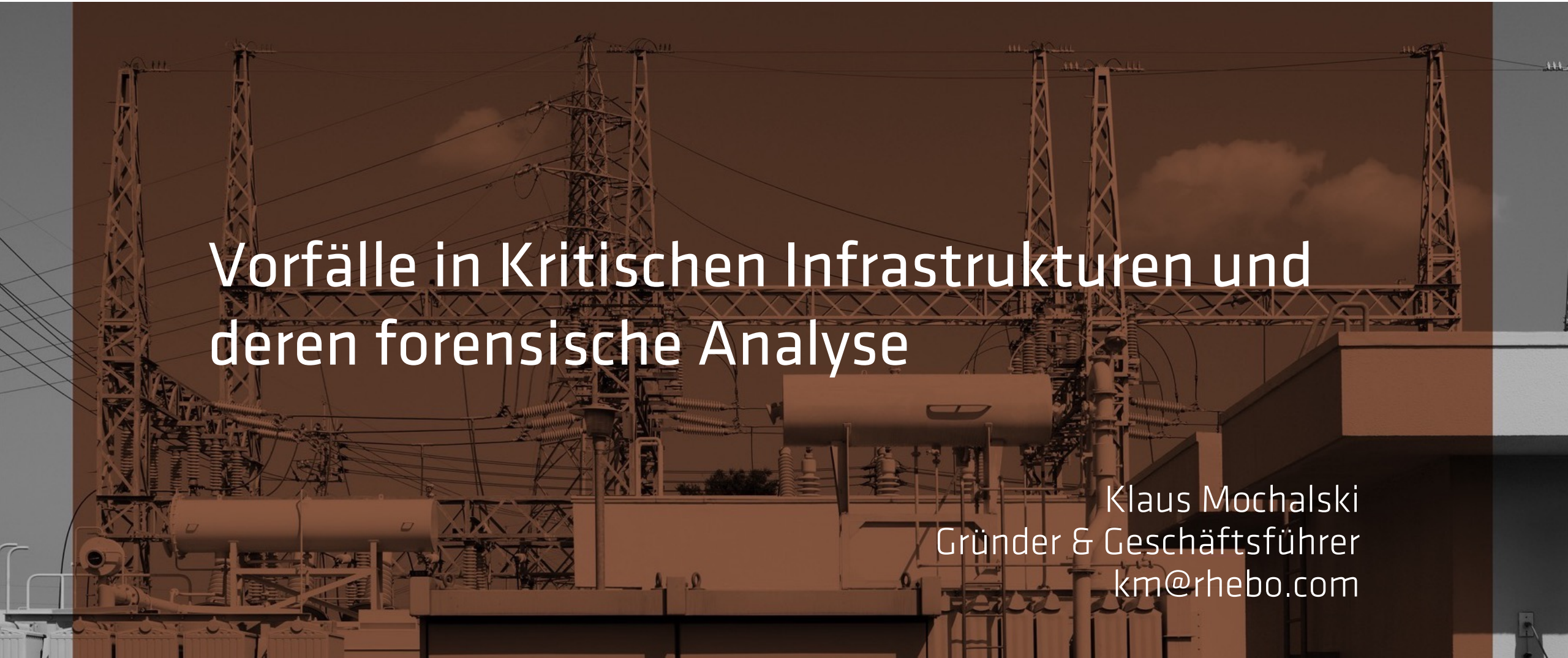
Rhebo

a Landis+Gyr company



Vorfälle in Kritischen Infrastrukturen und deren forensische Analyse

Klaus Mochalski
Gründer & Geschäftsführer
km@rhebo.com

Rhebo schafft Cybersicherheit & Verfügbarkeit für OT & IoT in Industrie & Kritischen Infrastrukturen.

2014 gegründet in Leipzig

~ 50k Installationen weltweit

~ 33% des deutsche Stromnetzes abgesichert

seit 2021 Teil von Landis+Gyr

Wissen Sie, wer sich in Ihrer Infrastruktur herumtreibt?

64 % unnötige Dienste oder Zombie-Geräte

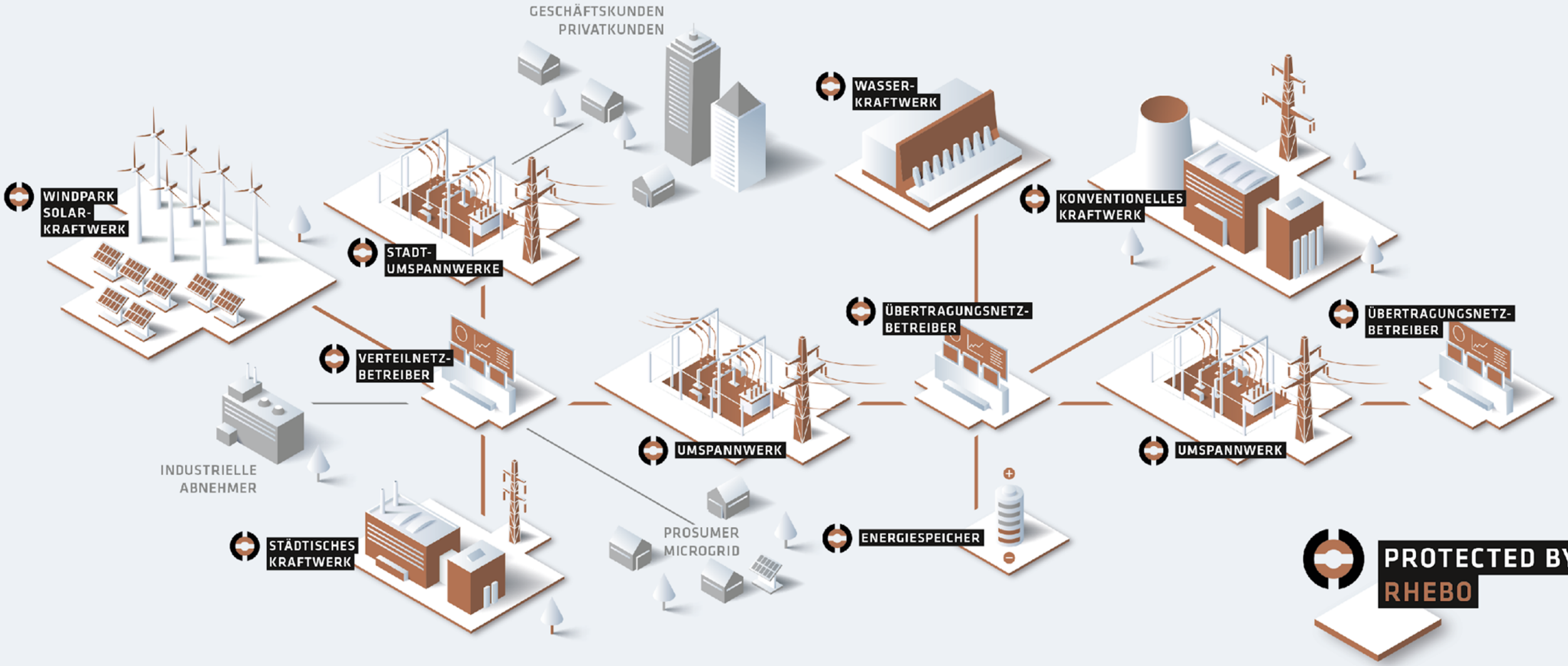
53 % unsichere Authentifizierungsmethoden

51 % mögliche Malware-Infektionen

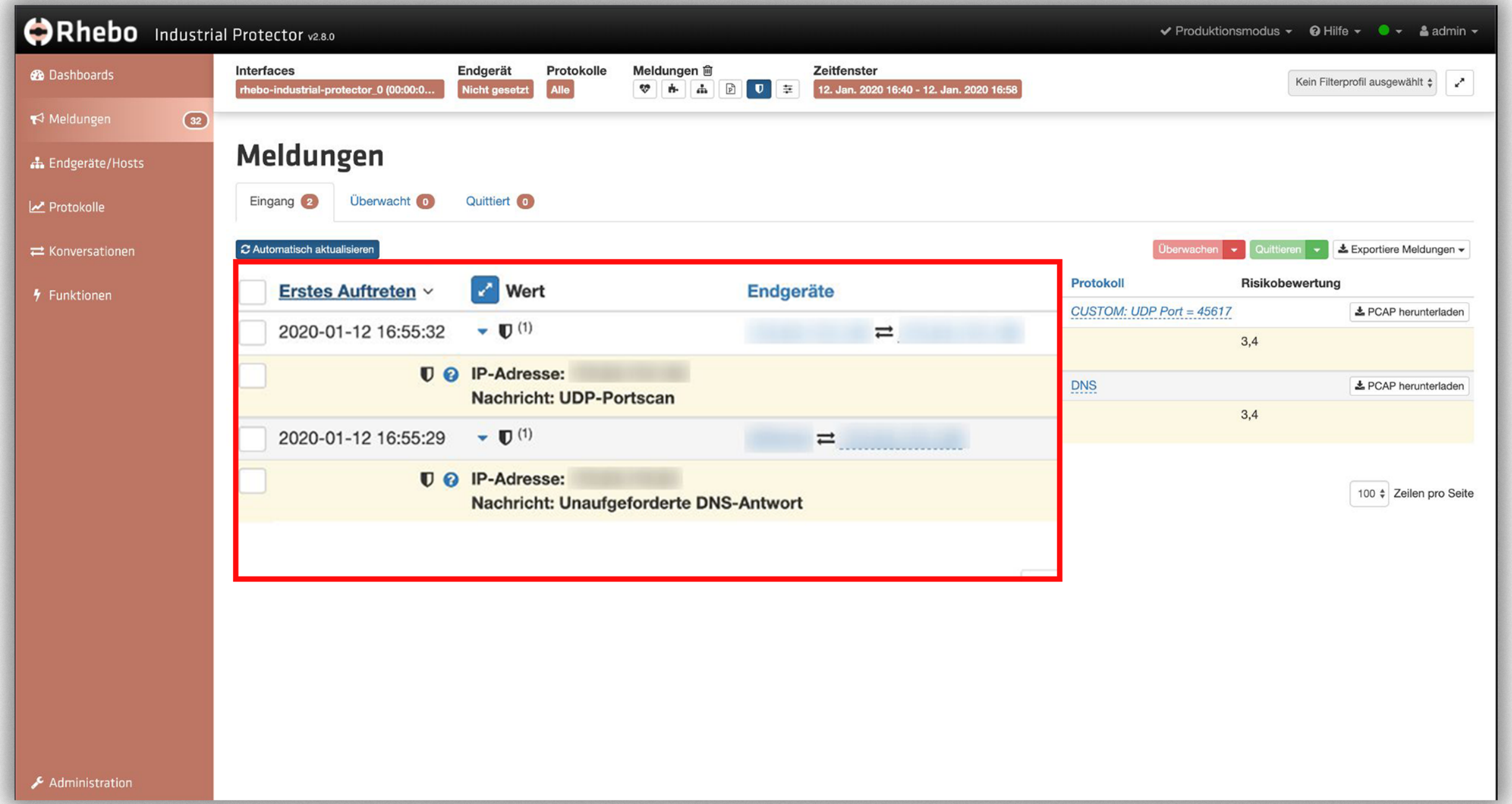
44 % anfällige Systeme, Geräte, Anwendungen

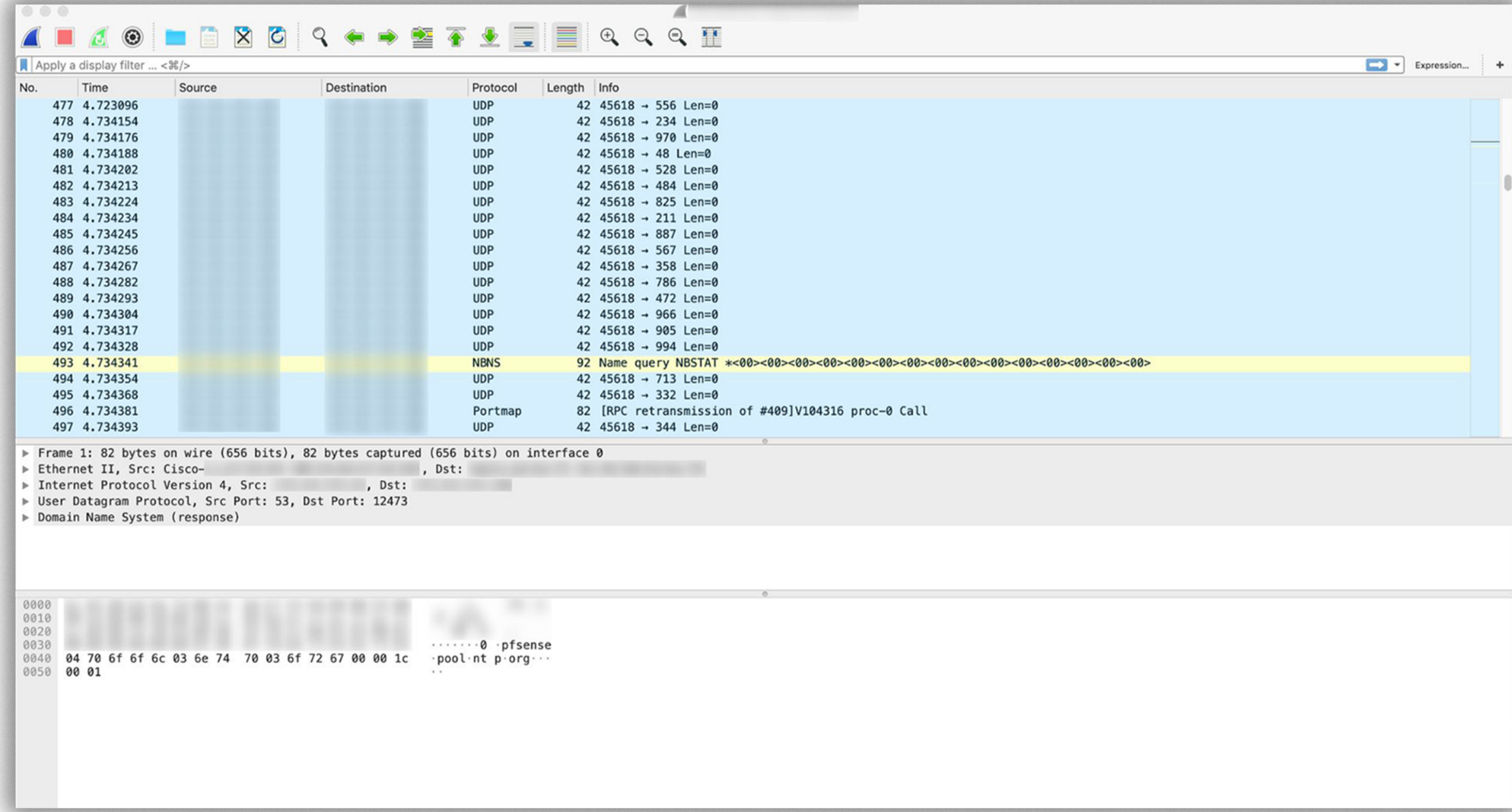
31 % Internetkommunikation

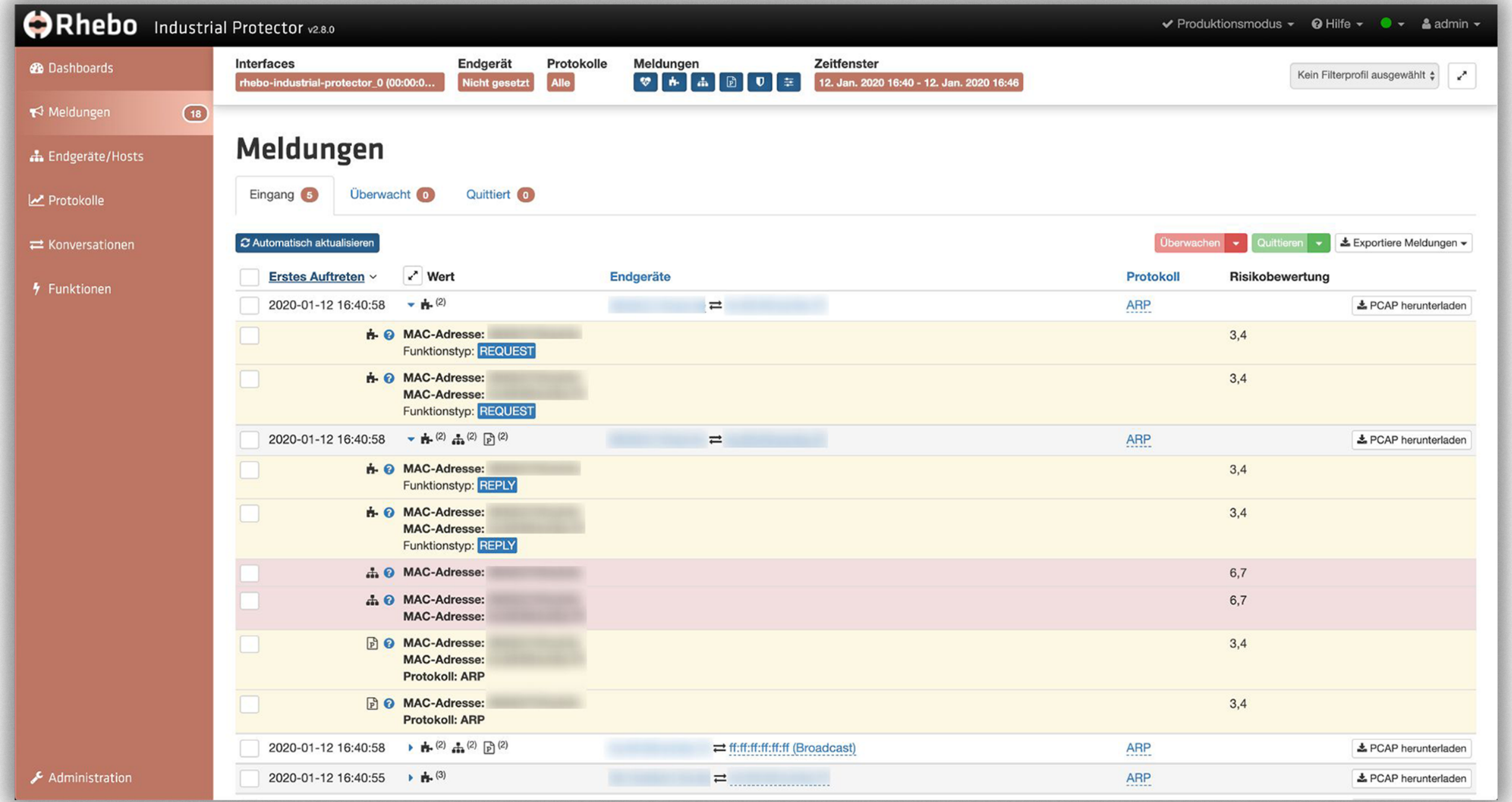
Beispiel Stromnetz: Sicherheit von der Leitwarte bis zum Umspannwerk

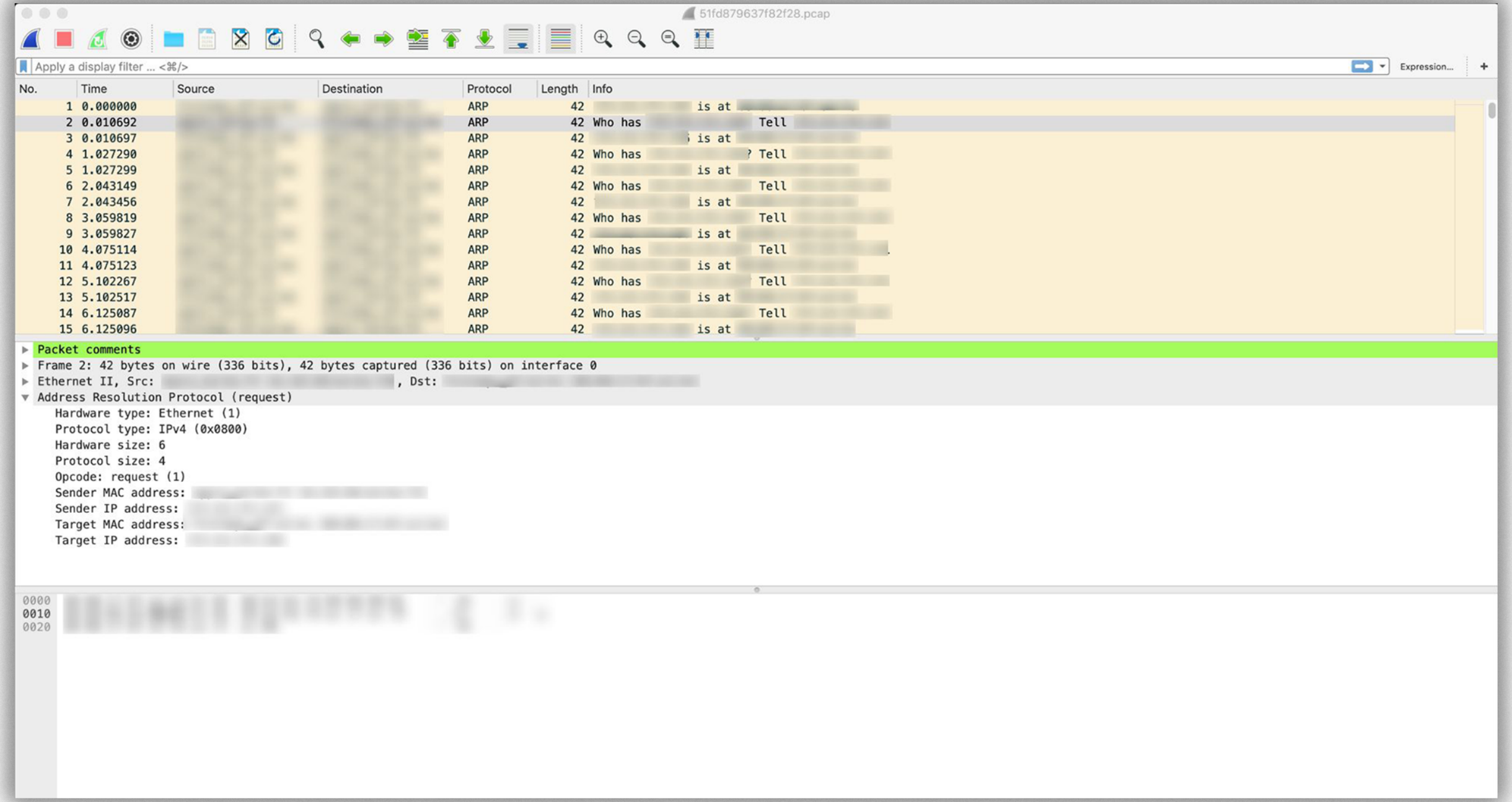


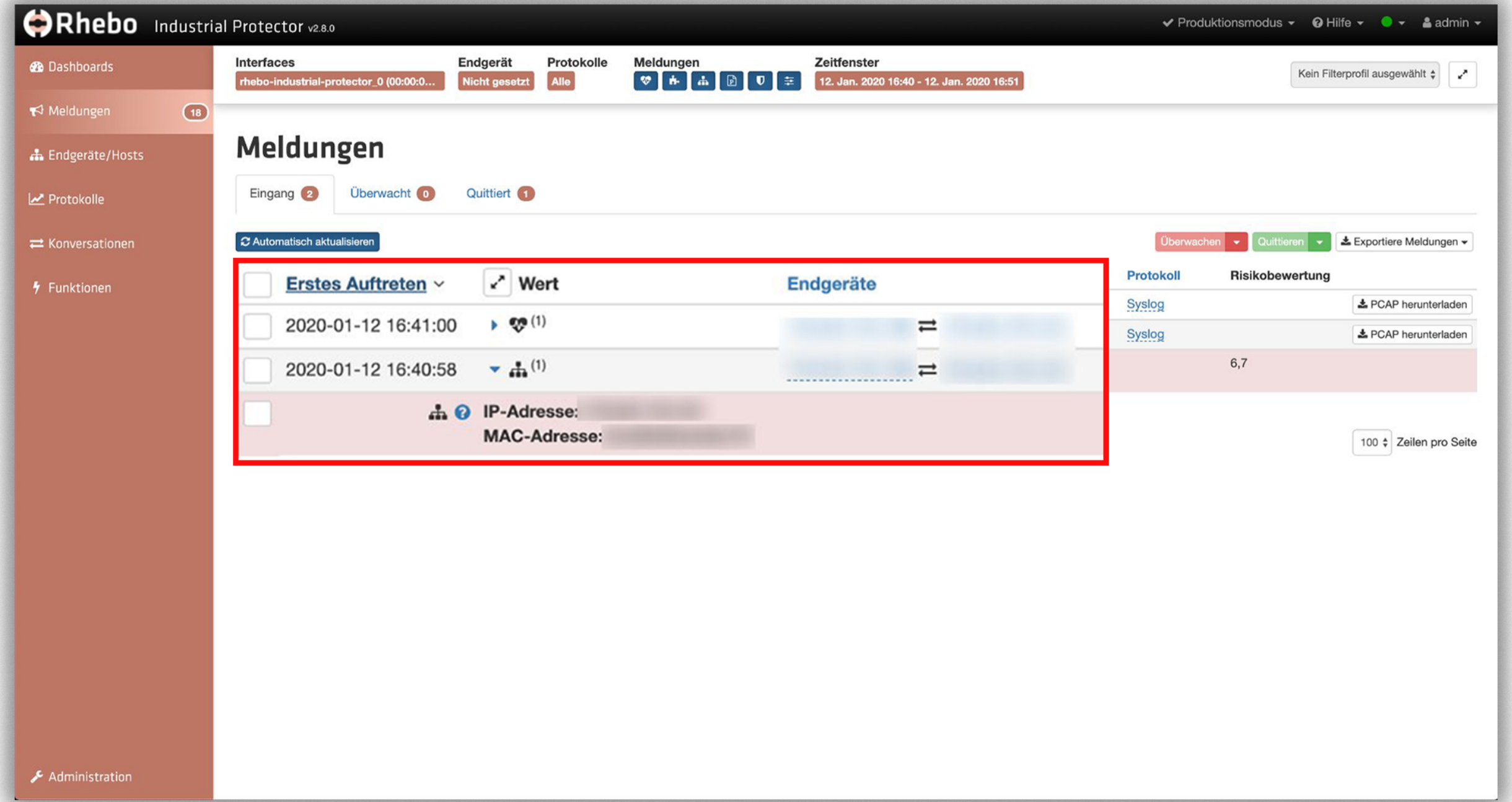
Forensische Analyse eines typischen mehrstufigen Cyberangriffs

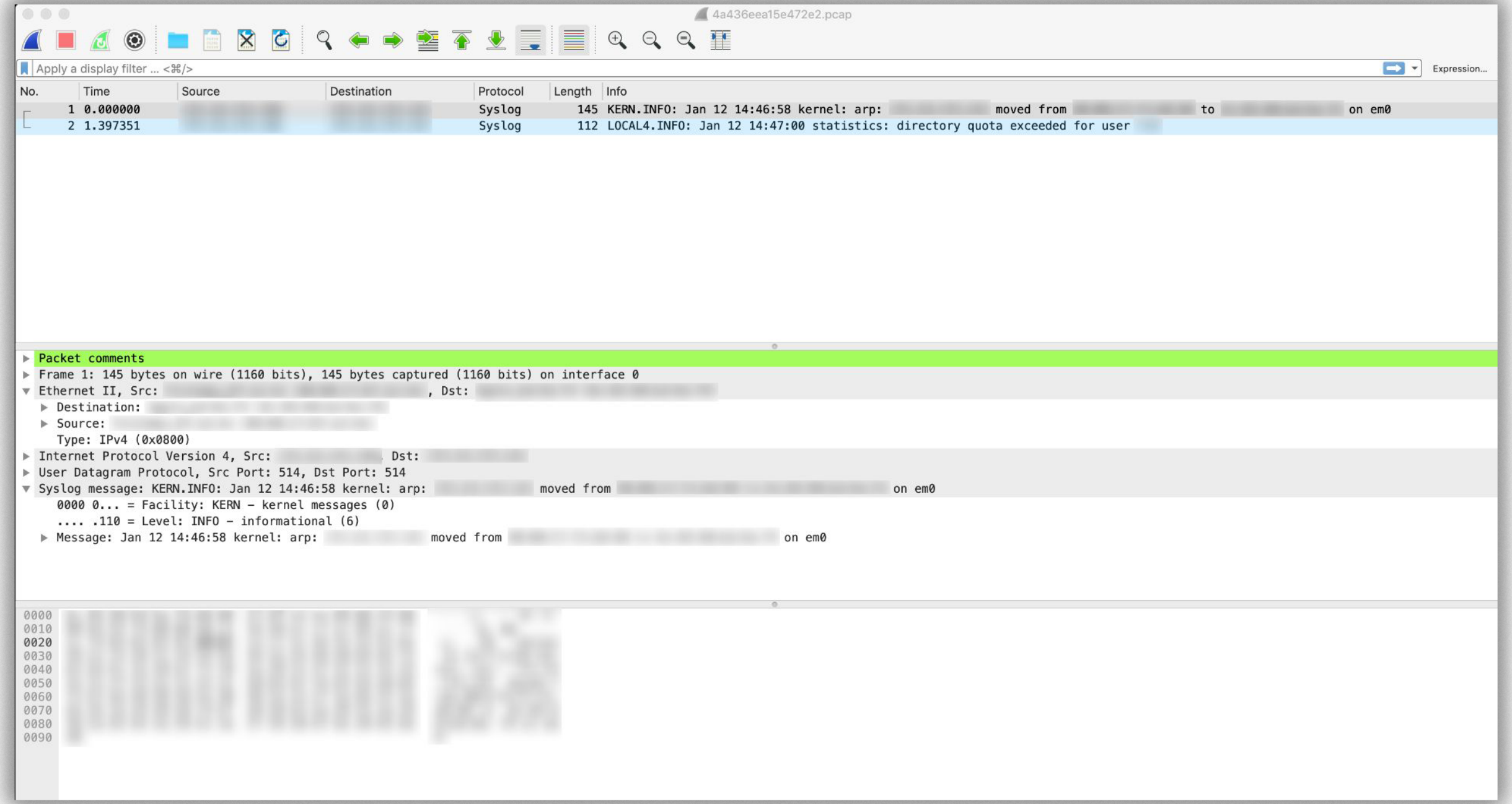

Rhebo Industrial Protector v2.8.0
Produktionsmodus
Hilfe
admin
Dashboards
Meldungen 32
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
Interfaces
rhebo-industrial-protector_0 (00:00:0...
Endgerät
Nicht gesetzt
Protokolle
Alle
Meldungen
Zeitfenster
12. Jan. 2020 16:40 - 12. Jan. 2020 16:58
Kein Filterprofil ausgewählt
Meldungen
Eingang 2
Überwacht 0
Quittiert 0
Automatisch aktualisieren
Überwachen
Quittieren
Exportiere Meldungen
Erstes Auftreten
Wert
Endgeräte
Protokoll
Risikobewertung
2020-01-12 16:55:32
(1)
CUSTOM: UDP Port = 45617
PCAP herunterladen
3,4
IP-Adresse:
Nachricht: UDP-Portscan
DNS
PCAP herunterladen
2020-01-12 16:55:29
(1)
3,4
IP-Adresse:
Nachricht: Unaufgeforderte DNS-Antwort
100
Zeilen pro Seite

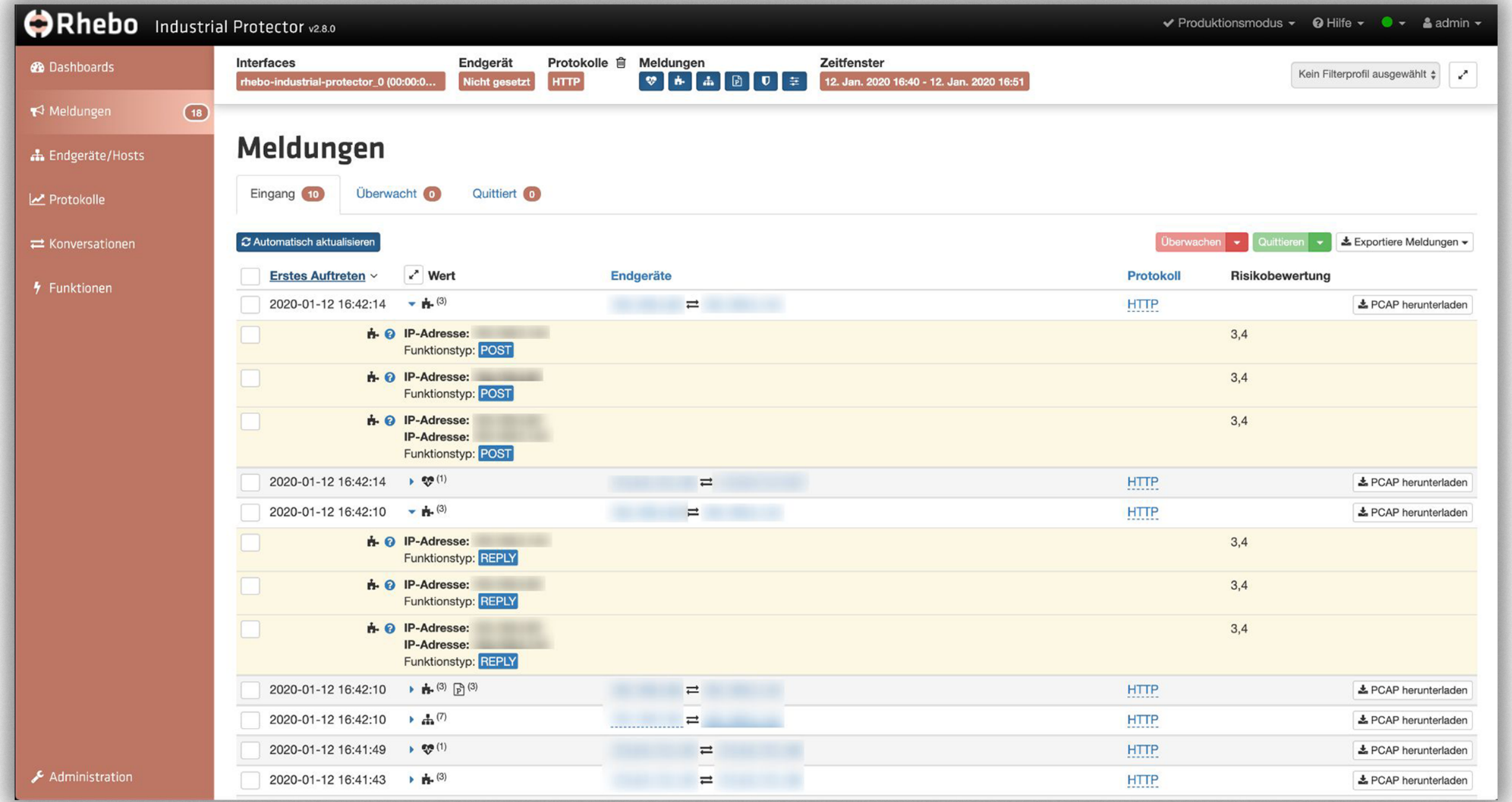

Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
477 4.723096 UDP 42 45618 → 556 Len=0
478 4.734154 UDP 42 45618 → 234 Len=0
479 4.734176 UDP 42 45618 → 970 Len=0
480 4.734188 UDP 42 45618 → 48 Len=0
481 4.734202 UDP 42 45618 → 528 Len=0
482 4.734213 UDP 42 45618 → 484 Len=0
483 4.734224 UDP 42 45618 → 825 Len=0
484 4.734234 UDP 42 45618 → 211 Len=0
485 4.734245 UDP 42 45618 → 887 Len=0
486 4.734256 UDP 42 45618 → 567 Len=0
487 4.734267 UDP 42 45618 → 358 Len=0
488 4.734282 UDP 42 45618 → 786 Len=0
489 4.734293 UDP 42 45618 → 472 Len=0
490 4.734304 UDP 42 45618 → 966 Len=0
491 4.734317 UDP 42 45618 → 905 Len=0
492 4.734328 UDP 42 45618 → 994 Len=0
493 4.734341 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
494 4.734354 UDP 42 45618 → 713 Len=0
495 4.734368 UDP 42 45618 → 332 Len=0
496 4.734381 Portmap 82 [RPC retransmission of #409]V104316 proc-0 Call
497 4.734393 UDP 42 45618 → 344 Len=0
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: Cisco-
, Dst:
Internet Protocol Version 4, Src:
, Dst:
User Datagram Protocol, Src Port: 53, Dst Port: 12473
Domain Name System (response)
0000
0010
0020
0030 ·····0 ·pfsense
0040 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 1c ·pool·nt p·org···
0050 00 01 ··

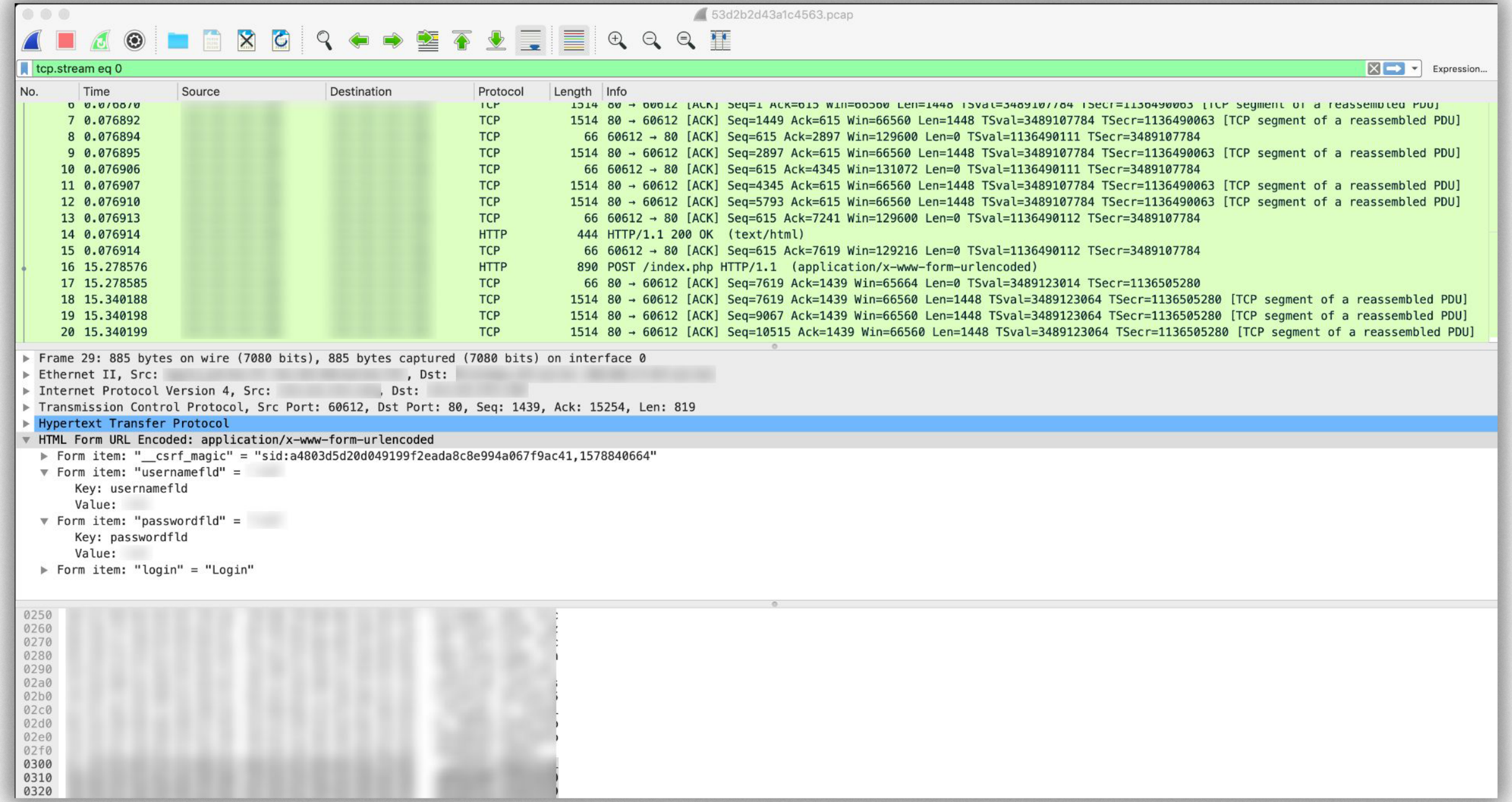

Rhebo Industrial Protector v2.8.0
Produktionsmodus
Hilfe
admin
Dashboards
Meldungen 18
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
Interfaces
rhebo-industrial-protector_0 (00:00:0...
Endgerät
Nicht gesetzt
Protokolle
Alle
Meldungen
Zeitfenster
12. Jan. 2020 16:40 - 12. Jan. 2020 16:46
Kein Filterprofil ausgewählt
Meldungen
Eingang 5
Überwacht 0
Quittiert 0
Automatisch aktualisieren
Überwachen
Quittieren
Exportiere Meldungen
Erstes Auftreten
Wert
Endgeräte
Protokoll
Risikobewertung
2020-01-12 16:40:58
ARP
PCAP herunterladen
MAC-Adresse:
Funktionstyp: REQUEST
3,4
MAC-Adresse:
MAC-Adresse:
Funktionstyp: REQUEST
3,4
2020-01-12 16:40:58
ARP
PCAP herunterladen
MAC-Adresse:
Funktionstyp: REPLY
3,4
MAC-Adresse:
MAC-Adresse:
Funktionstyp: REPLY
3,4
MAC-Adresse:
6,7
MAC-Adresse:
MAC-Adresse:
6,7
MAC-Adresse:
MAC-Adresse:
Protokoll: ARP
3,4
MAC-Adresse:
Protokoll: ARP
3,4
2020-01-12 16:40:58
ff:ff:ff:ff:ff:ff (Broadcast)
ARP
PCAP herunterladen
2020-01-12 16:40:55
ARP
PCAP herunterladen

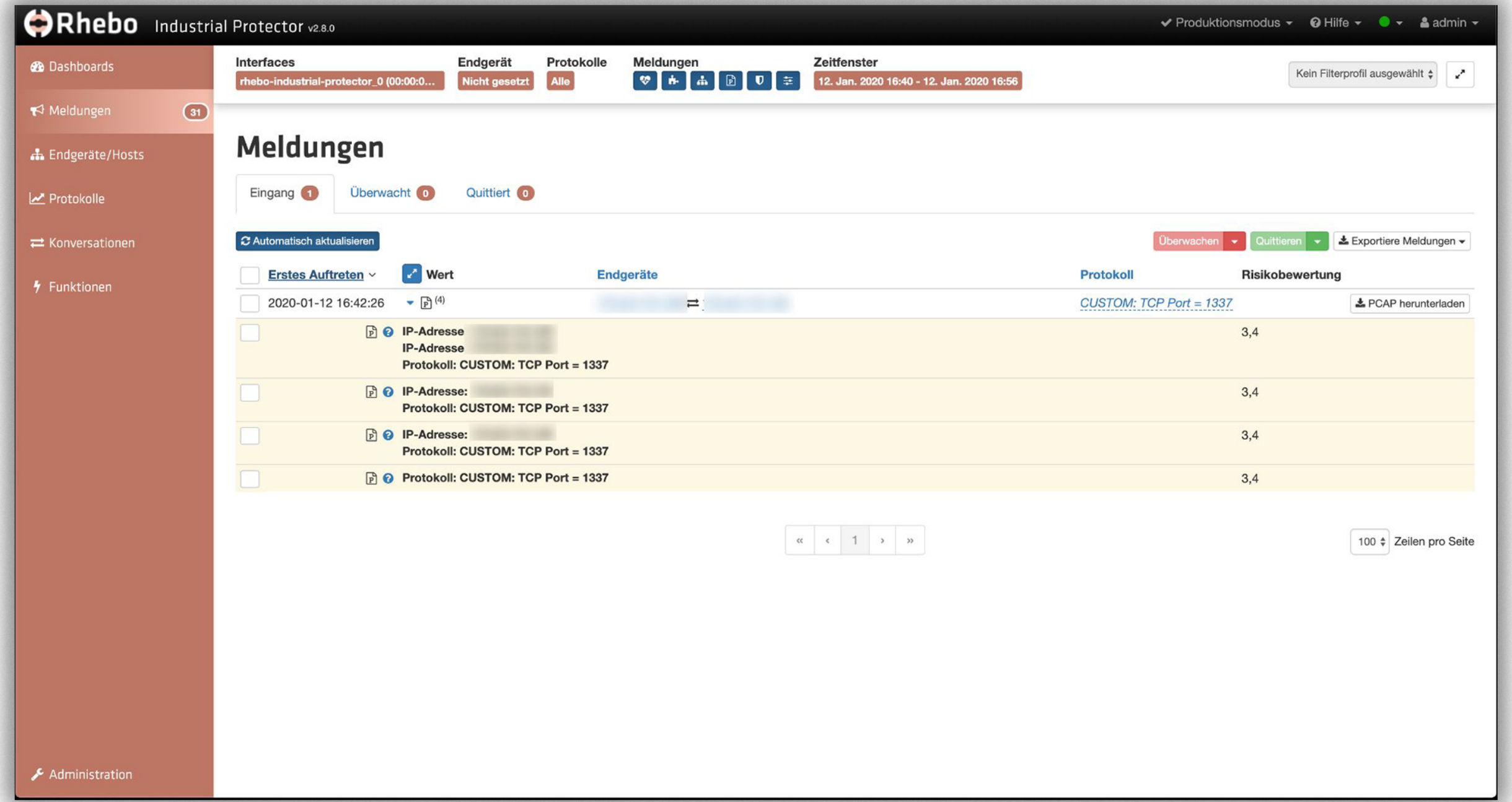

51fd879637f82f28.pcap
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 ARP 42 is at
2 0.010692 ARP 42 Who has Tell
3 0.010697 ARP 42 is at
4 1.027290 ARP 42 Who has Tell
5 1.027299 ARP 42 is at
6 2.043149 ARP 42 Who has Tell
7 2.043456 ARP 42 is at
8 3.059819 ARP 42 Who has Tell
9 3.059827 ARP 42 is at
10 4.075114 ARP 42 Who has Tell
11 4.075123 ARP 42 is at
12 5.102267 ARP 42 Who has Tell
13 5.102517 ARP 42 is at
14 6.125087 ARP 42 Who has Tell
15 6.125096 ARP 42 is at
Packet comments
Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: , Dst:
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address:
Sender IP address:
Target MAC address:
Target IP address:
0000
0010
0020


Rhebo Industrial Protector v2.8.0
Produktionsmodus
Hilfe
admin
Dashboards
Meldungen 18
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
Interfaces
rhebo-industrial-protector_0 (00:00:0...
Endgerät
Nicht gesetzt
Protokolle
Alle
Meldungen
Zeitfenster
12. Jan. 2020 16:40 - 12. Jan. 2020 16:51
Kein Filterprofil ausgewählt
Meldungen
Eingang 2
Überwacht 0
Quittiert 1
Automatisch aktualisieren
Überwachen
Quittieren
Exportiere Meldungen
Erstes Auftreten
Wert
Endgeräte
Protokoll
Risikobewertung
2020-01-12 16:41:00
(1)
Syslog
PCAP herunterladen
2020-01-12 16:40:58
(1)
Syslog
PCAP herunterladen
6,7
IP-Adresse:
MAC-Adresse:
100
Zeilen pro Seite


4a436eea15e472e2.pcap
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 Syslog 145 KERN.INFO: Jan 12 14:46:58 kernel: arp: moved from to on em0
2 1.397351 Syslog 112 LOCAL4.INFO: Jan 12 14:47:00 statistics: directory quota exceeded for user
Packet comments
Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Ethernet II, Src: , Dst:
Destination:
Source:
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Dst:
User Datagram Protocol, Src Port: 514, Dst Port: 514
Syslog message: KERN.INFO: Jan 12 14:46:58 kernel: arp: moved from on em0
0000 0... = Facility: KERN - kernel messages (0)
.... .110 = Level: INFO - informational (6)
Message: Jan 12 14:46:58 kernel: arp: moved from on em0
0000
0010
0020
0030
0040
0050
0060
0070
0080
0090


Rhebo Industrial Protector v2.8.0
Produktionsmodus
Hilfe
admin
Dashboards
Meldungen 18
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
Interfaces
rhebo-industrial-protector_0 (00:00:0...
Endgerät
Nicht gesetzt
Protokolle
HTTP
Meldungen
Zeitfenster
12. Jan. 2020 16:40 - 12. Jan. 2020 16:51
Kein Filterprofil ausgewählt
Meldungen
Eingang 10
Überwacht 0
Quittiert 0
Automatisch aktualisieren
Überwachen
Quittieren
Exportiere Meldungen
Erstes Auftreten
Wert
Endgeräte
Protokoll
Risikobewertung
2020-01-12 16:42:14
HTTP
PCAP herunterladen
IP-Adresse:
Funktionstyp: POST
3,4
2020-01-12 16:42:10
Funktionstyp: REPLY
2020-01-12 16:42:14
2020-01-12 16:42:10
2020-01-12 16:41:49
2020-01-12 16:41:43


53d2b2d43a1c4563.pcap
tcp.stream eq 0
Expression...
No. Time Source Destination Protocol Length Info
6 0.076870 TCP 1514 80 → 60612 [ACK] Seq=1 Ack=615 Win=66560 Len=1448 TSval=3489107784 TSecr=1136490063 [TCP segment of a reassembled PDU]
7 0.076892 TCP 1514 80 → 60612 [ACK] Seq=1449 Ack=615 Win=66560 Len=1448 TSval=3489107784 TSecr=1136490063 [TCP segment of a reassembled PDU]
8 0.076894 TCP 66 60612 → 80 [ACK] Seq=615 Ack=2897 Win=129600 Len=0 TSval=1136490111 TSecr=3489107784
9 0.076895 TCP 1514 80 → 60612 [ACK] Seq=2897 Ack=615 Win=66560 Len=1448 TSval=3489107784 TSecr=1136490063 [TCP segment of a reassembled PDU]
10 0.076906 TCP 66 60612 → 80 [ACK] Seq=615 Ack=4345 Win=131072 Len=0 TSval=1136490111 TSecr=3489107784
11 0.076907 TCP 1514 80 → 60612 [ACK] Seq=4345 Ack=615 Win=66560 Len=1448 TSval=3489107784 TSecr=1136490063 [TCP segment of a reassembled PDU]
12 0.076910 TCP 1514 80 → 60612 [ACK] Seq=5793 Ack=615 Win=66560 Len=1448 TSval=3489107784 TSecr=1136490063 [TCP segment of a reassembled PDU]
13 0.076913 TCP 66 60612 → 80 [ACK] Seq=615 Ack=7241 Win=129600 Len=0 TSval=1136490112 TSecr=3489107784
14 0.076914 HTTP 444 HTTP/1.1 200 OK (text/html)
15 0.076914 TCP 66 60612 → 80 [ACK] Seq=615 Ack=7619 Win=129216 Len=0 TSval=1136490112 TSecr=3489107784
16 15.278576 HTTP 890 POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
17 15.278585 TCP 66 80 → 60612 [ACK] Seq=7619 Ack=1439 Win=65664 Len=0 TSval=3489123014 TSecr=1136505280
18 15.340188 TCP 1514 80 → 60612 [ACK] Seq=7619 Ack=1439 Win=66560 Len=1448 TSval=3489123064 TSecr=1136505280 [TCP segment of a reassembled PDU]
19 15.340198 TCP 1514 80 → 60612 [ACK] Seq=9067 Ack=1439 Win=66560 Len=1448 TSval=3489123064 TSecr=1136505280 [TCP segment of a reassembled PDU]
20 15.340199 TCP 1514 80 → 60612 [ACK] Seq=10515 Ack=1439 Win=66560 Len=1448 TSval=3489123064 TSecr=1136505280 [TCP segment of a reassembled PDU]
Frame 29: 885 bytes on wire (7080 bits), 885 bytes captured (7080 bits) on interface 0
Ethernet II, Src: , Dst:
Internet Protocol Version 4, Src: , Dst:
Transmission Control Protocol, Src Port: 60612, Dst Port: 80, Seq: 1439, Ack: 15254, Len: 819
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "__csrf_magic" = "sid:a4803d5d20d049199f2eada8c8e994a067f9ac41,1578840664"
Form item: "usernamefld" =
Key: usernamefld
Value:
Form item: "passwordfld" =
Key: passwordfld
Value:
Form item: "login" = "Login"
0250
0260
0270
0280
0290
02a0
02b0
02c0
02d0
02e0
02f0
0300
0310
0320


Rhebo Industrial Protector v2.8.0
Produktionsmodus
Hilfe
admin
Dashboards
Meldungen 31
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
Interfaces
rhebo-industrial-protector_0 (00:00:0...
Endgerät
Nicht gesetzt
Protokolle
Alle
Meldungen
Zeitfenster
12. Jan. 2020 16:40 - 12. Jan. 2020 16:56
Kein Filterprofil ausgewählt
Meldungen
Eingang 1
Überwacht 0
Quittiert 0
Automatisch aktualisieren
Überwachen
Quittieren
Exportiere Meldungen
Erstes Auftreten
Wert
Endgeräte
Protokoll
Risikobewertung
2020-01-12 16:42:26
(4)
CUSTOM: TCP Port = 1337
PCAP herunterladen
IP-Adresse
IP-Adresse
Protokoll: CUSTOM: TCP Port = 1337
3,4
IP-Adresse:
Protokoll: CUSTOM: TCP Port = 1337
3,4
IP-Adresse:
Protokoll: CUSTOM: TCP Port = 1337
3,4
Protokoll: CUSTOM: TCP Port = 1337
3,4
« ‹ 1 › »
100 Zeilen pro Seite

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 7276b8cfba1825ff.pcap

```
whoami
root
pfSsh.php playback enableallowallwan

Starting the pfSense developer shell........

..Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
..Reloading the filter configuration...Configuring firewall......done.
```

26 client pkts, 2 server pkts, 3 turns.

Rhebo

a Landis+Gyr company

WISSEN SIE, WER SICH IN IHRER INFRASTRUKTUR HERUMTREIBT?

Klaus Mochalski

Gründer & Geschäftsführer

km@rhebo.com

+49 151 27612501

SYSKRON

Thesen zur Diskussion

Rhebo

- IT-Sicherheit ist eine Aufgabe des TÄGLICHEN Betriebs.
- Einzelmaßnahmen sind nutzlos.
- Systematisches Vorgehen ist der Schlüssel zum Erfolg (z.B. NIST CSF: Identify, Protect, Detect, Respond, Recover).
- 9 von 10 Störungen haben NICHTS mit Cybersecurity zu tun.
- Was man nicht kennt, kann man nicht schützen.
- Künstliche Intelligenz und Machine Learning haben in Industrieanlagen nichts zu suchen.