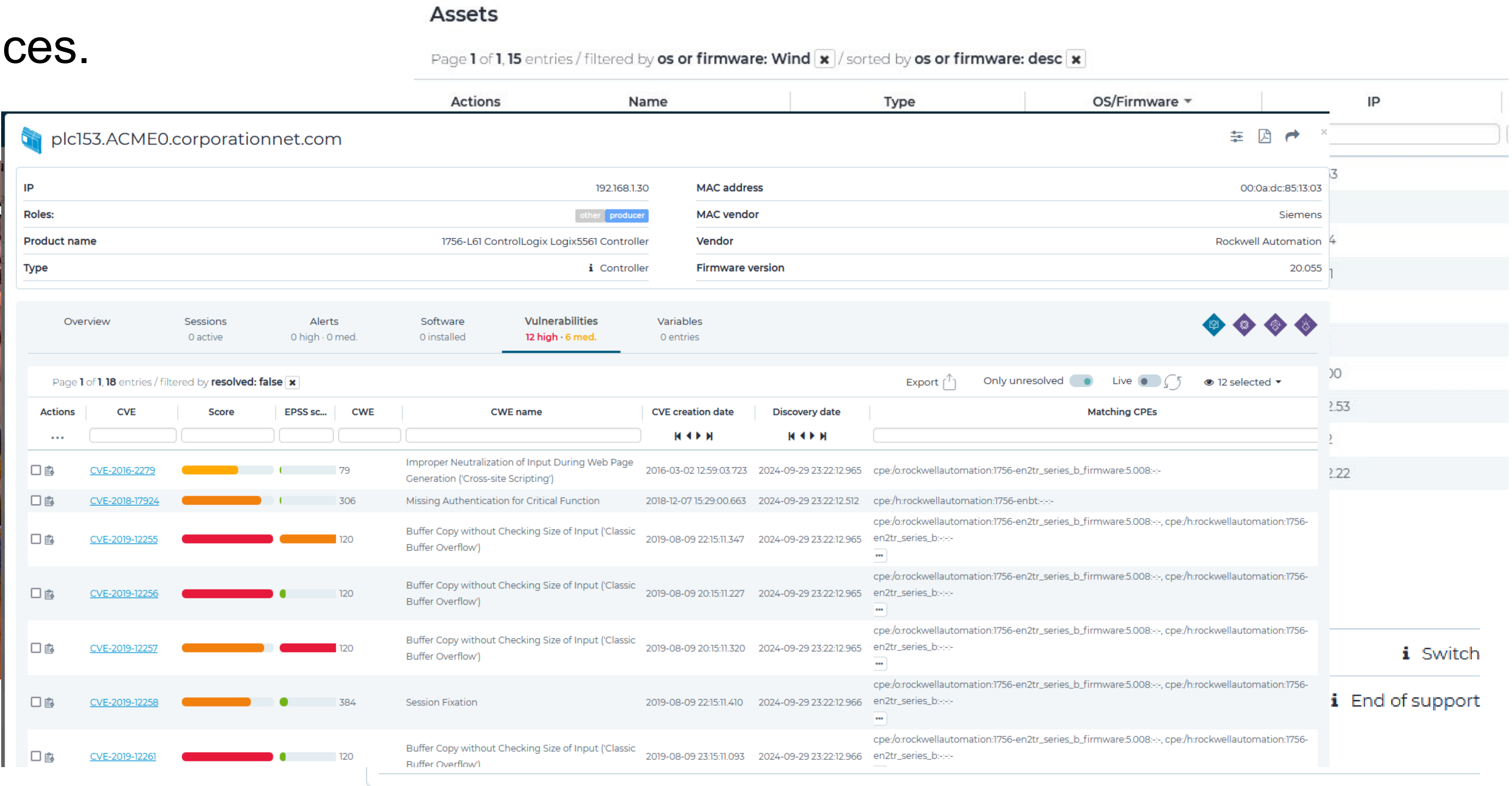


```
 8 0.029952    10.          80.          FTP           73 Request: USER fı
 9 0.039362    80.          10.          FTP           94 Response: 331 Password required for fı
10 0.040139    10.          80.          FTP           77 Request: PASS dı
11 0.049313    80.          10.          FTP           73 Response: 230 Logged on
12 0.049334    10.          80.          FTP           64 Request: FEAT
13 0.058982    80.          10.          FTP          180 Response: 211-Features:
```

OT (Security) in the wild

4. Legacy devices.





Assets

Page 1 of 1, 15 entries / filtered by **os or firmware: Wind** ✖ / sorted by **os or firmware: desc** ✖

Actions	Name	Type	OS/Firmware ▾	IP

ℹ Switch

ℹ End of support

plc153.ACME0.corporationnet.com

IP	192.168.1.30	**MAC address**	00:0a:dc:85:13:03
Roles:	other producer	**MAC vendor**	Siemens
Product name	1756-L61 ControlLogix Logix5561 Controller	**Vendor**	Rockwell Automation
Type	ℹ Controller	**Firmware version**	20.055

Overview	Sessions	Alerts	Software	Vulnerabilities	Variables
	0 active	0 high · 0 med.	0 installed	12 high · 6 med.	0 entries

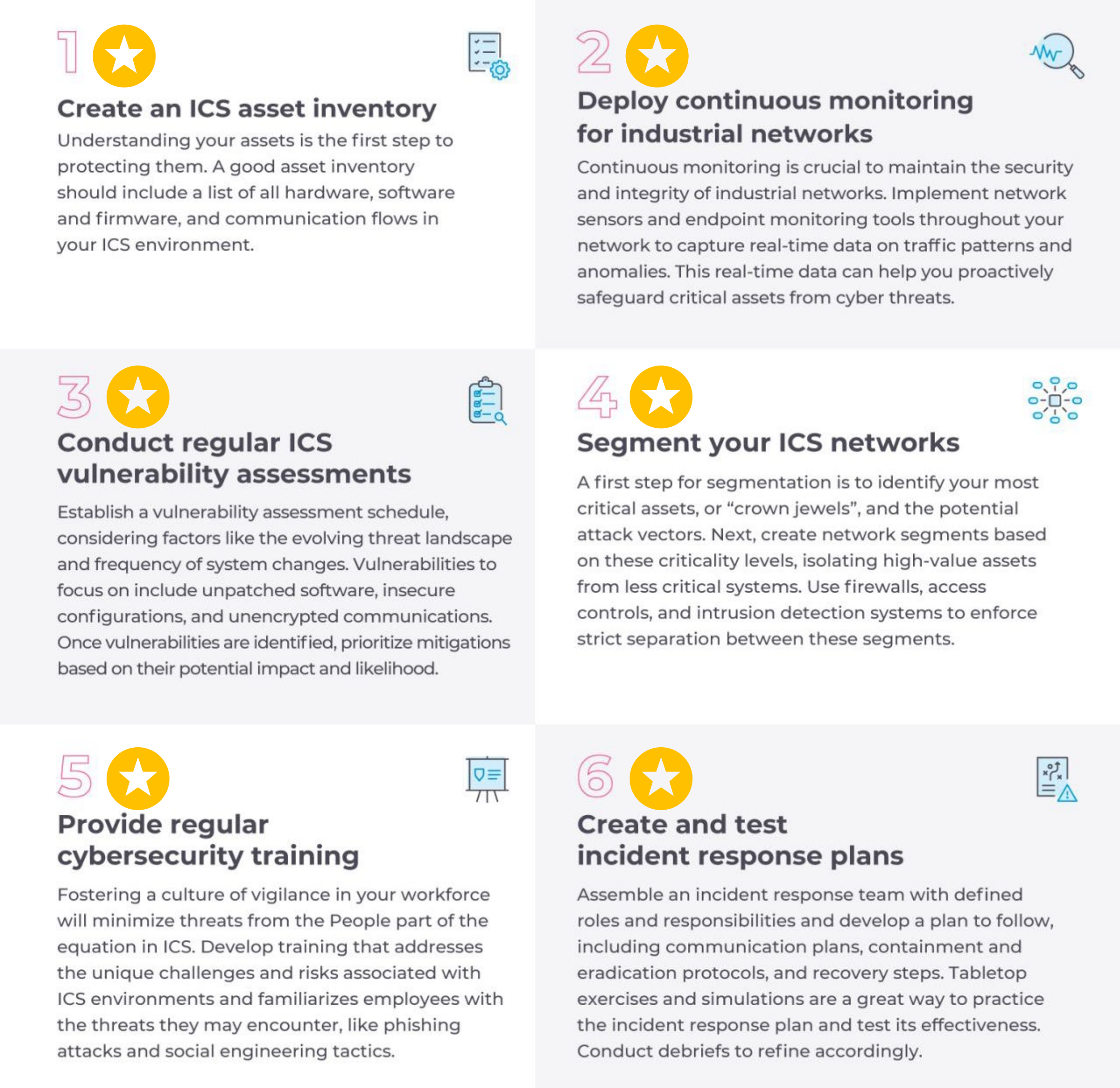
Page 1 of 1, 18 entries / filtered by **resolved: false** ✖

Export · Only unresolved · Live · 12 selected ▾

Actions	CVE	Score	EPSS sc...	CWE	CWE name	CVE creation date	Discovery date	Matching CPEs
□	CVE-2016-2279			79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2016-03-02 12:59:03.723	2024-09-29 23:22:12.965	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-
□	CVE-2018-17924			306	Missing Authentication for Critical Function	2018-12-07 15:29:00.663	2024-09-29 23:22:12.512	cpe:/h:rockwellautomation:1756-enbt:-:-:-
□	CVE-2019-12255			120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-08-09 22:15:11.347	2024-09-29 23:22:12.965	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-, cpe:/h:rockwellautomation:1756-en2tr_series_b:-:-:- ...
□	CVE-2019-12256			120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-08-09 20:15:11.227	2024-09-29 23:22:12.965	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-, cpe:/h:rockwellautomation:1756-en2tr_series_b:-:-:- ...
□	CVE-2019-12257			120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-08-09 20:15:11.320	2024-09-29 23:22:12.965	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-, cpe:/h:rockwellautomation:1756-en2tr_series_b:-:-:- ...
□	CVE-2019-12258			384	Session Fixation	2019-08-09 22:15:11.410	2024-09-29 23:22:12.966	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-, cpe:/h:rockwellautomation:1756-en2tr_series_b:-:-:- ...
□	CVE-2019-12261			120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-08-09 23:15:11.093	2024-09-29 23:22:12.966	cpe:/o:rockwellautomation:1756-en2tr_series_b_firmware:5.008:-:-, cpe:/h:rockwellautomation:1756-en2tr_series_b:-:-:-

First steps & IDS

Best Practices for OT Security



1 ★ Create an ICS asset inventory

Understanding your assets is the first step to protecting them. A good asset inventory should include a list of all hardware, software and firmware, and communication flows in your ICS environment.

2 ★ Deploy continuous monitoring for industrial networks

Continuous monitoring is crucial to maintain the security and integrity of industrial networks. Implement network sensors and endpoint monitoring tools throughout your network to capture real-time data on traffic patterns and anomalies. This real-time data can help you proactively safeguard critical assets from cyber threats.

3 ★ Conduct regular ICS vulnerability assessments

Establish a vulnerability assessment schedule, considering factors like the evolving threat landscape and frequency of system changes. Vulnerabilities to focus on include unpatched software, insecure configurations, and unencrypted communications. Once vulnerabilities are identified, prioritize mitigations based on their potential impact and likelihood.

4 ★ Segment your ICS networks

A first step for segmentation is to identify your most critical assets, or “crown jewels”, and the potential attack vectors. Next, create network segments based on these criticality levels, isolating high-value assets from less critical systems. Use firewalls, access controls, and intrusion detection systems to enforce strict separation between these segments.

5 ★ Provide regular cybersecurity training

Fostering a culture of vigilance in your workforce will minimize threats from the People part of the equation in ICS. Develop training that addresses the unique challenges and risks associated with ICS environments and familiarizes employees with the threats they may encounter, like phishing attacks and social engineering tactics.

6 ★ Create and test incident response plans

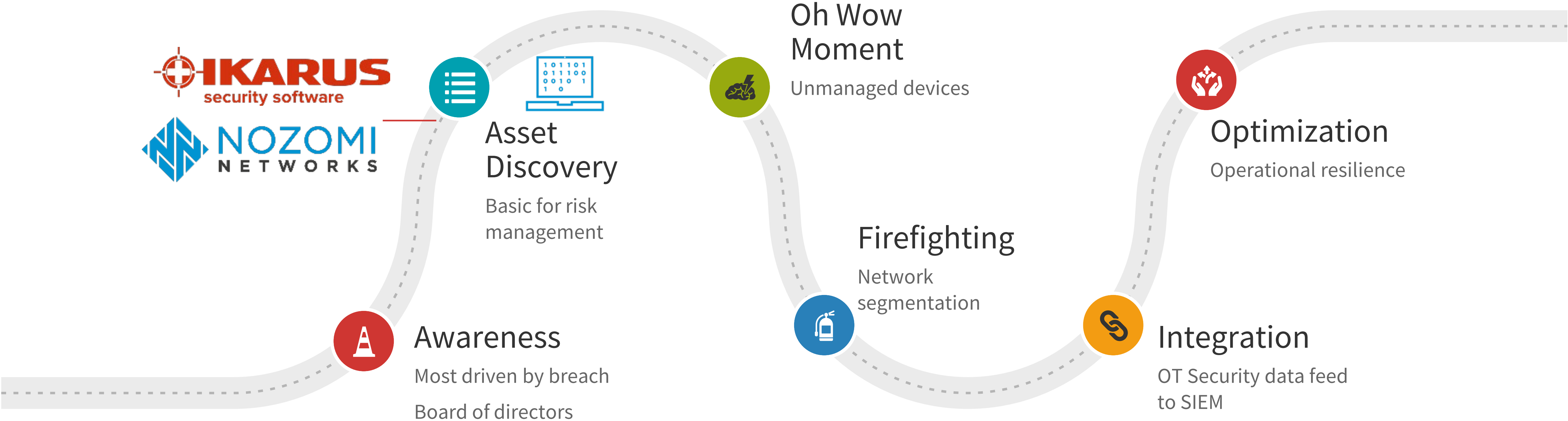
Assemble an incident response team with defined roles and responsibilities and develop a plan to follow, including communication plans, containment and eradication protocols, and recovery steps. Tabletop exercises and simulations are a great way to practice the incident response plan and test its effectiveness. Conduct debriefs to refine accordingly.

Journey of a Industrial Cybersecurity Program

A & O: Asset Inventory!

“Our common journey get started with a proof of value (PoV)“

“We want to enable your OT Security capabilities“



Awareness

Most driven by breach

Board of directors

Asset Discovery

Basic for risk management

Oh Wow Moment

Unmanaged devices

Firefighting

Network segmentation

Integration

OT Security data feed to SIEM

Optimization

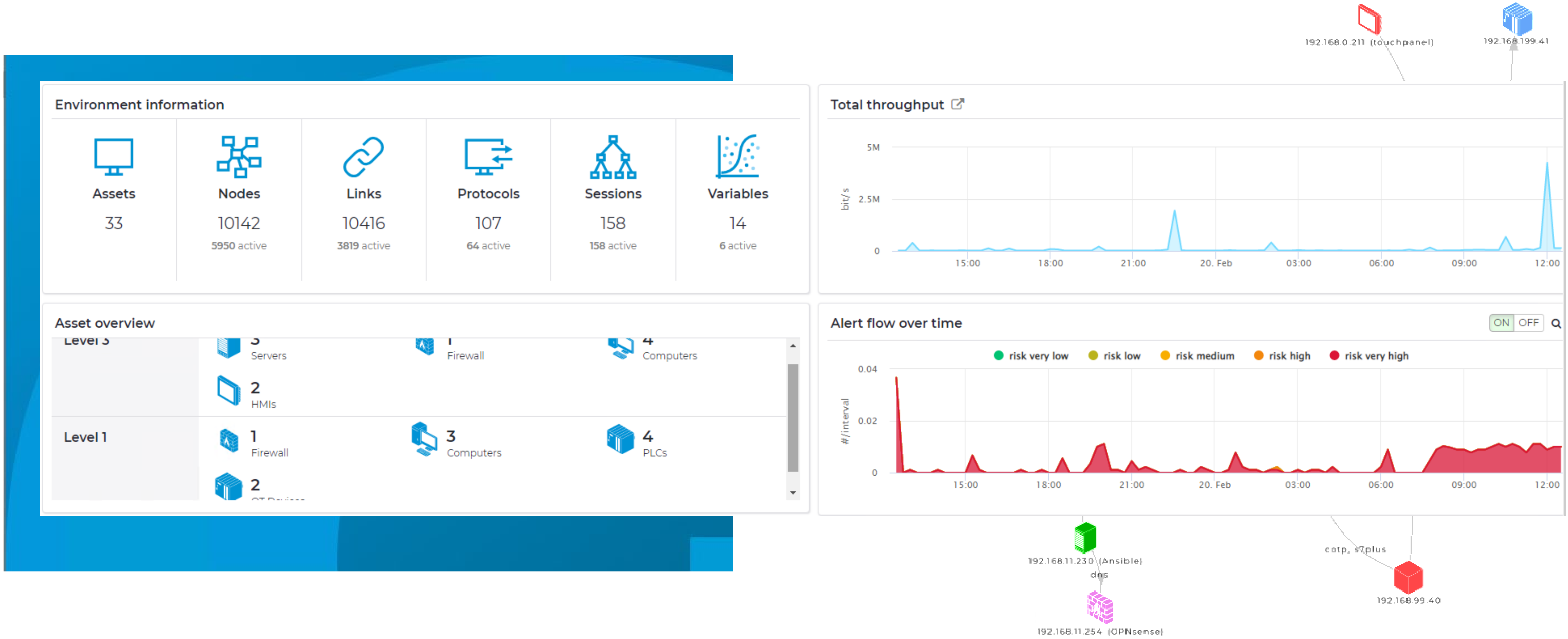
Operational resilience

60% of orgs are here

30% of orgs are here

10% of orgs are here

IDS: Visibility



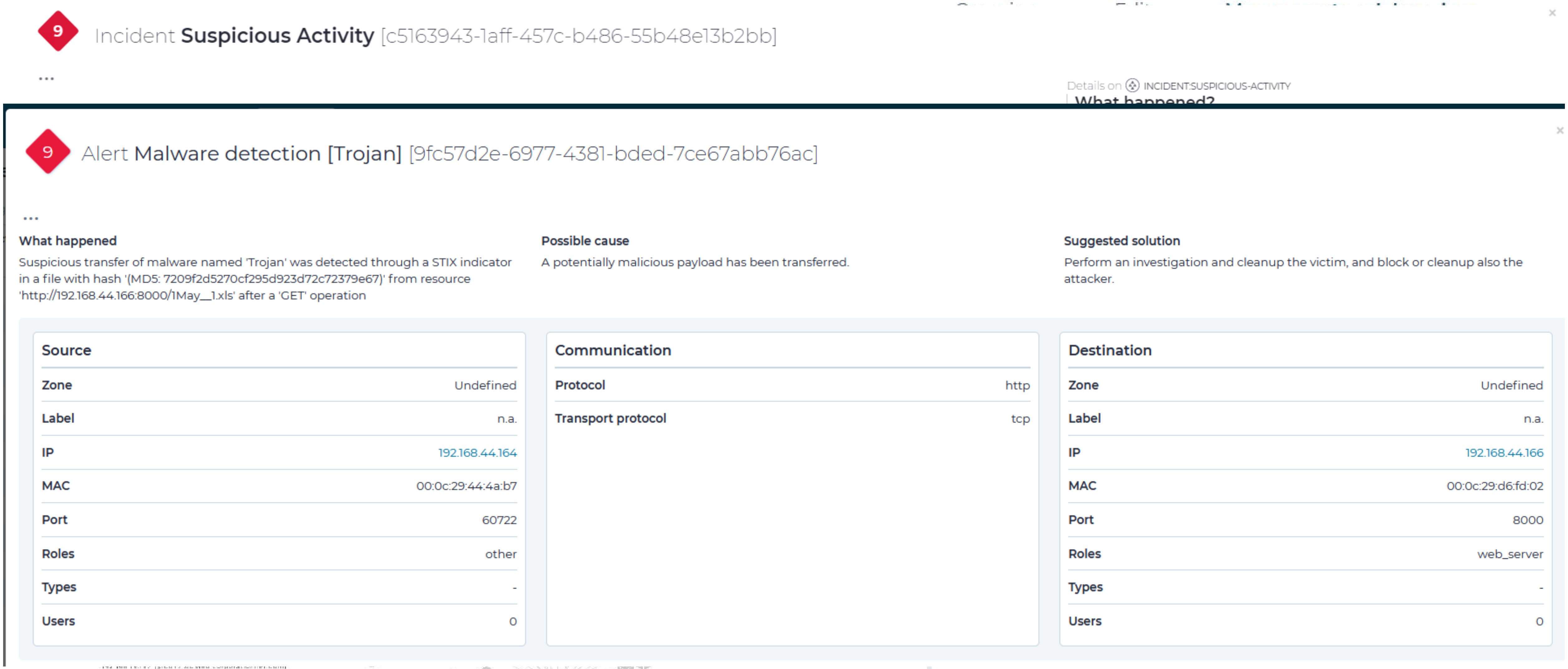
Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
33	10142	10416	107	158	14
	5950 active	3819 active	64 active	158 active	6 active

Asset overview

Level 3	3 Servers	1 Firewall	4 Computers
	2 HMIs		
Level 1	1 Firewall	3 Computers	4 PLCs
	2 OT Devices		

IDS: Anomaly & Threat Detection



9 Incident **Suspicious Activity** [c5163943-1aff-457c-b486-55b48e13b2bb]

...

Details on INCIDENT:SUSPICIOUS-ACTIVITY

What happened?

9 Alert **Malware detection [Trojan]** [9fc57d2e-6977-4381-bded-7ce67abb76ac]

...

What happened

Suspicious transfer of malware named 'Trojan' was detected through a STIX indicator in a file with hash '(MD5: 7209f2d5270cf295d923d72c72379e67)' from resource 'http://192.168.44.166:8000/1May__1.xls' after a 'GET' operation

Possible cause

A potentially malicious payload has been transferred.

Suggested solution

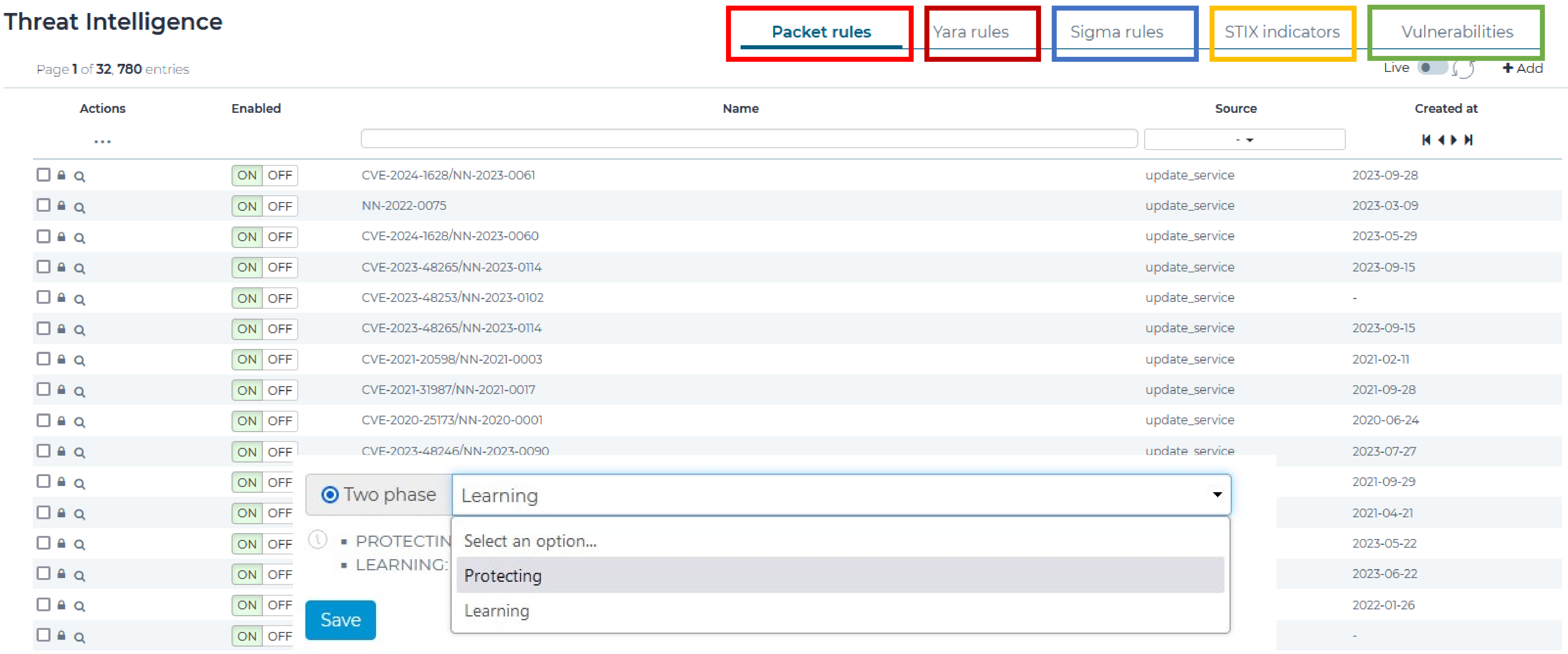
Perform an investigation and cleanup the victim, and block or cleanup also the attacker.

Source	
Zone	Undefined
Label	n.a.
IP	192.168.44.164
MAC	00:0c:29:44:4a:b7
Port	60722
Roles	other
Types	-
Users	0

Communication	
Protocol	http
Transport protocol	tcp

Destination	
Zone	Undefined
Label	n.a.
IP	192.168.44.166
MAC	00:0c:29:d6:fd:02
Port	8000
Roles	web_server
Types	-
Users	0

Threat Intelligence



Threat Intelligence

Page 1 of 32, 780 entries

Actions	Enabled	Name	Source	Created at
☐ 🔒 🔍	ON OFF	CVE-2024-1628/NN-2023-0061	update_service	2023-09-28
☐ 🔒 🔍	ON OFF	NN-2022-0075	update_service	2023-03-09
☐ 🔒 🔍	ON OFF	CVE-2024-1628/NN-2023-0060	update_service	2023-05-29
☐ 🔒 🔍	ON OFF	CVE-2023-48265/NN-2023-0114	update_service	2023-09-15
☐ 🔒 🔍	ON OFF	CVE-2023-48253/NN-2023-0102	update_service	-
☐ 🔒 🔍	ON OFF	CVE-2023-48265/NN-2023-0114	update_service	2023-09-15
☐ 🔒 🔍	ON OFF	CVE-2021-20598/NN-2021-0003	update_service	2021-02-11
☐ 🔒 🔍	ON OFF	CVE-2021-31987/NN-2021-0017	update_service	2021-09-28
☐ 🔒 🔍	ON OFF	CVE-2020-25173/NN-2020-0001	update_service	2020-06-24
☐ 🔒 🔍	ON OFF	CVE-2023-48246/NN-2023-0090	update_service	2023-07-27
☐ 🔒 🔍	ON OFF			2021-09-29
☐ 🔒 🔍	ON OFF			2021-04-21
☐ 🔒 🔍	ON OFF			2023-05-22
☐ 🔒 🔍	ON OFF			2023-06-22
☐ 🔒 🔍	ON OFF			2022-01-26
☐ 🔒 🔍	ON OFF			-

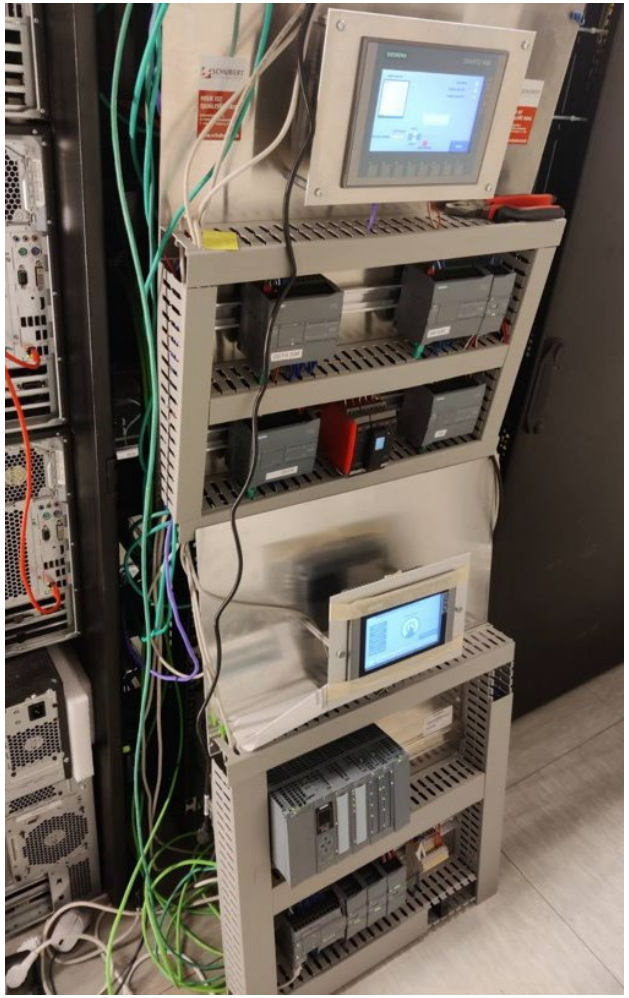
● Two phase: Learning

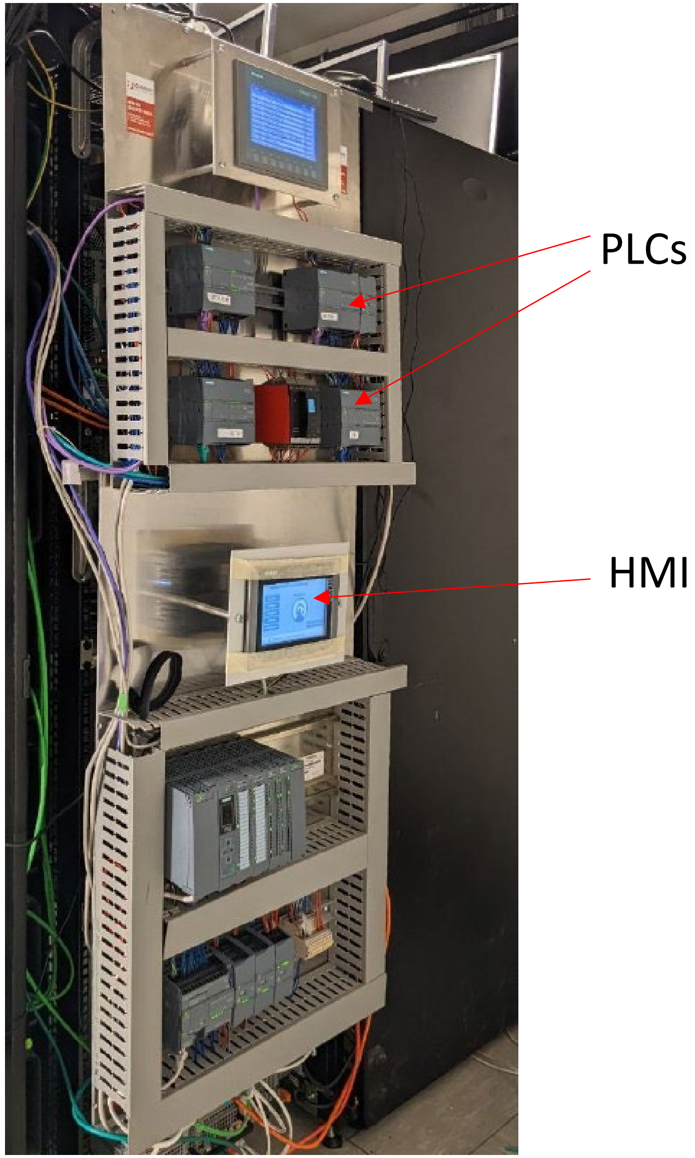
- PROTECTIN
- LEARNING:

Industrial Honeypot

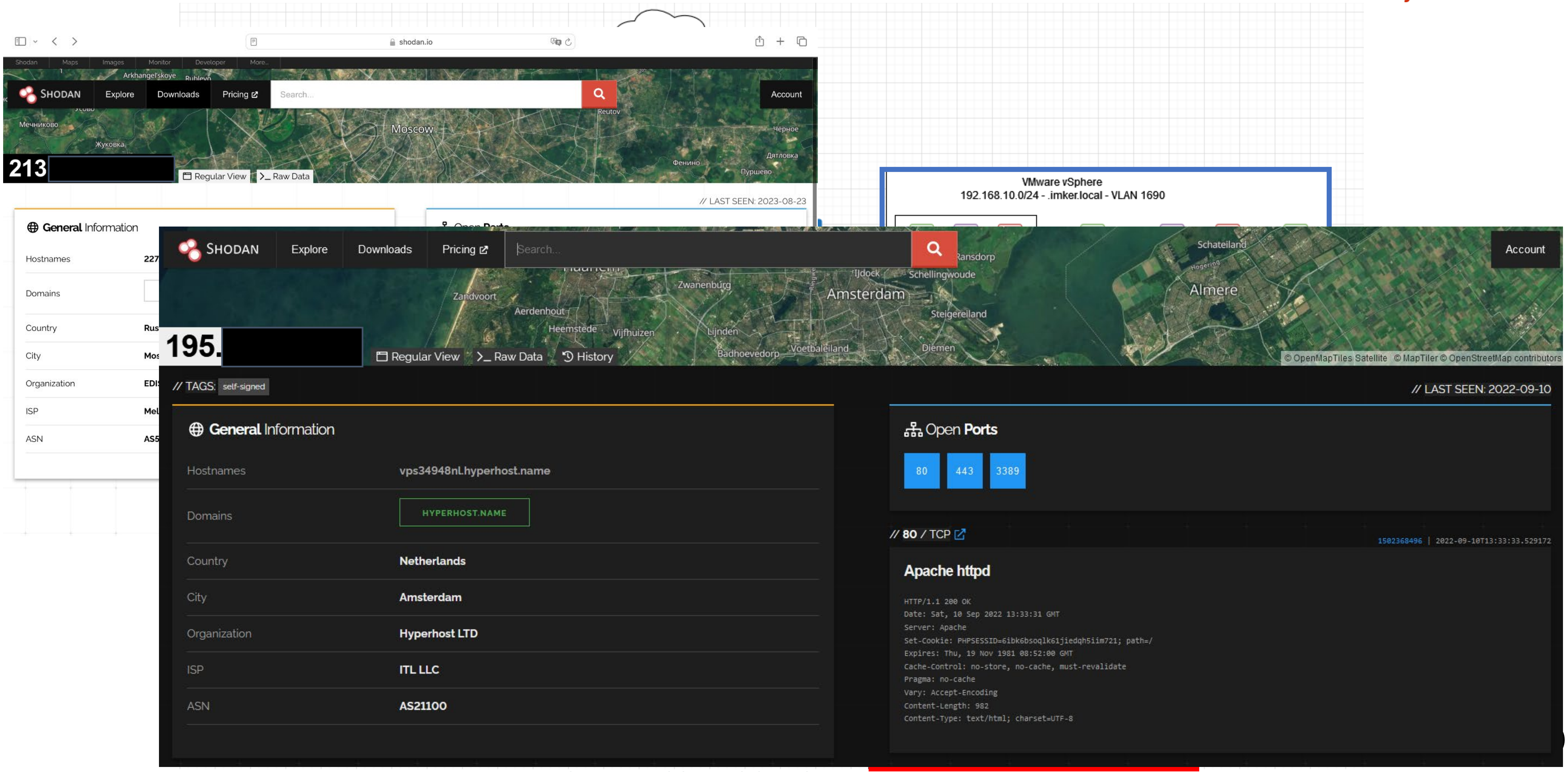
Level der Interaktion	Interaktion mit Host	Interaktion mit Programm	Programm verändern
Low	✓	✗	✗
Medium	✓	✓	✗
High	✓	✓	✓

High-Interaction Honeypot @ fhstp





Under the hood



213 [redacted]

// LAST SEEN: 2023-08-23

General Information

Hostnames	227
Domains	
Country	Rus
City	Mos
Organization	EDI
ISP	Mel
ASN	AS5

195.[redacted]

// TAGS: self-signed

// LAST SEEN: 2022-09-10

General Information

Hostnames	vps34948nl.hyperhost.name
Domains	HYPERHOST.NAME
Country	Netherlands
City	Amsterdam
Organization	Hyperhost LTD
ISP	ITL LLC
ASN	AS21100

Open **Ports**

80 443 3389

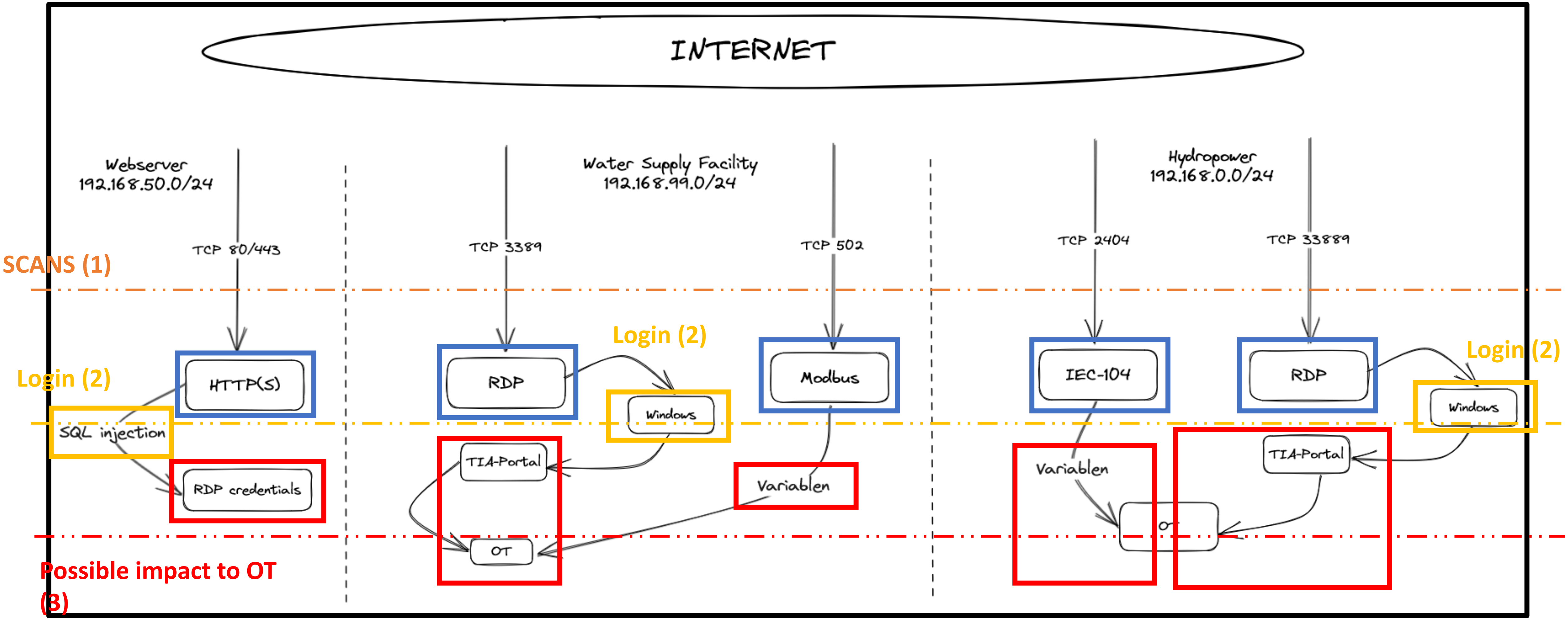
// **80** / TCP

1502368496 | 2022-09-10T13:33:33.529172

Apache httpd

```
HTTP/1.1 200 OK
Date: Sat, 10 Sep 2022 13:33:31 GMT
Server: Apache
Set-Cookie: PHPSESSID=6ibk6bsoqlk61jiedqh5iim721; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 982
Content-Type: text/html; charset=UTF-8
```

Attack surface



SCANS (1)

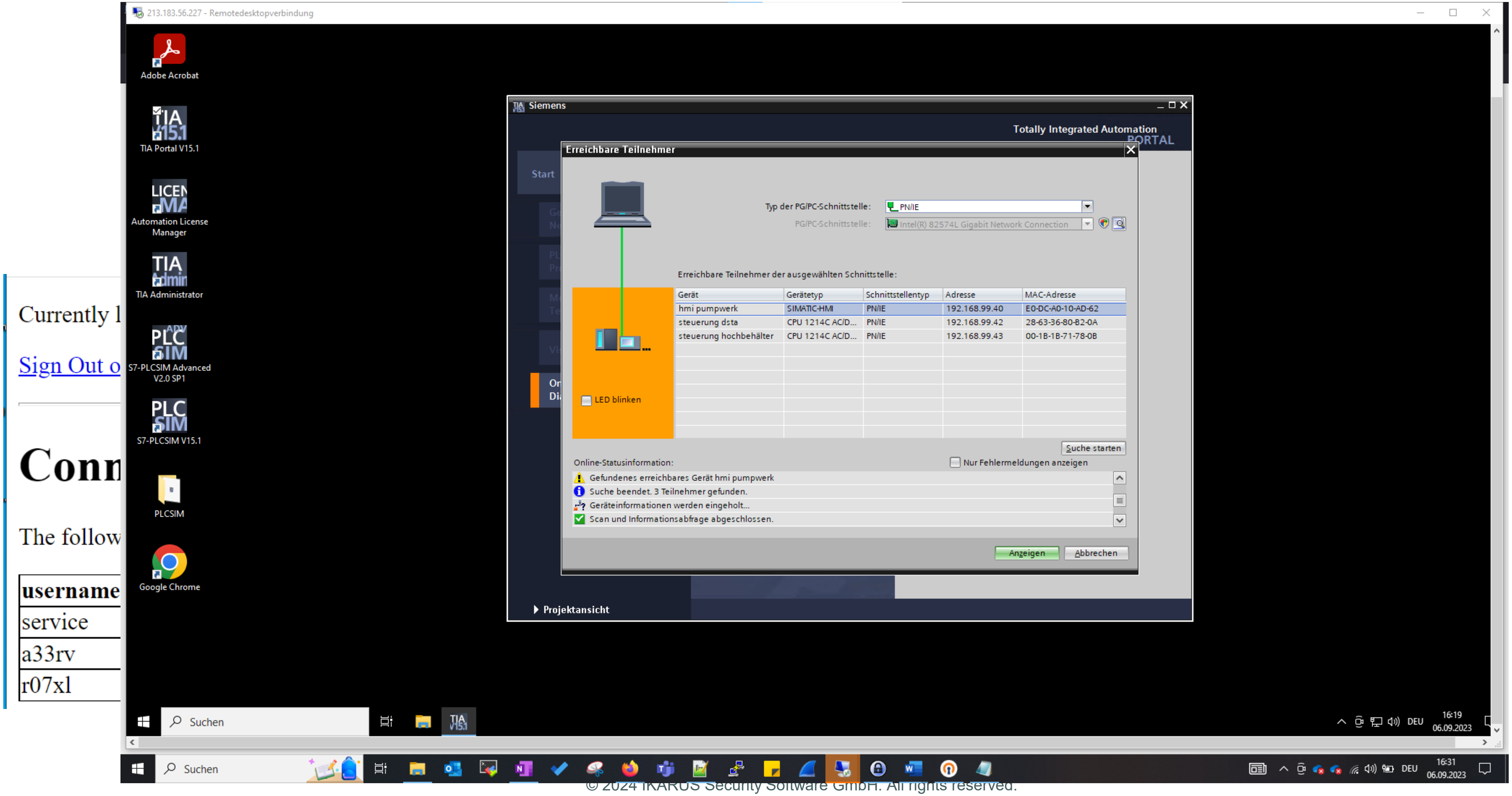
Login (2)

Login (2)

Login (2)

Possible impact to OT (3)

Look & feel



Currently l

Sign Out o

Conn

The follow

username
service
a33rv
r07xl

213.183.56.227 - Remotedesktopverbindung

Siemens

Totally Integrated Automation PORTAL

Erreichbare Teilnehmer

Typ der PG/PC-Schnittstelle: PN/IE

PG/PC-Schnittstelle: Intel(R) 82574L Gigabit Network Connection

Erreichbare Teilnehmer der ausgewählten Schnittstelle:

Gerät	Gerätetyp	Schnittstellentyp	Adresse	MAC-Adresse
hmi pumpwerk	SIMATIC-HMI	PN/IE	192.168.99.40	E0-DC-A0-10-AD-62
steuerung dsta	CPU 1214C AC/D...	PN/IE	192.168.99.42	28-63-36-80-B2-0A
steuerung hochbehälter	CPU 1214C AC/D...	PN/IE	192.168.99.43	00-1B-1B-71-78-0B

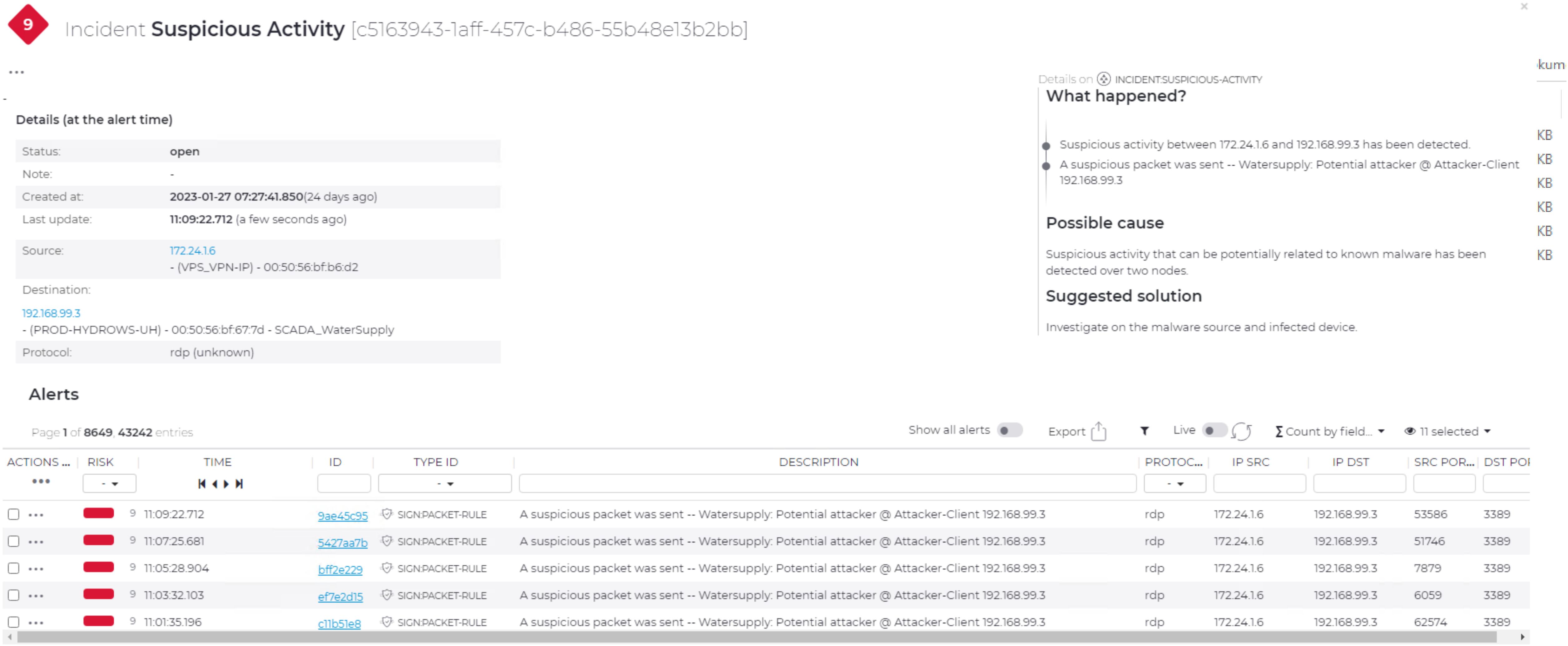
□ LED blinken

Online-Statusinformation:

□ Nur Fehlermeldungen anzeigen

```
Gefundenes erreichbares Gerät hmi pumpwerk
Suche beendet. 3 Teilnehmer gefunden.
Geräteinformationen werden eingeholt...
Scan und Informationsabfrage abgeschlossen.
```

What happened so far?



9 Incident **Suspicious Activity** [c5163943-1aff-457c-b486-55b48e13b2bb]

...

Details (at the alert time)

Status:	**open**
Note:	-
Created at:	**2023-01-27 07:27:41.850**(24 days ago)
Last update:	**11:09:22.712** (a few seconds ago)
Source:	172.24.1.6 - (VPS_VPN-IP) - 00:50:56:bf:b6:d2
Destination:	192.168.99.3 - (PROD-HYDROWS-UH) - 00:50:56:bf:67:7d - SCADA_WaterSupply
Protocol:	rdp (unknown)

Details on INCIDENT:SUSPICIOUS-ACTIVITY

What happened?

- Suspicious activity between 172.24.1.6 and 192.168.99.3 has been detected.
- A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3

Possible cause

Suspicious activity that can be potentially related to known malware has been detected over two nodes.

Suggested solution

Investigate on the malware source and infected device.

kum

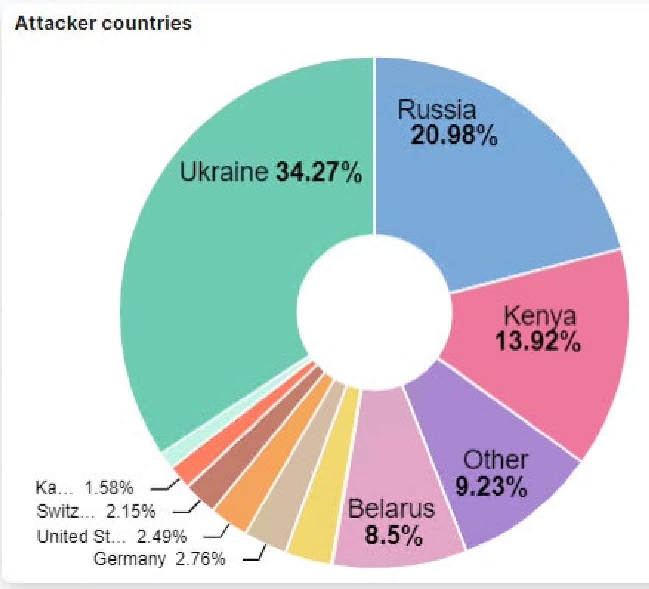
KB
KB
KB
KB
KB
KB

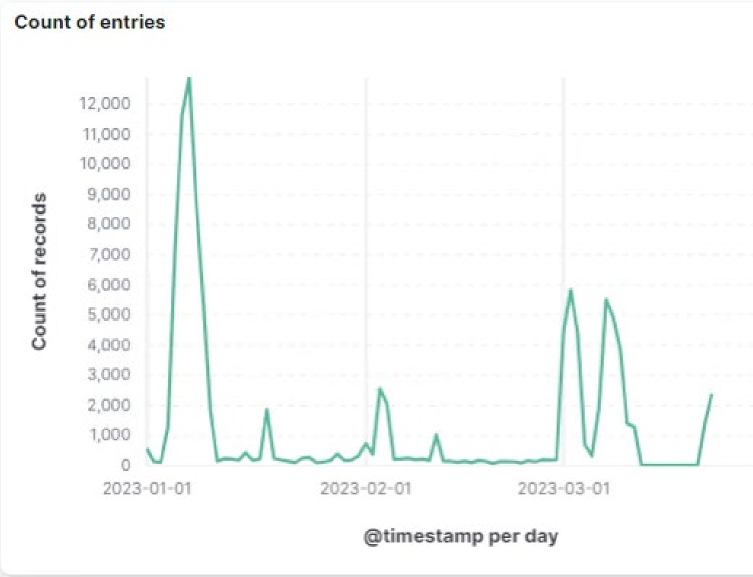
Alerts

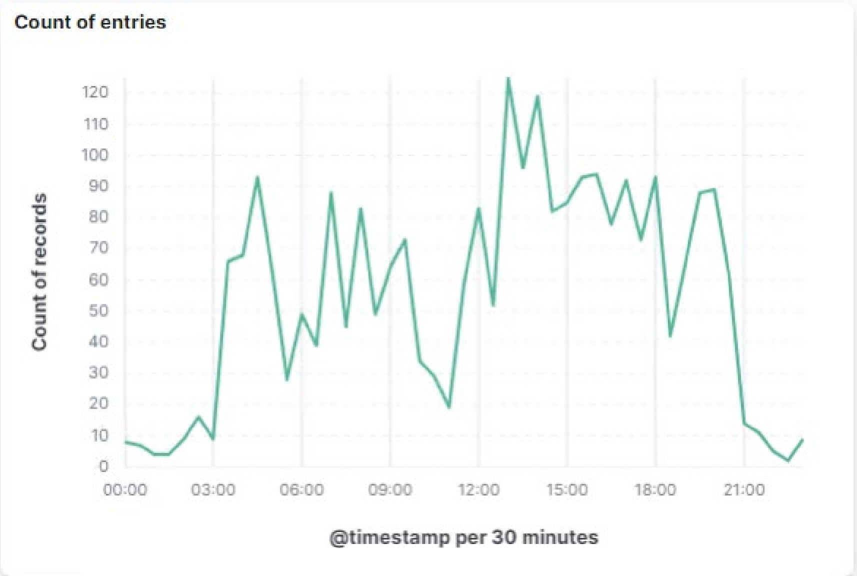
Page **1** of **8649**, **43242** entries

ACTIONS ...	RISK	TIME	ID	TYPE ID	DESCRIPTION	PROTOC...	IP SRC	IP DST	SRC POR...	DST POI
□ •••	🟥 9	11:09:22.712	9ae45c95	SIGN:PACKET-RULE	A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3	rdp	172.24.1.6	192.168.99.3	53586	3389
□ •••	🟥 9	11:07:25.681	5427aa7b	SIGN:PACKET-RULE	A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3	rdp	172.24.1.6	192.168.99.3	51746	3389
□ •••	🟥 9	11:05:28.904	bff2e229	SIGN:PACKET-RULE	A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3	rdp	172.24.1.6	192.168.99.3	7879	3389
□ •••	🟥 9	11:03:32.103	ef7e2d15	SIGN:PACKET-RULE	A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3	rdp	172.24.1.6	192.168.99.3	6059	3389
□ •••	🟥 9	11:01:35.196	c11b51e8	SIGN:PACKET-RULE	A suspicious packet was sent -- Watersupply: Potential attacker @ Attacker-Client 192.168.99.3	rdp	172.24.1.6	192.168.99.3	62574	3389

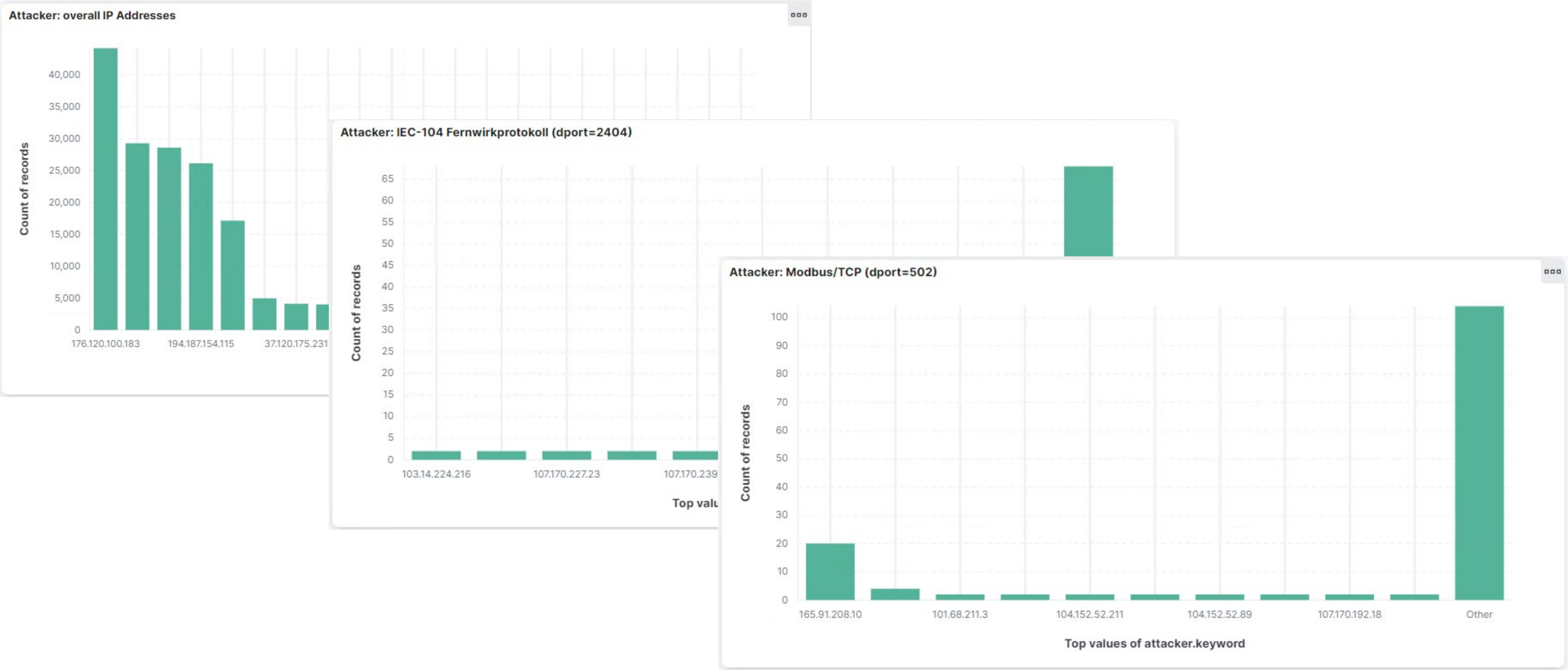
Trends: Q1 2023





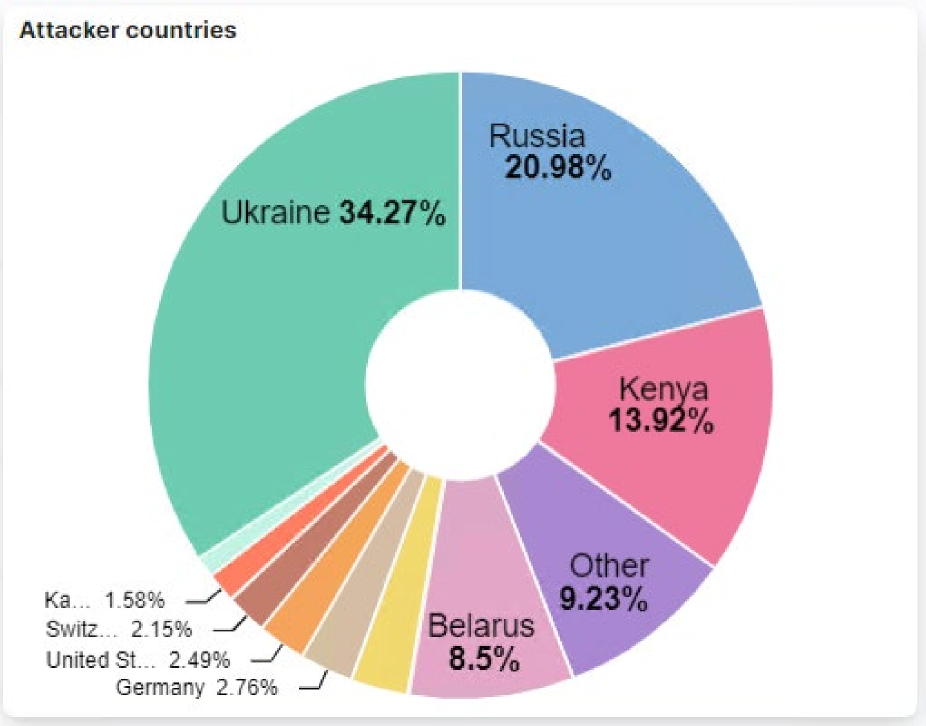


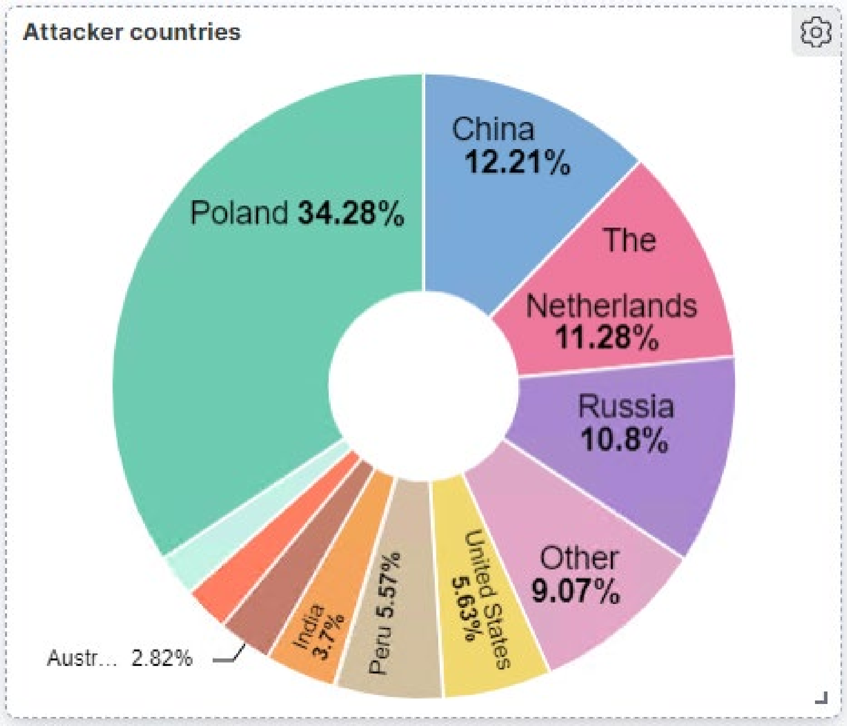
Trends: Q1 2023



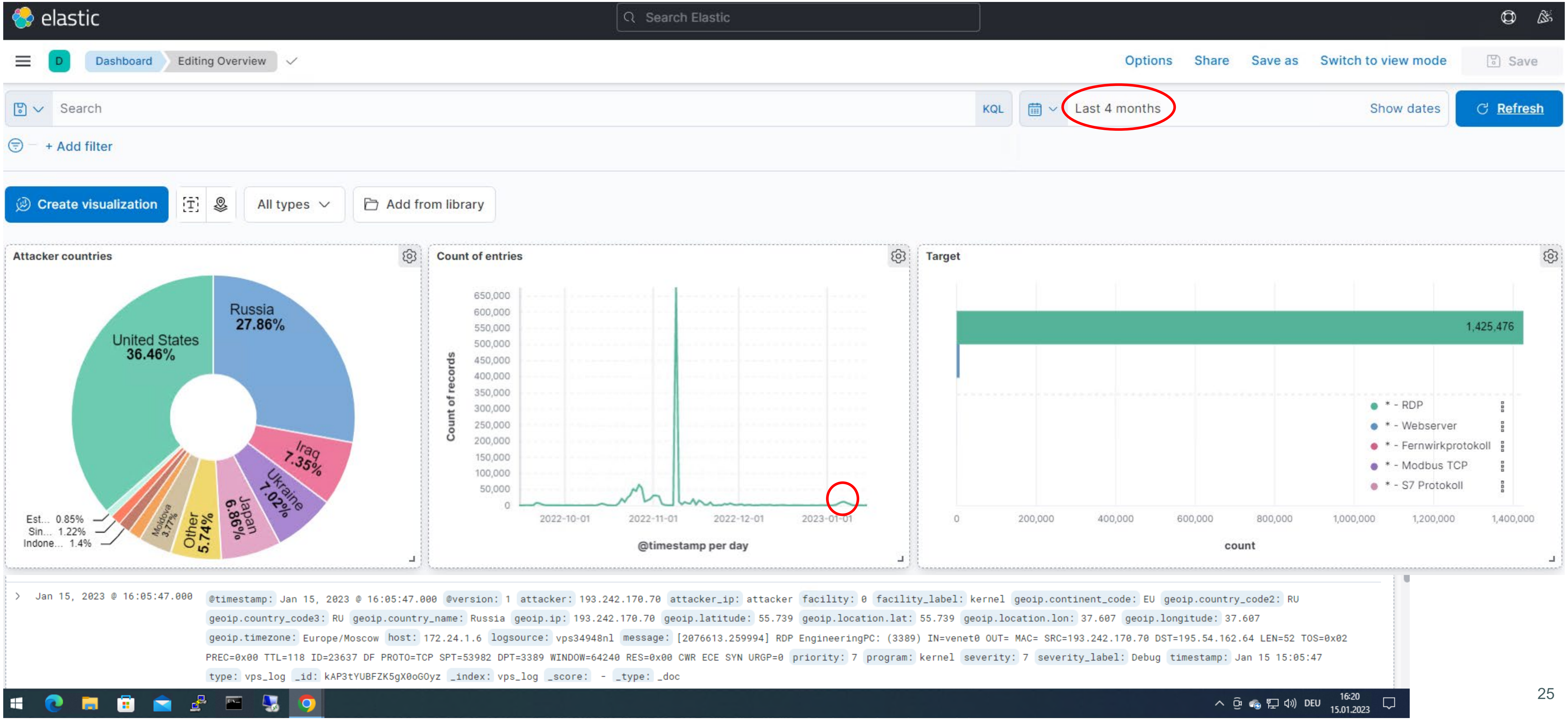
Trends: 01/2024

> VPS von Niederlanden zu Russland



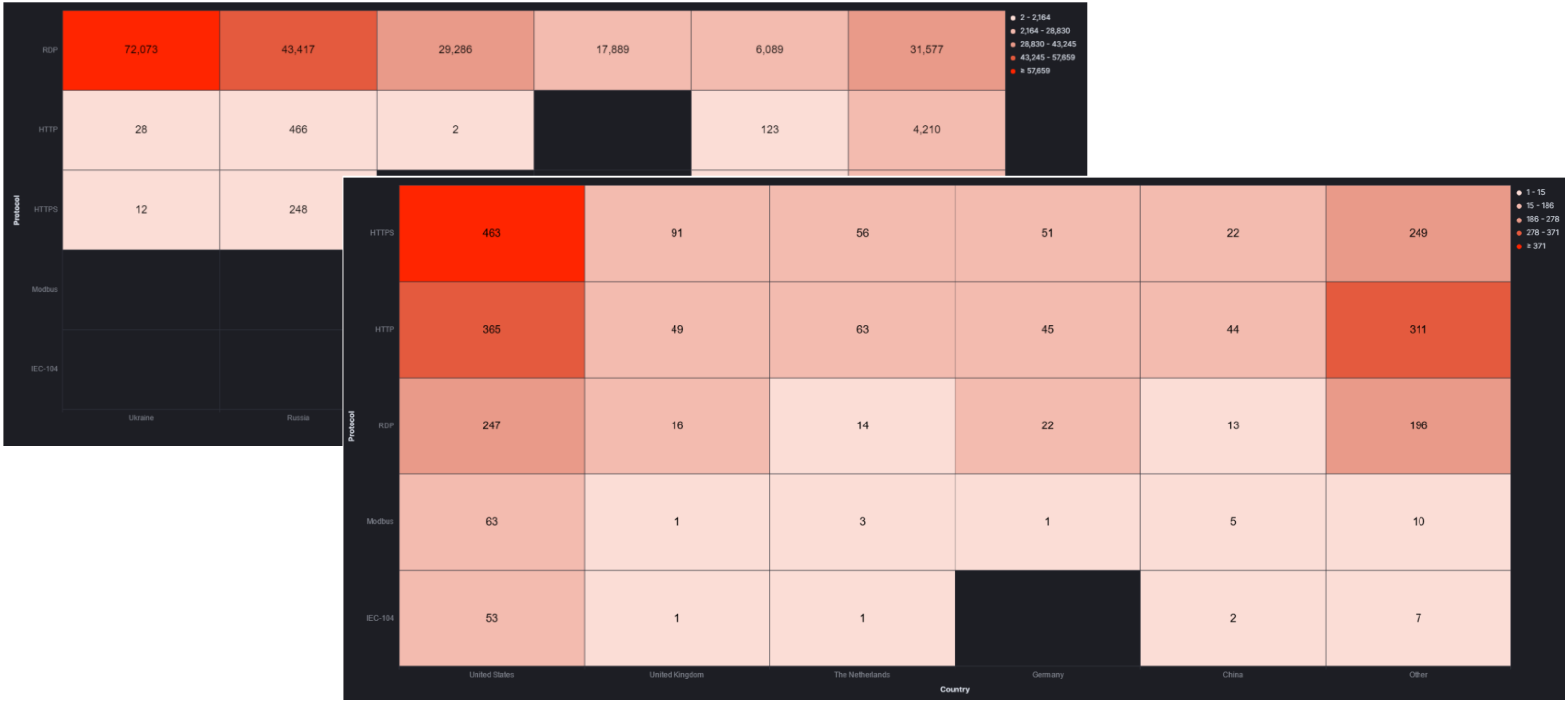


Factor time



```
>  Jan 15, 2023 @ 16:05:47.000   @timestamp: Jan 15, 2023 @ 16:05:47.000 @version: 1 attacker: 193.242.170.70 attacker_ip: attacker facility: 0 facility_label: kernel geoip.continent_code: EU geoip.country_code2: RU
                                geoip.country_code3: RU geoip.country_name: Russia geoip.ip: 193.242.170.70 geoip.latitude: 55.739 geoip.location.lat: 55.739 geoip.location.lon: 37.607 geoip.longitude: 37.607
                                geoip.timezone: Europe/Moscow host: 172.24.1.6 logsource: vps34948nl message: [2076613.259994] RDP EngineeringPC: (3389) IN=venet0 OUT= MAC= SRC=193.242.170.70 DST=195.54.162.64 LEN=52 TOS=0x02
                                PREC=0x00 TTL=118 ID=23637 DF PROTO=TCP SPT=53982 DPT=3389 WINDOW=64240 RES=0x00 CWR ECE SYN URGP=0 priority: 7 program: kernel severity: 7 severity_label: Debug timestamp: Jan 15 15:05:47
                                type: vps_log _id: kAP3tYUBFZK5gX0oGOyz _index: vps_log _score: - _type: _doc
```

Trends: 2023 → 2024



Protocol	Ukraine	Russia				
RDP	72,073	43,417	29,286	17,889	6,089	31,577
HTTP	28	466	2		123	4,210
HTTPS	12	248				
Modbus						
IEC-104						

- ● 2 - 2,164
- ● 2,164 - 28,830
- ● 28,830 - 43,245
- ● 43,245 - 57,659
- ● ≥ 57,659

Protocol	United States	United Kingdom	The Netherlands	Germany	China	Other
HTTPS	463	91	56	51	22	249
HTTP	365	49	63	45	44	311
RDP	247	16	14	22	13	196
Modbus	63	1	3	1	5	10
IEC-104	53	1	1		2	7

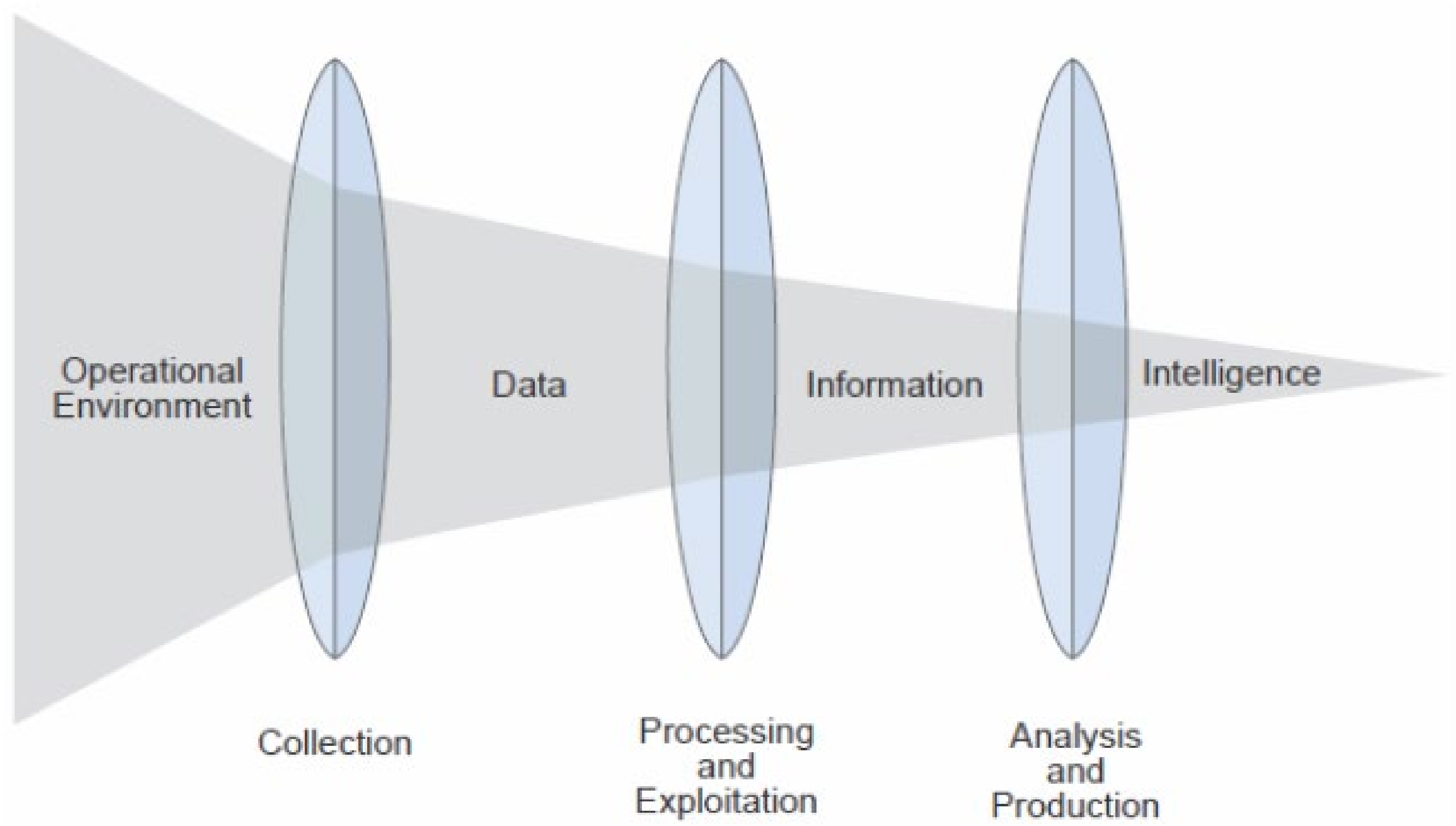
Country

- ● 1 - 15
- ● 15 - 186
- ● 186 - 278
- ● 278 - 371
- ● ≥ 371

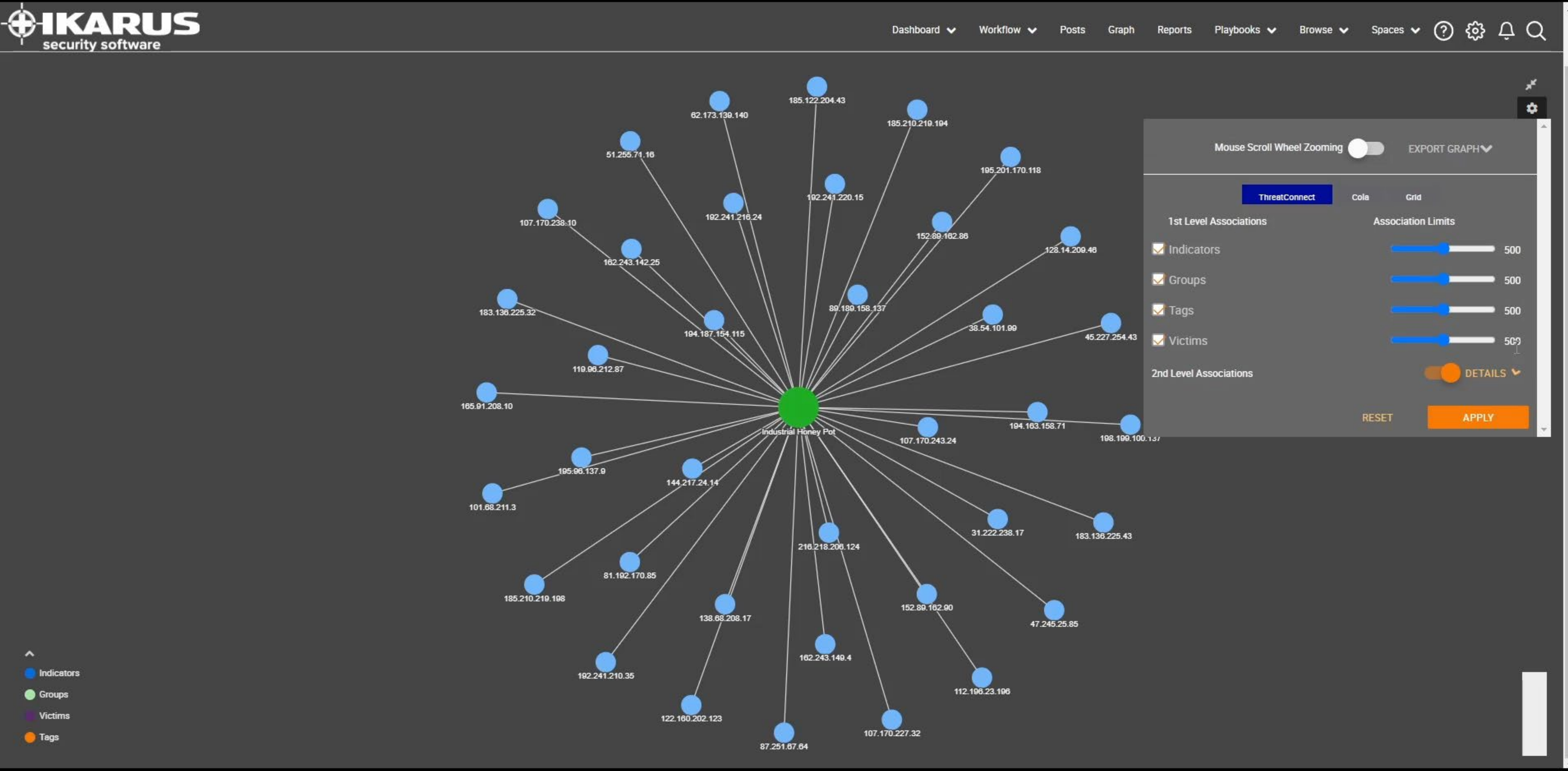
Data → Information → Intelligence

IKARUS security software

IKARUS threat.intelligence



M. E. Dempsey, *Joint Intelligence*, 2013



Mouse Scroll Wheel Zooming ○ EXPORT GRAPH

ThreatConnect Cola Grid

1st Level Associations	Association Limits
☑ Indicators	500
☑ Groups	500
☑ Tags	500
☑ Victims	500

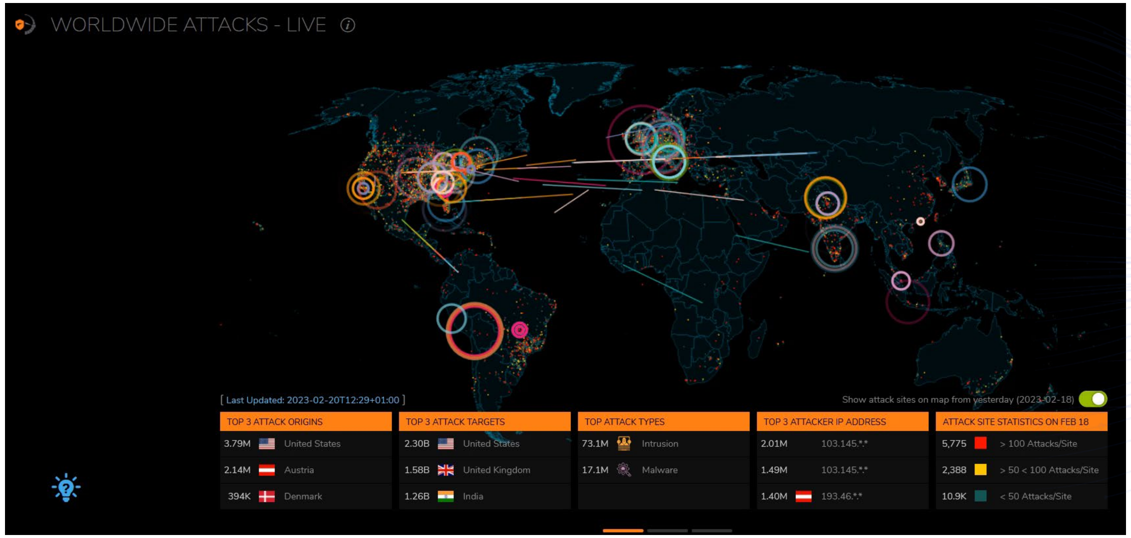
2nd Level Associations ● DETAILS

RESET APPLY

- ● Indicators
- ● Groups
- ● Victims
- ● Tags

Connecting the Dots

Wie gewonnene Informationen weiterverwendet werden können.

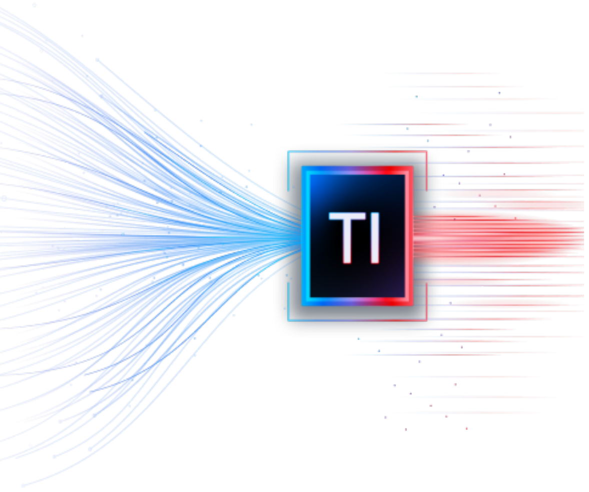


WORLDWIDE ATTACKS - LIVE

[Last Updated: 2023-02-20T12:29+01:00]

Show attack sites on map from yesterday (2023-02-18)

TOP 3 ATTACK ORIGINS	TOP 3 ATTACK TARGETS	TOP ATTACK TYPES	TOP 3 ATTACKER IP ADDRESS	ATTACK SITE STATISTICS ON FEB 18
3.79M United States	2.30B United States	73.1M Intrusion	2.01M 103.145.*.*	5,775 🟥 > 100 Attacks/Site
2.14M Austria	1.58B United Kingdom	17.1M Malware	1.49M 103.145.*.*	2,388 🟨 > 50 < 100 Attacks/Site
394K Denmark	1.26B India		1.40M 193.46.*.*	10.9K 🟩 < 50 Attacks/Site



- *IDS / IPS / Firewall etc.*
- *Security Operations Center (SOC)*
- *Incident Response (IR)*
- *Vulnerability Management*
- *Produktionsleitung*
- *CISO*
- *…*

IKARUS Security Software in a nutshell

IKARUS security software

ENTERPRISE CYBER SECURITY

- Antivirus
- EDR
- Mobile Security
- MDM
- Mail Security
- Threat Intelligence
- Malware Scanner
- Malware Scan Service
- Incident Response
- Managed Defense

INDUSTRIAL CYBER SECURITY

- OT Security Sensor
- OT Security Sensor Management
- OT Security Professional Services

IKARUS security software

Austrian cybersecurity manufacturer with in-house development, virus lab and customer support.
Certified system integrator, platinum partner & MSSP (Managed Security Service Provider) of international technology partners.

YOU ARE HERE

Trellix
Leading cyber actors hunting technologies

CHECK POINT
Market-leading solution for mobile threat defence

HarfangLab
Leading endpoint protection solutions

MANDIANT NOW PART OF Google Cloud
Global Leading Cyber Threat Intelligence for IT

NOZOMI NETWORKS
Global Leading OT/IoT Security Technology

Dipl.-Ing. Martin Strommer
Team Lead OT Security
strommer.m@ikarus.at

IKARUS
security software

NOZOMI NETWORKS

HarfangLab

MANDIANT
NOW PART OF Google Cloud

You‘ve heard from us.

We want to hear from **you**.

+43 1 58995 - 500

sales@ikarus.at

https://www.ikarussecurity.com/