Hacknowledge

# IoT under the Lens: Zeek and ELK Analytics

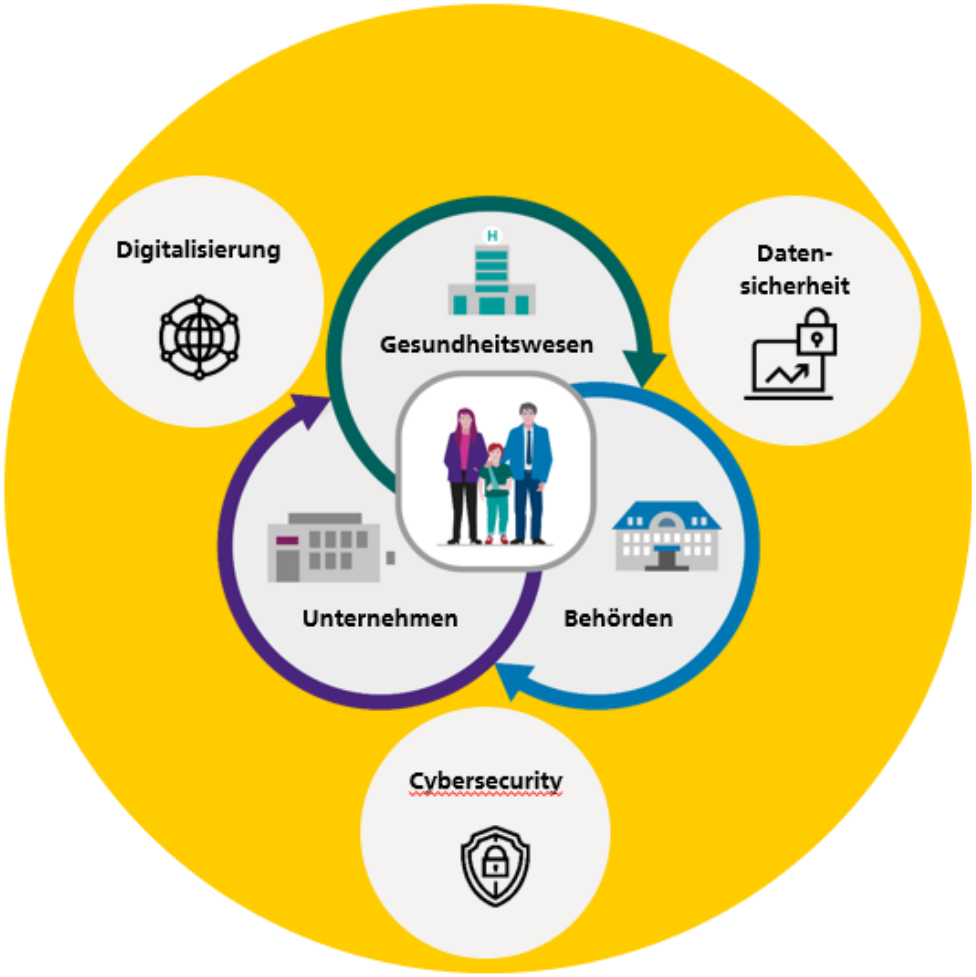
Simple and Efficient

# Kommunikations-Services Post

Der Motor für eine digitale und vernetzte Schweiz

# Wir treiben die digitale Transformation in der Schweiz voran

## Unsere Mission




Interaktionen – einfach, sicher, digital.

Wir ermöglichen **Menschen**, **Unternehmen** und **Behörden** intuitive **digitale Interaktionen** sowie den **einfachen** und **sicheren Umgang** mit ihren **Daten**.

Hacknowledge

# Interaktionen – einfach, sicher, digital

## Wir orchestrieren ihre Kommunikation

| | Weitere Industrien und Märkte | KMU | Gesundheitswesen | Behörden |
|---|---|---|---|---|
| | (Finanzdienstleister & weitere)<br><br>In- & Ausland | KLARA | E-Patientendossier<br>Cuore B2B2C<br>Time4Patient | DIALOG6<br>CITIZEN powered by T2i<br>E-Voting-System |
| **Kommunikations-Plattformen** | unblu, e, youdoc powered by T2i, SPOTME, IncaMail, tresorit, HRCAFÉ powered by T2i | | | |
| **Enabler-Services** | SwissID | SwissID Sign | Hacknowledge | terreActive |

Hacknowledge

# IoT under the Lens: Zeek and ELK Analytics

Simple and Efficient

Hacknowledge

# ~$ whoami

# Romain Petro

→ Formerly Security Engineer (at Hacknowledge)
→ Formerly Team Leader (at Hacknowledge)
→ Currently **SIEM Architect** (at Hacknowledge)

Specialized on Microsoft Sentinel, Splunk and Elastic

Technical lead on the Elastic Stack
→ Maintenance, monitoring, enhancements

# About Hacknowledge

We provide simple, efficient and pragmatic solutions and services to improve our customers' cybersecurity maturity.

Switzerland: Headquarter and central hub for operations, incl. Datacenters

Luxembourg: Commercial representation for BENELUX clients, hub for Offensive security

52 employees – incl. 47 security engineers

ISO 27001 certification

majority shareholder since 2022

SWISS POST




Hacknowledge

# Sensors components

## Our Sensors

- Custom development
- Optimized
- Hardware or virtual
- Managed by Hacknowledge
- Many interfaces

### Sensor's characteristic

- 4 x SFP+ 10 Gbs interfaces
- 6x 1Gbs copper interfaces
- 8 cores processors
- 16G Ram-Disk (all logs are cached and managed in RAM to extend SSD life)

CITRIX XenServer

Microsoft

vmware

KVM

### Log collector

- Push / Fetch
- Cache and filter
- Local correlation
- Enrichment and tech partnerships

### IDS

- Span , tap , rspan
- Managed by Hacknowledge
- Different feeds
- CIRCL, FIRST, Commercial, Gov...

### Honeypots

- As many as needed
- Low or high interaction
- Different services : file, web, VOIP, DB,..

### Vulnerability scanning

- Launched from sensor
- Provides you with visibility
- Helps to prioritize and understand alerts



Hacknowledge

# IDS Setup problematics

1. We setup Network Intrusion Detection systems on our sensors
2. We ask the customer to replicate the traffic of its network equipments
3. The customer doesn’t always have the technical background to correctly setup a port mirroring

→ We end up with a partial network coverage on our customer networks

Few years ago, we added **Zeek** as a debug tool for IDS setup.
Instead of a Tcpdump manual session, we bring more context for the customer:

- Which VLANs are we observing
- Which kind of protocols do we catch
- Which subnets are we monitoring

# ELK Stack components

## Logstash

### Logs management

- Free license
- Infinite volume
- Solution Open Source
- Important community
- Customizable for any source

## Elasticsearch

### Database

- Open source
- Frequently updated
- Vitesse de traitement
- Multi format (noSQL)

## Kafka

### Logs processing

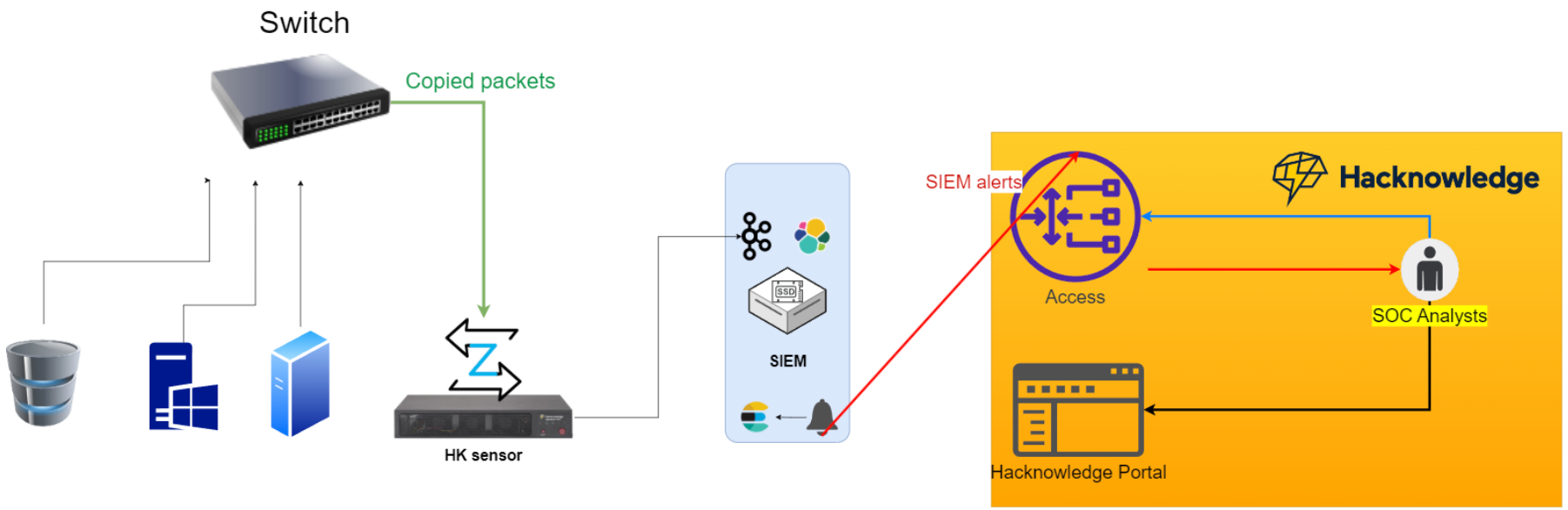
- Fault tolerance
- High flow
- Small latency
- Ingestion variety

## Kibana

### Search and Analytics

- Easy to use for everyone
- Permissions split
- Logs access (low and high level)
- Security detections

# Common ELK Architecture



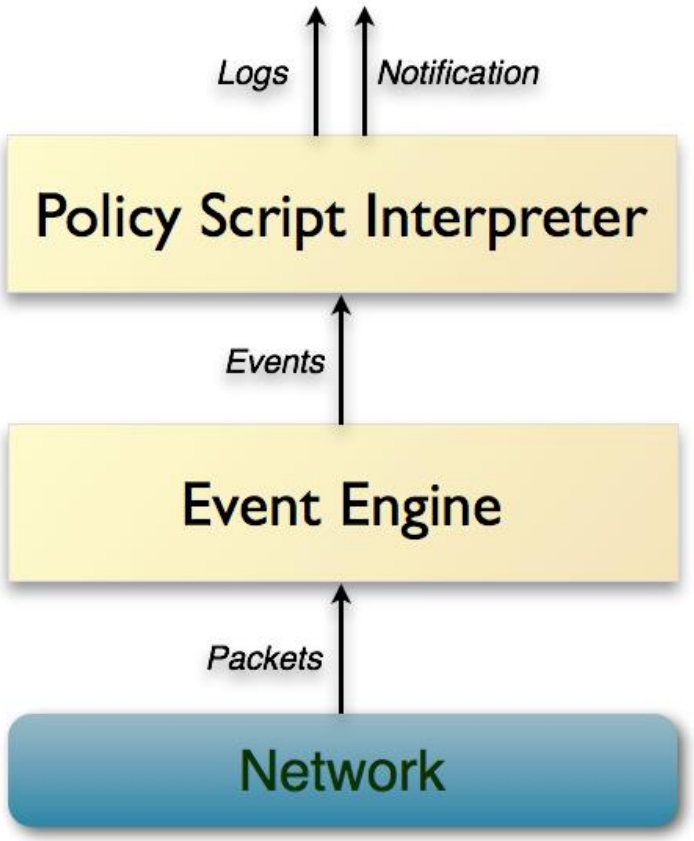

Hacknowledge

# Zeek in a nutshell

- Open source Network Security Monitoring tool
- Formerly known as Bro
- ECS format (made for Elastic)
- 50+ log files
- Highly customizable

- conn.log
- dns.log
- http.log
- files.log
- ftp.log
- ssl.log
- x509.log
- smtp.log
- ssh.log
- pe.log
- dhcp.log
- ntp.log
- SMB Logs (plus DCE-RPC, Kerberos, NTLM)
- irc.log
- rdp.log
- ldap.log and ldap_search.log
- traceroute.log
- tunnel.log
- dpd.log
- known_*.log and software.log
- weird.log and notice.log
- capture_loss.log and reporter.log

# Zeek architecture






Hacknowledge

# Zeek dashboards

elastic

Find apps, content, and more. ^/

Dashboard > Connections

Full screen | Share | Clone | Edit

**Network Logs** Panel filters

## General

Overview
Security Overview
ICS/IoT Security Overview - UNUSED
Connections
Actions and Results
Files
Executables
Software
Zeek Known Summary
Zeek Intelligence
Zeek Notices
Zeek Weird
Signatures
Suricata Alerts

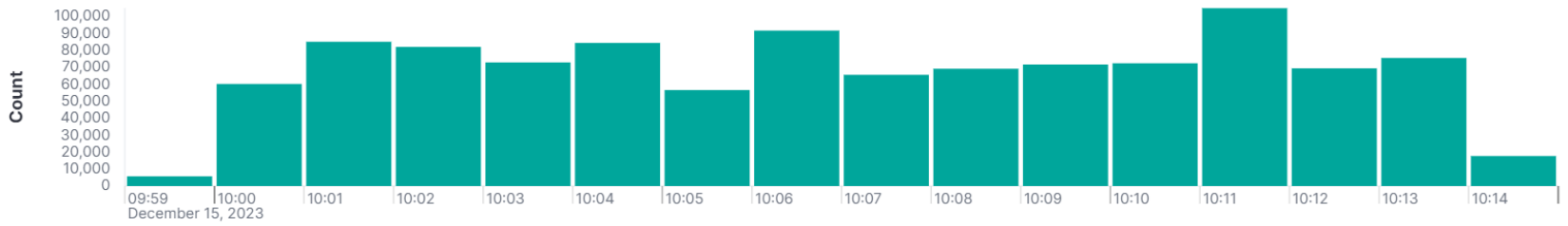
## Common Protocols

DCE/RPC ● DHCP ● DNS ● FTP / TFTP ● HTTP ● IRC ● Kerberos ● LDAP ● MQTT ● MySQL ● NTLM ● NTP ● OSPF ● QUIC ● RADIUS ● RDP ● RFB ● SIP ● SMB ● SMTP ● SNMP ● SSH ● SSL / X.509 Certificates ● STUN ● Syslog ● TDS / TDS RPC / TDS SQL ● Telnet / rlogin / rsh ● Tunnels

**Connections - Log Count**

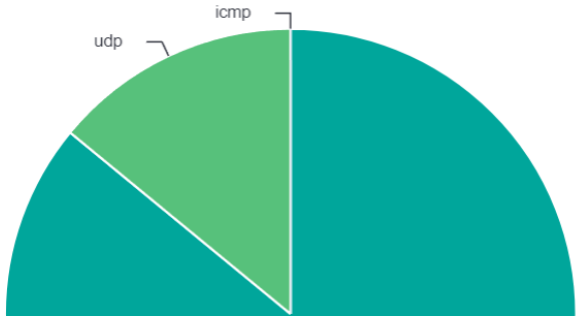
1,084,652

**Connections - Log Count Over Time**

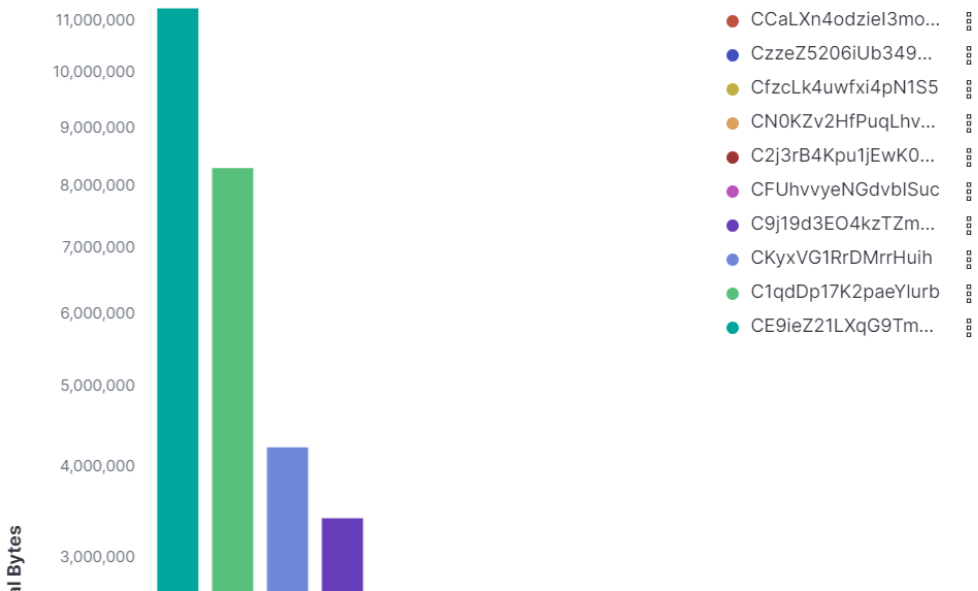



**Network Layer**

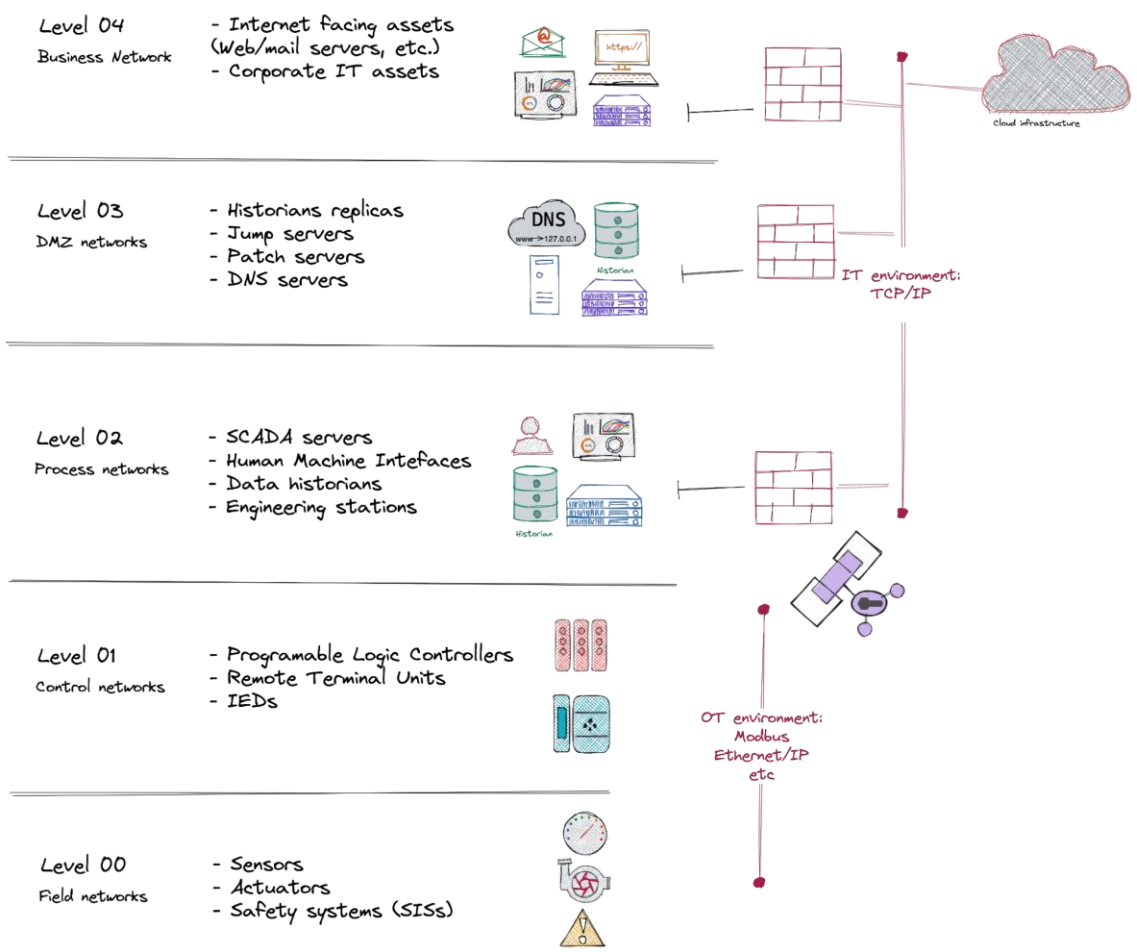
**Connections - Protocol**




**Connections - Top 10 - Total Bytes By Connection**



# ICS/IoT Environment






Hacknowledge

# Zeek for IoT ?

- We almost deploy Zeek by default when we setup new sensors
- We need an easy and effective tool to monitor IoT environments
- We keep the same workflow for « usual » deployments and IoT ones
- Zeek can monitor IoT protocols:

BACnet ● BSAP ● DNP3 ● EtherCAT ● EtherNet/IP ● GENISYS ● Modbus ● OPCUA Binary ● PROFINET ● S7comm ● Synchrophasor ● Best Guess

**Conclusion: Let’s use Zeek !**

# Zeek Modbus – Raw logs

Zeek Modbus | Filter your data using KQL syntax | Last 15 minutes | Refresh

Search field names

Filter by type 0

**Selected fields** 8

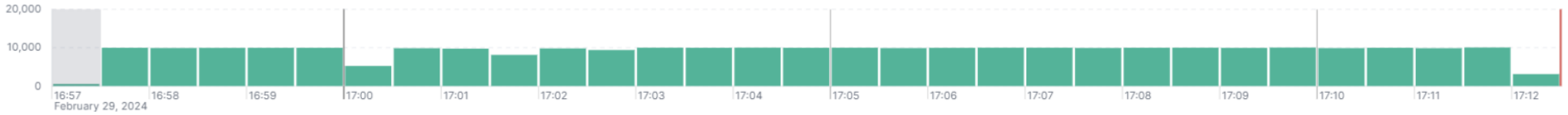
- source.address
- source.port
- destination.address
- destination.port
- event.action
- event.outcome
- zeek.modbus.function
- zeek.modbus.pdu_type

**Available fields** 39

**Popular**

- event.category
- event.dataset
- event.kind
- event.module
- event.type
- zeek.modbus.tid
- zeek.modbus.unit
- _id
- _index

**284,566** hits




Feb 29, 2024 @ 16:57:29.893 - Feb 29, 2024 @ 17:12:29.893 (interval: Auto - 30 seconds)

Documents | Field statistics BETA

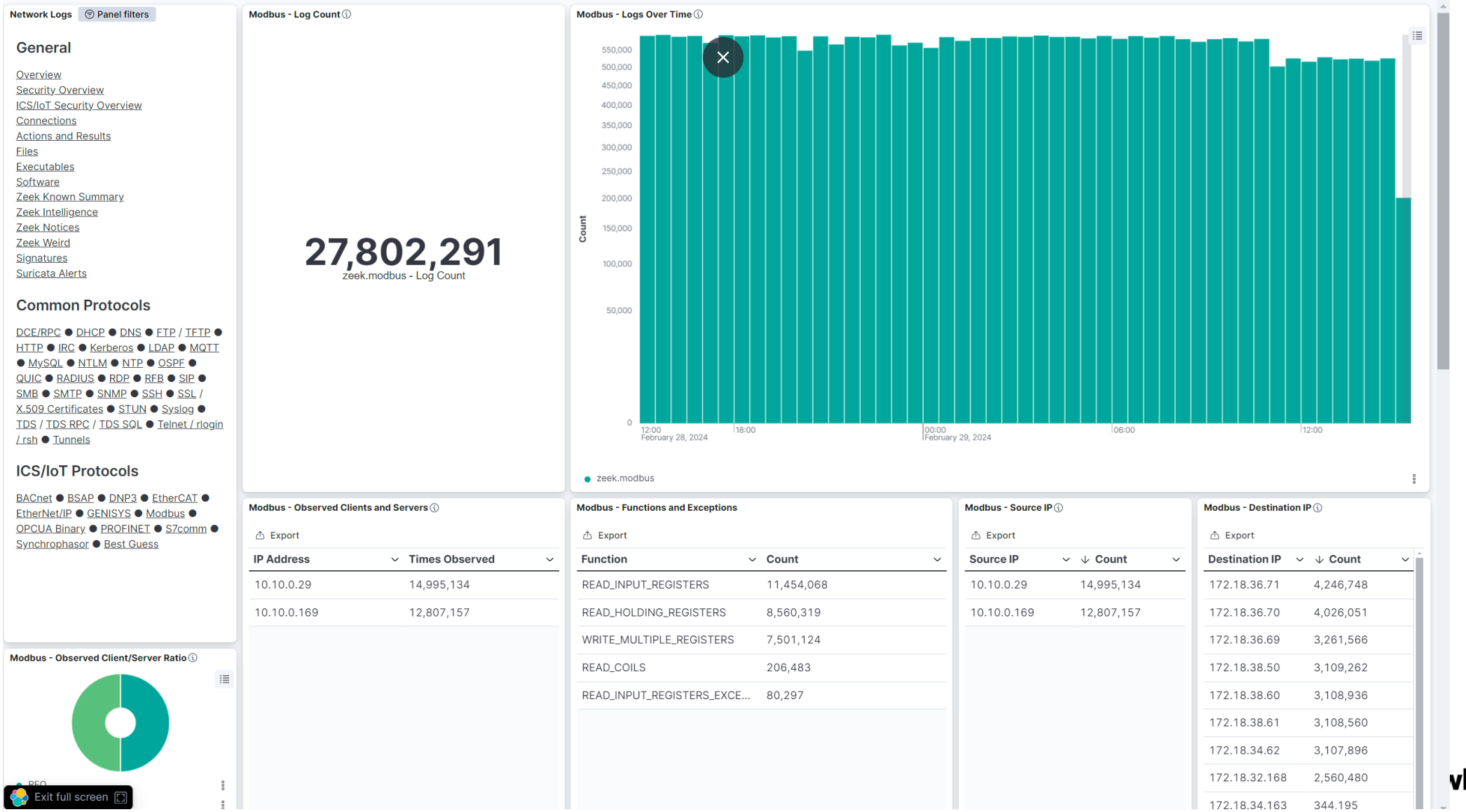
Columns | 1 field sorted

| @timestamp | source.address | source.port | destination.address | destination.port | event.action | event.outcome | zeek.modbus.functi... | zeek.modbus.pdu_t... |
|---|---|---|---|---|---|---|---|---|
| Feb 29, 2024 @ 17:12:09.436 | 10.10.0.29 | 58,324 | 172.18.34.62 | 502 | WRITE_MULTIPLE_REG... | success | WRITE_MULTIPLE_REG... | RESP |
| Feb 29, 2024 @ 17:12:09.436 | 10.10.0.29 | 58,324 | 172.18.34.62 | 502 | WRITE_MULTIPLE_REG... | success | WRITE_MULTIPLE_REG... | REQ |
| Feb 29, 2024 @ 17:12:09.435 | 10.10.0.29 | 58,324 | 172.18.34.62 | 502 | READ_HOLDING_REGIS... | success | READ_HOLDING_REGIS... | REQ |
| Feb 29, 2024 @ 17:12:09.435 | 10.10.0.29 | 58,324 | 172.18.34.62 | 502 | READ_HOLDING_REGIS... | success | READ_HOLDING_REGIS... | RESP |
| Feb 29, 2024 @ 17:12:09.432 | 10.10.0.169 | 49,772 | 172.18.36.71 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | RESP |
| Feb 29, 2024 @ 17:12:09.432 | 10.10.0.169 | 49,777 | 172.18.36.69 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | RESP |
| Feb 29, 2024 @ 17:12:09.432 | 10.10.0.169 | 49,777 | 172.18.36.69 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | REQ |
| Feb 29, 2024 @ 17:12:09.402 | 10.10.0.169 | 50,071 | 172.18.36.69 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | RESP |
| Feb 29, 2024 @ 17:12:09.402 | 10.10.0.169 | 50,071 | 172.18.36.69 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | REQ |
| Feb 29, 2024 @ 17:12:09.402 | 10.10.0.169 | 49,774 | 172.18.36.71 | 502 | READ_INPUT_REGISTERS | success | READ_INPUT_REGISTERS | RESP |
| Feb 29, 2024 @ 17:12:09.390 | 10.10.0.29 | 58,335 | 172.18.38.61 | 502 | WRITE_MULTIPLE_REG... | success | WRITE_MULTIPLE_REG... | RESP |
| Feb 29, 2024 @ 17:12:09.390 | 10.10.0.29 | 58,335 | 172.18.38.61 | 502 | WRITE_MULTIPLE_REG... | success | WRITE_MULTIPLE_REG... | REQ |
| Feb 29, 2024 @ 17:12:09.389 | 10.10.0.29 | 58,335 | 172.18.38.61 | 502 | READ_HOLDING_REGIS... | success | READ_HOLDING_REGIS... | RESP |
| Feb 29, 2024 @ 17:12:09.389 | 10.10.0.29 | 58,327 | 172.18.38.50 | 502 | WRITE_MULTIPLE_REG... | success | WRITE_MULTIPLE_REG... | RESP |
| Feb 29, 2024 @ 17:12:09.388 | 10.10.0.29 | 58,327 | 172.18.38.50 | 502 | READ_HOLDING_REGIS... | success | READ_HOLDING_REGIS... | RESP |



Hacknowledge

# Zeek Modbus - Dashboards



# Zeek Modbus – Transforms (CMDB style)

| source.address | destination.address.terms | zeek.modbus.function.terms |
|---|---|---|
| 10.10.0.169 | {<br>"172.18.38.45": 909404,<br>"192.168.102.28": 4967525,<br>"172.18.36.71": 112165384,<br>"172.18.34.163": 9086793,<br>"172.18.34.162": 4544017,<br>"172.18.36.70": 106036405,<br>"192.168.102.15": 1080441,<br>"172.18.36.69": 87357295,<br>"192.168.102.27": 4542429,<br>"192.168.102.25": 4542272<br>} | {<br>"READ_INPUT_REGISTERS_EXCEPTION": 421739,<br>"READ_HOLDING_REGISTERS": 24676643,<br>"READ_COILS": 5450719,<br>"READ_INPUT_REGISTERS": 305137345<br>} |
| 10.10.0.29 | {<br>"172.18.38.61": 75112682,<br>"172.18.38.50": 75005528,<br>"172.18.32.168": 73463305,<br>"172.18.38.60": 74897132,<br>"172.18.34.62": 75127206<br>} | {<br>"WRITE_MULTIPLE_REGISTERS": 186933741,<br>"READ_HOLDING_REGISTERS": 186672112<br>} |

# Zeek Modbus – Machine Learning

## Jobs

ml_zeek_modbushigh_count_by_destination_country

Security: Network - Looks for an unusually large spike in network activity to one destination country in the network logs. This could be due to unusually large amounts of reconnaissance or enumeration traffic. Data exfiltration activity may also produce such a surge in traffic to a destination country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.

security network

ml_zeek_modbushigh_count_network_denies

Security: Network - Looks for an unusually large spike in network traffic that was denied by network ACLs or firewall rules. Such a burst of denied traffic is usually either 1) a misconfigured application or firewall or 2) suspicious or malicious activity. Unsuccessful attempts at network transit, in order to connect to command-and-control (C2), or engage in data exfiltration, may produce a burst of failed connections. This could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.

security network

ml_zeek_modbushigh_count_network_events

Security: Network - Looks for an unusually large spike in network traffic. Such a burst of traffic, if not caused by a surge in business activity, can be due to suspicious or malicious activity. Large-scale data exfiltration may produce a burst of network traffic; this could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.

security network

ml_zeek_modbusrare_destination_country

Security: Network - looks for an unusual destination country name in the network logs. This can be due to initial access, persistence, command-and-control, or exfiltration activity. For example, when a user clicks on a link in a phishing email or opens a malicious document, a request may be sent to download and run a payload from a server in a country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.

security network

# Zeek Modbus – Anomaly Explorer




Hacknowledge

# Zeek Modbus – Anomalies

**Anomalies**

Severity: critical | Interval: Auto

| Time | Severity | Detector | Influenced by | Actual | Typical | Description | Actions |
|---|---|---|---|---|---|---|---|
| February 13th 2024 | 96 | high_count | destination.ip: 172.18.36.71<br>destination.ip: 172.18.36.70<br>destination.ip: 172.18.36.69<br>destination.ip: 172.18.34.62<br>destination.ip: 172.18.38.60<br>destination.ip: 172.18.38.61<br>destination.ip: 172.18.38.50<br>destination.ip: 172.18.32.168<br>source.ip: 10.10.0.169<br>source.ip: 10.10.0.29<br>show less | 293223 | 274234 | 1.1x higher | |
| February 23rd 2024 | 86 | high_count | destination.ip: 172.18.36.71<br>destination.ip: 172.18.36.70<br>destination.ip: 172.18.36.69<br>destination.ip: 172.18.38.60<br>destination.ip: 172.18.38.50<br>destination.ip: 172.18.38.61<br>destination.ip: 172.18.34.62<br>destination.ip: 172.18.32.168<br>source.ip: 10.10.0.169<br>source.ip: 10.10.0.29<br>show less | 294551 | 276416 | 1.1x higher | |

# Zeek with Elastic conclusions

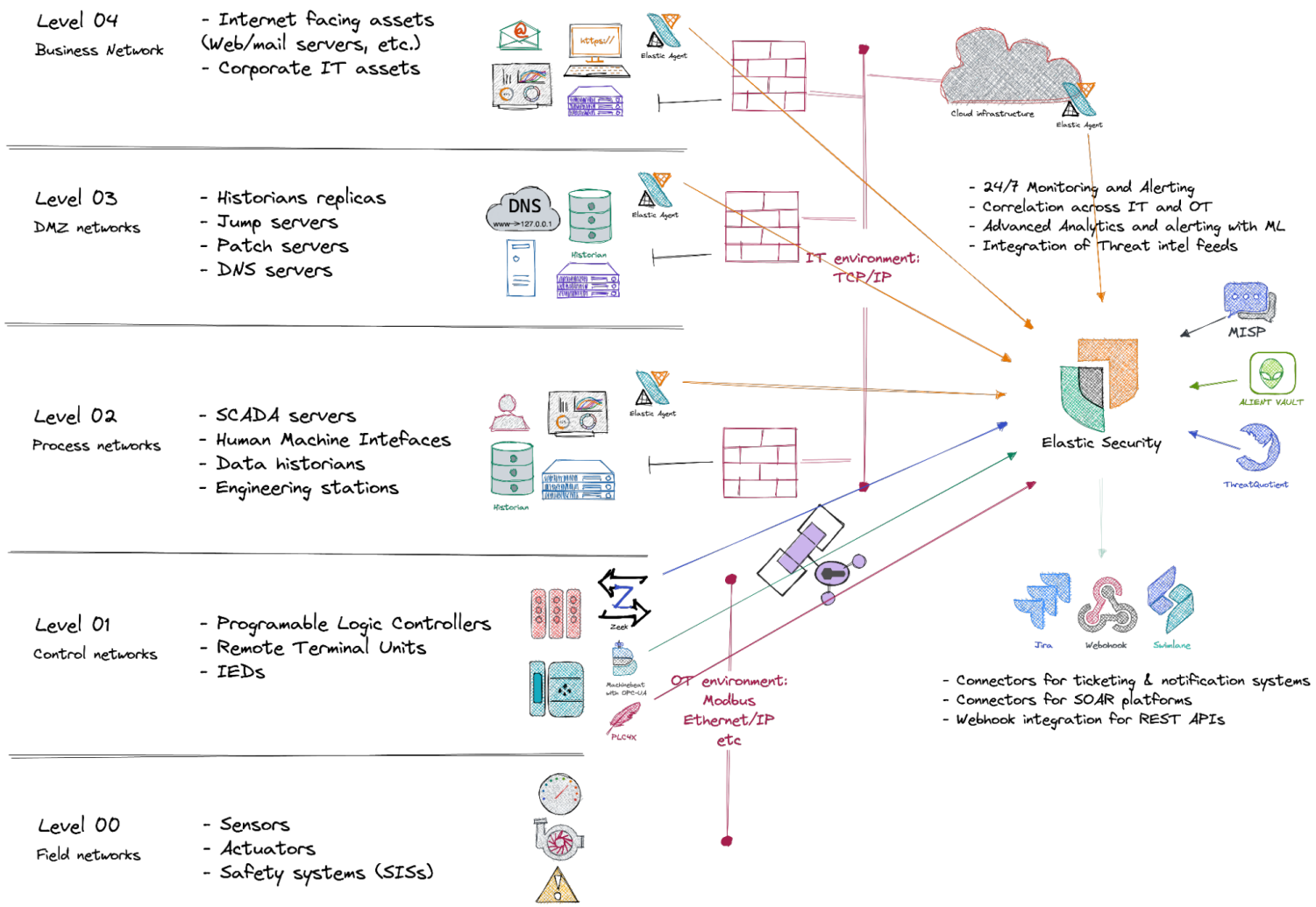
+ Pros

- Easy to setup
- No differenciation between IT and IoT environments
- Really flexible and customizable -> develop your own use-cases
- Good complementarity with the Elastic Agent for higher level machines

- Cons

- Huge amount of data to process/store
- Fully passive
- No real CMDB view

# ICS/IoT Security – Full Elastic coverage






Hacknowledge

# Thank you!
# Questions?

(See you soon)



Hacknowledge

Hacknowledge

**Hacknowledge SA**
Rue de Lausanne 35A
1110 Morges
Switzerland
+41 21 519 05 01

**Hacknowledge Lux SA**
9 Rue du Laboratoire
1911 Luxembourg
Luxembourg
+352 20 30 15 86

hacknowledge.com