Rhebo

Industrial Network Continuity

Dr. Frank Stummer
Staatliche Berufschule Bayreuth
09.04.2019

# Cybersicherheit und Verfügbarkeit in ICS
# Herausforderungen der zunehmenden Vernetzung in der Industrie


DIGITAL FORENSICS

Rhebo
Industrial Network Continuity

VIZZLO

**Vernetzte Produktion**

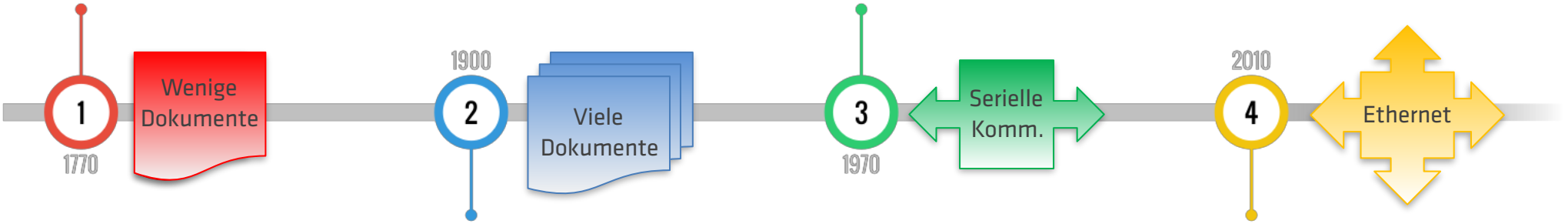
Standards

Reale Beispiele

# Kommunikationstechnologie in Industrie 4.0

**Mechanisierung**
- Dampfmaschine
- Webstuhl
- Treibriemenanlage

**Automatisierung**
- Computer
- Roboter
- Sensoren




**Massenproduktion**
- Fließband
- Elekrizität
- Verkehrsmöglichkeiten

**Industrie 4.0**
- Cyber-Physikalische Systeme
- Internet of Things
- Internet of Services

# Vorteile und Herausforderungen der Industrie 4.0


**Industrie 4.0**

- Cyber-Physikalische Systeme
- Internet of Things
- Internet of Services

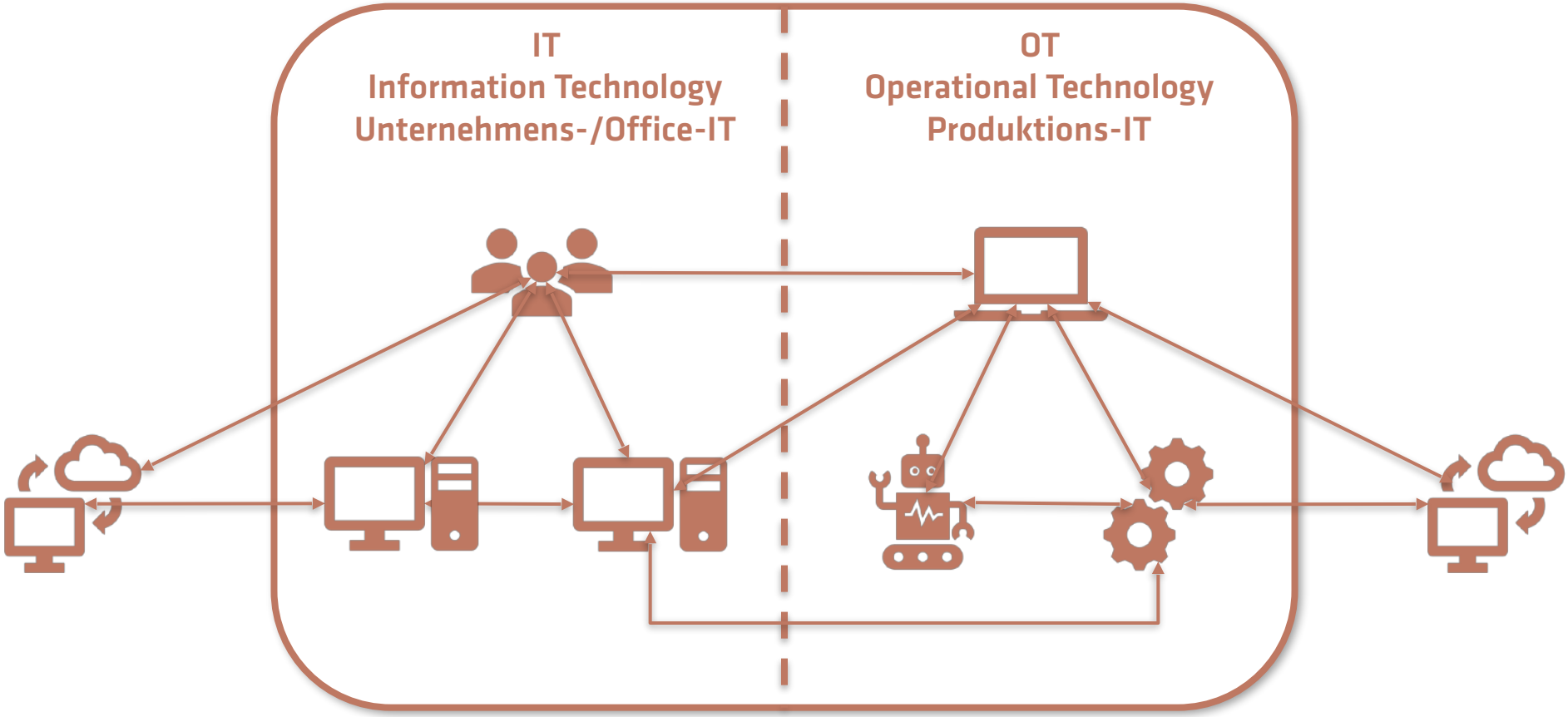
Höhere Flexibilität und Effizienz der industriellen Produktion durch:

- vollständig vernetzte Industriesteuerungen,
- ermöglicht durch die Verschmelzung mit den IT-Systemen,
- basierend auf der Internet-Technologie (Ethernet & TCP/IP).

Mit einigen neuen Herausforderungen:

- höhere Komplexität, geringere Sichtbarkeit,
- mehr Fehlerquellen,
- neue und mehr Sicherheitsbedrohungen.

# IT und OT in einem Unternehmen



# Die Ziele der OT und der IT vereinheitlichen sich

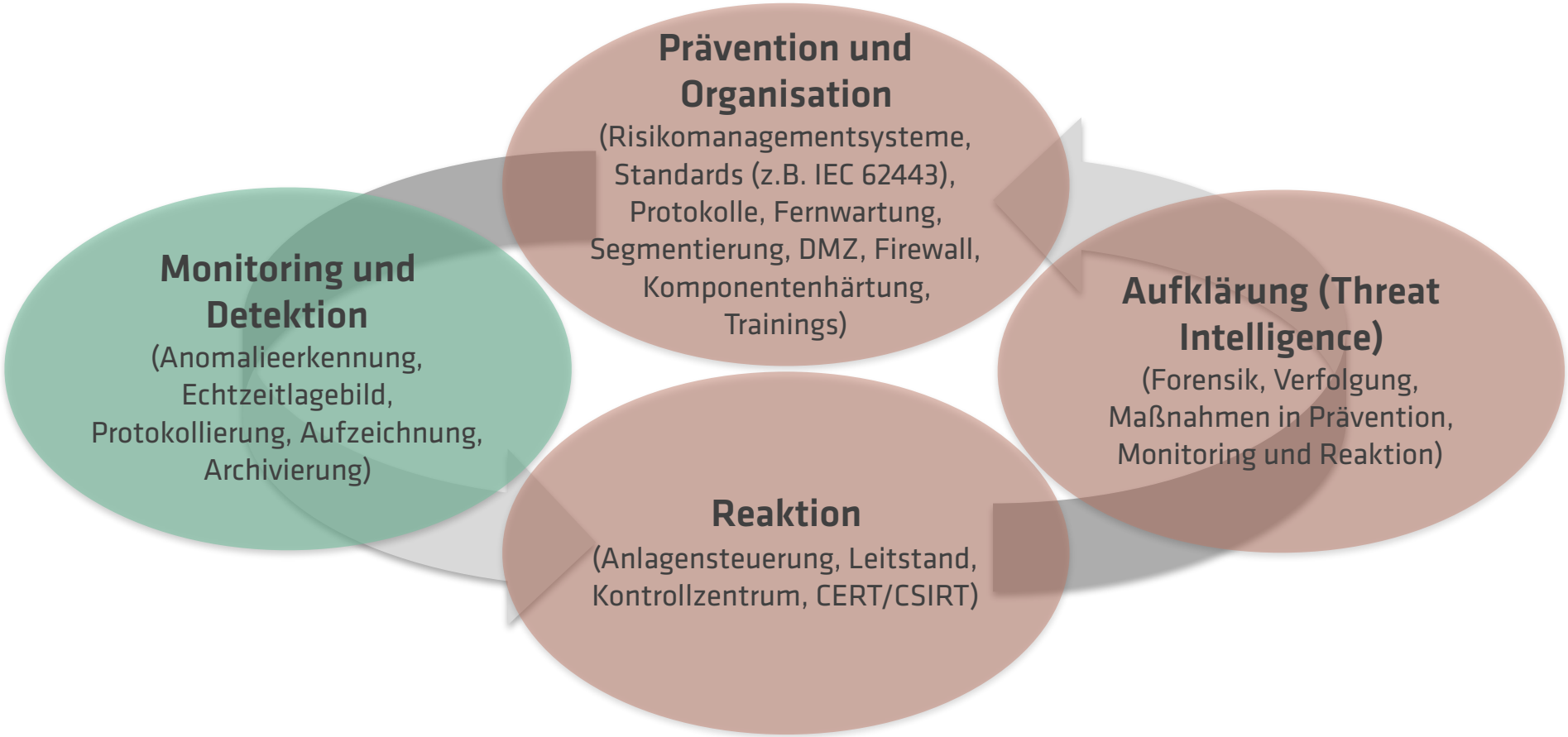
Produktion/ OT:

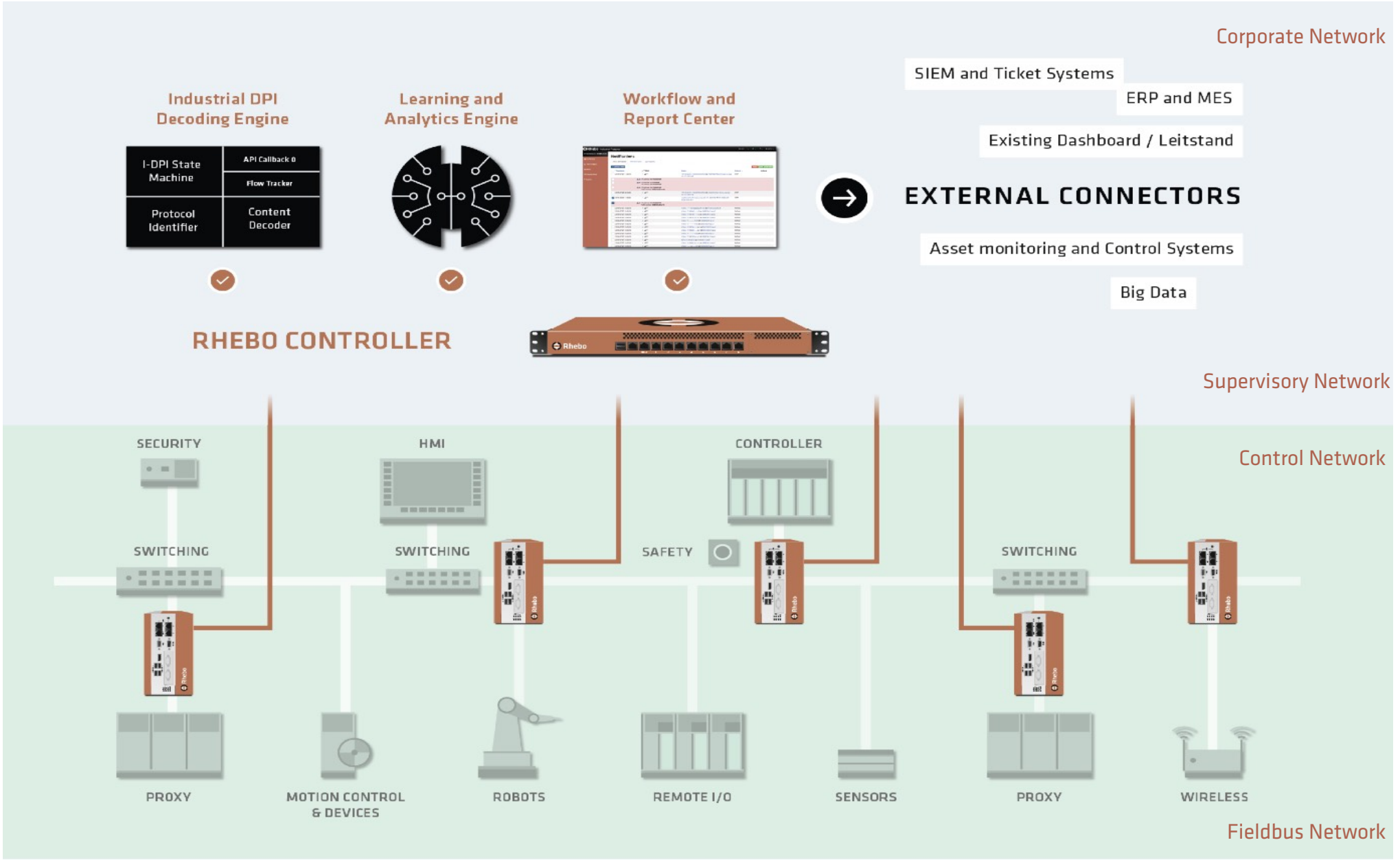
1. Funktionale Sicherheit
2. Verfügbarkeit
3. Integrität
4. Sicherheit for Angriffen

IT Systeme:

1. Sicherheit vor Angriffen
2. Datenschutz
3. Integrität
4. Verfügbarkeit

# Sicherheit (und Verfügbarkeit) in der Produktion




Corporate Network
Industrial DPI Decoding Engine
Learning and Analytics Engine
Workflow and Report Center
I-DPI State Machine
API Callback 0
Flow Tracker
Protocol Identifier
Content Decoder
SIEM and Ticket Systems
ERP and MES
Existing Dashboard / Leitstand
EXTERNAL CONNECTORS
Asset monitoring and Control Systems
Big Data
RHEBO CONTROLLER
Supervisory Network
Control Network
SECURITY
HMI
CONTROLLER
SWITCHING
SWITCHING
SAFETY
SWITCHING
PROXY
MOTION CONTROL & DEVICES
ROBOTS
REMOTE I/O
SENSORS
PROXY
WIRELESS
Fieldbus Network

# Wie wird 100% Sichtbarkeit erreicht?

Frame (L2): Physical device, media port, frame, VLAN, L2 protocol, function decode…

```
Device=02:14:4f...
Proto=EtherCAT
Vendor=Rockwell
Vendor=Siemens
Proto=LLDP
FirmwareVer=v04.02
Funct=LogicalWrite
Funct=PhysicalRead
APRDsession=0x0004
APRDvalue=0x0130
Proto=ARP
...
```

Packet (L3 to L7+): Logical address, host, protocol, application…

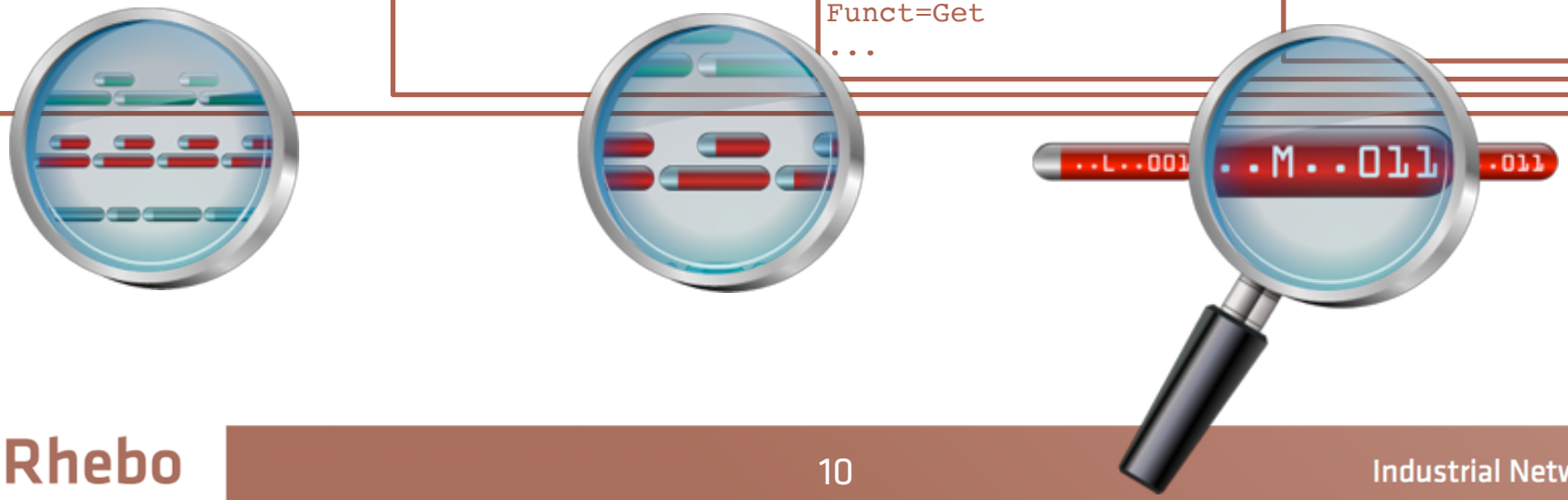
```
Proto=Profinet
Funct=DCP_Set
Proto=EtherCAT
Funct=LogicalWrite
Proto=DHCP
Proto=HTTP
Proto=FTP
```

Command and Function Decode:

```
Proto=Profinet
Funct=DCP_Set
Proto=EtherCAT
Funct=LogicalWrite
Proto=DHCP
Funct=Discover
Proto=HTTP
Funct=Get
...
```

Values Extraction:

```
User_Prm_Data_Len=2
User_Prm_Data=0x00,0x00
Temperature=32degrees
...
```



# Aktuell unterstützte Protokolle (v2.4)

## Industrieprotokolle

BACnet
CIP
DNP3
ELCOM-90
EtherCAT
Haag Damon
HART
iba Device Config. Protocol
IEC60870-5-104
IEC61850-GOOSE
IEC61850-GSSE
IEC61850-MMS
IEC61850-SMV
LonTalk
Modbus
MRP
OPC UA
OpenProtocol
Powerlink
Proficy iFix
Profinet
Profinet IO CM
PSI
RK 512
S7
Sercos III
Sinec H1
WinCC

## Netzwerkprotokolle

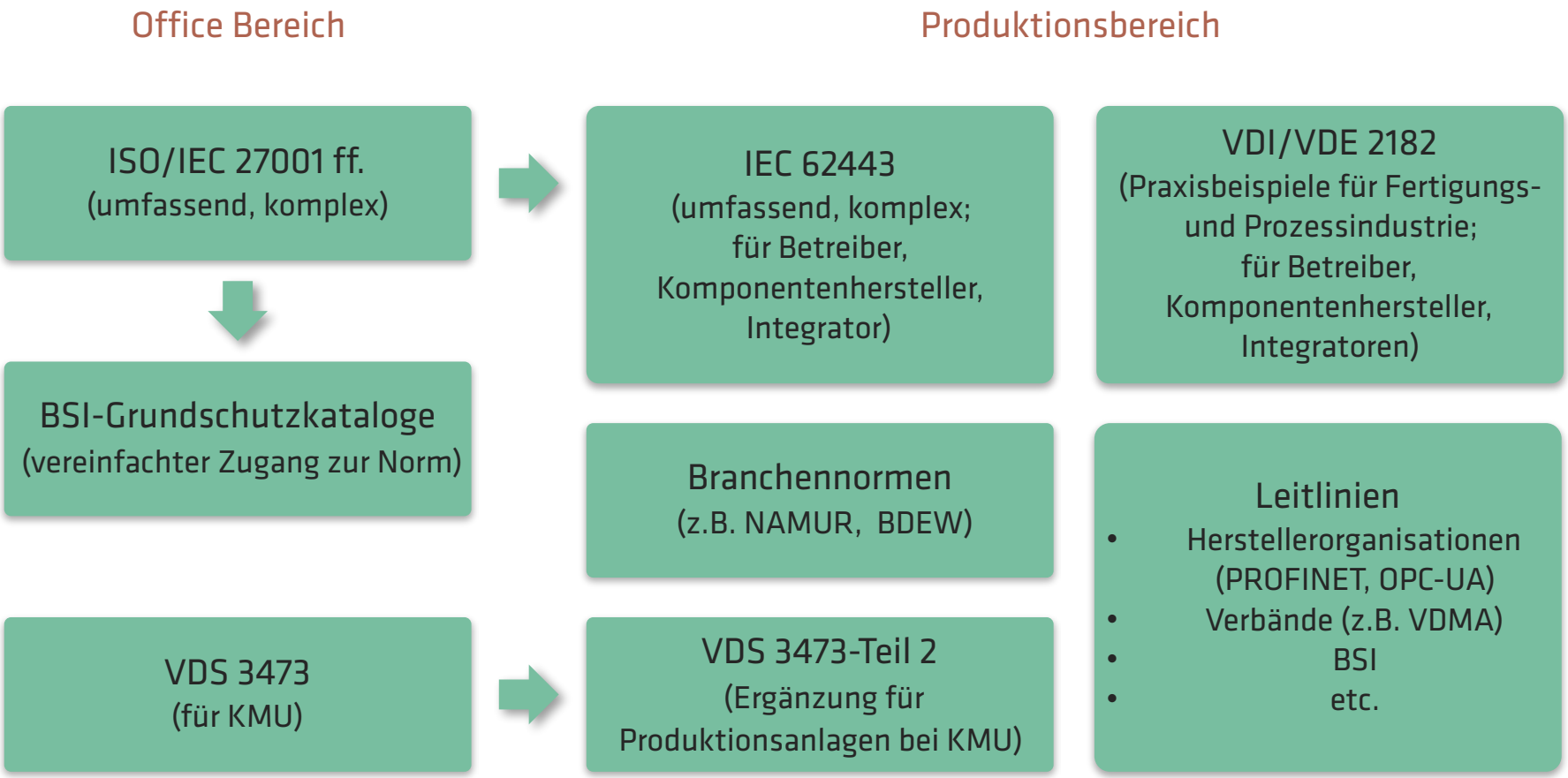
Acronis Backup
Adobe Server
ARP
AXIS Camera Management
Canon BJNP
CDP
CGMP
Cisco
Cisco DCE
COTP
DCE/RPC
DEC
DHCP
DNS
DTP
ECTP
EGP
EIGRP
FTP Control
FTP Data
HP
HP DTC
HP Extended LLC
HP Probe
HSR
HSRP
HTTP
HTTPS
ICMP
IGMP
IPv6
Kerberos
LDAP
LLC
LLDP
LLMNR
McAfee ePO
mDNS
NetBIOS
NFS
NTP
OSPF
PIM
PTP
QUIC
RDP
Remote Shell
Rhebo
SentinelSRM
SKINNY SCCP
SMB
SMTP
SNMP
SQLNET2
SSDP
SSH
SSL
STP
Symantic Endpoint Protection Manag.
Syslog
TDS
Telnet
TFTP
TNS
VMWare-Lab-Manager
VNC
VRRP
WLCCP
X11

Vernetzte Produktion

**Standards**

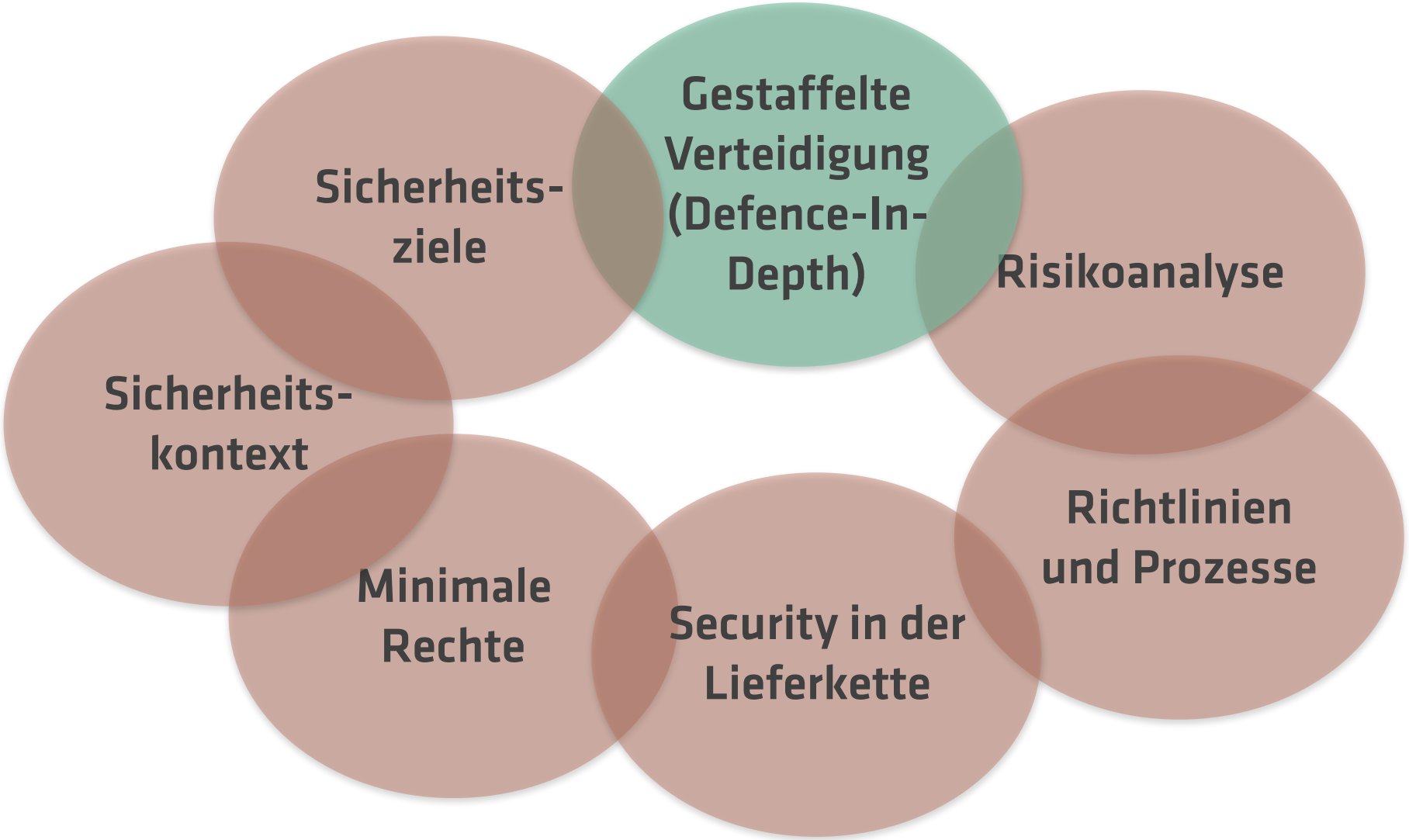
Reale Beispiele

# IT-Sicherheit: Normen, Standards, Richtlinien

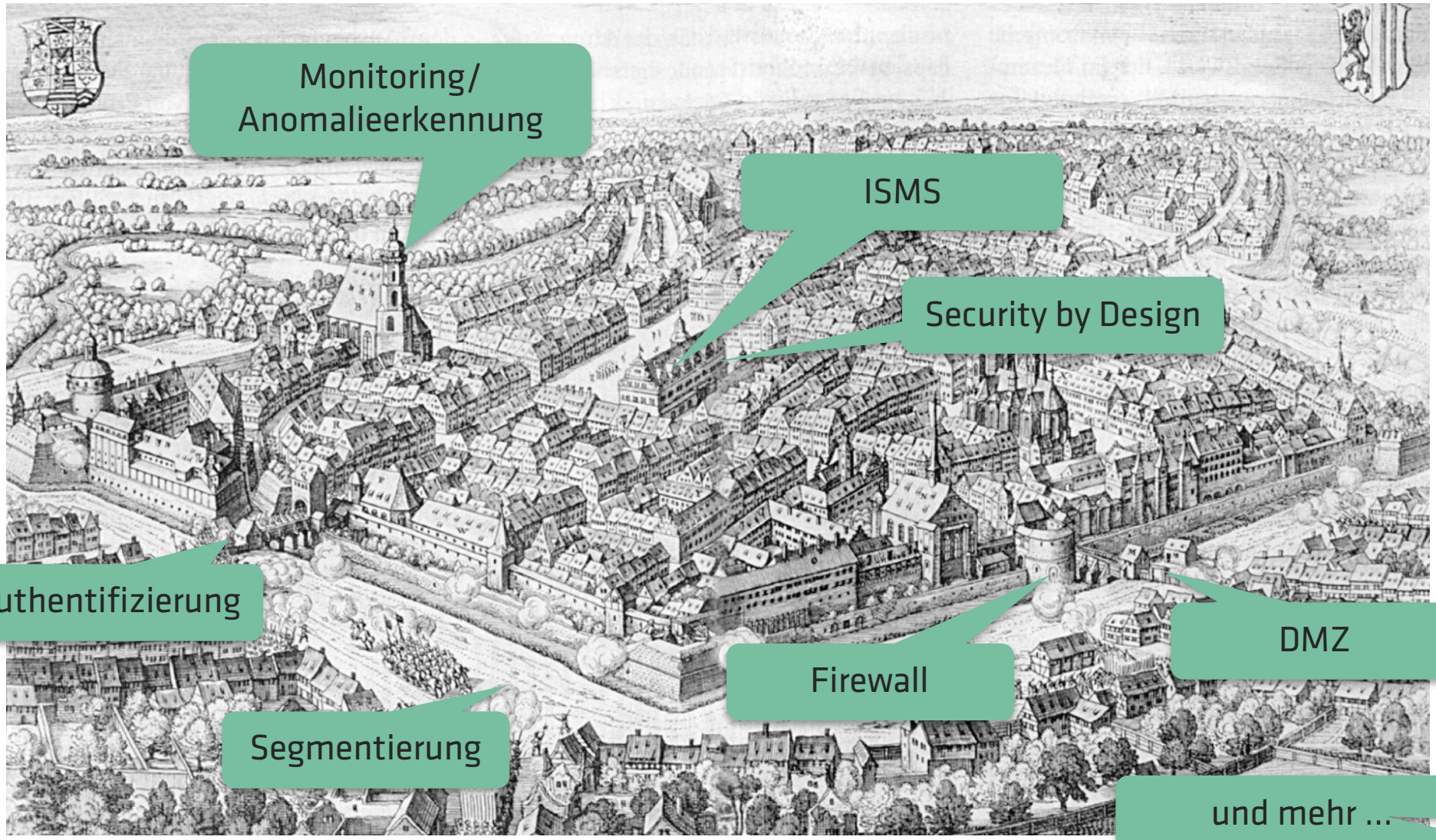


# Der (grobe) Weg durch die IEC62443

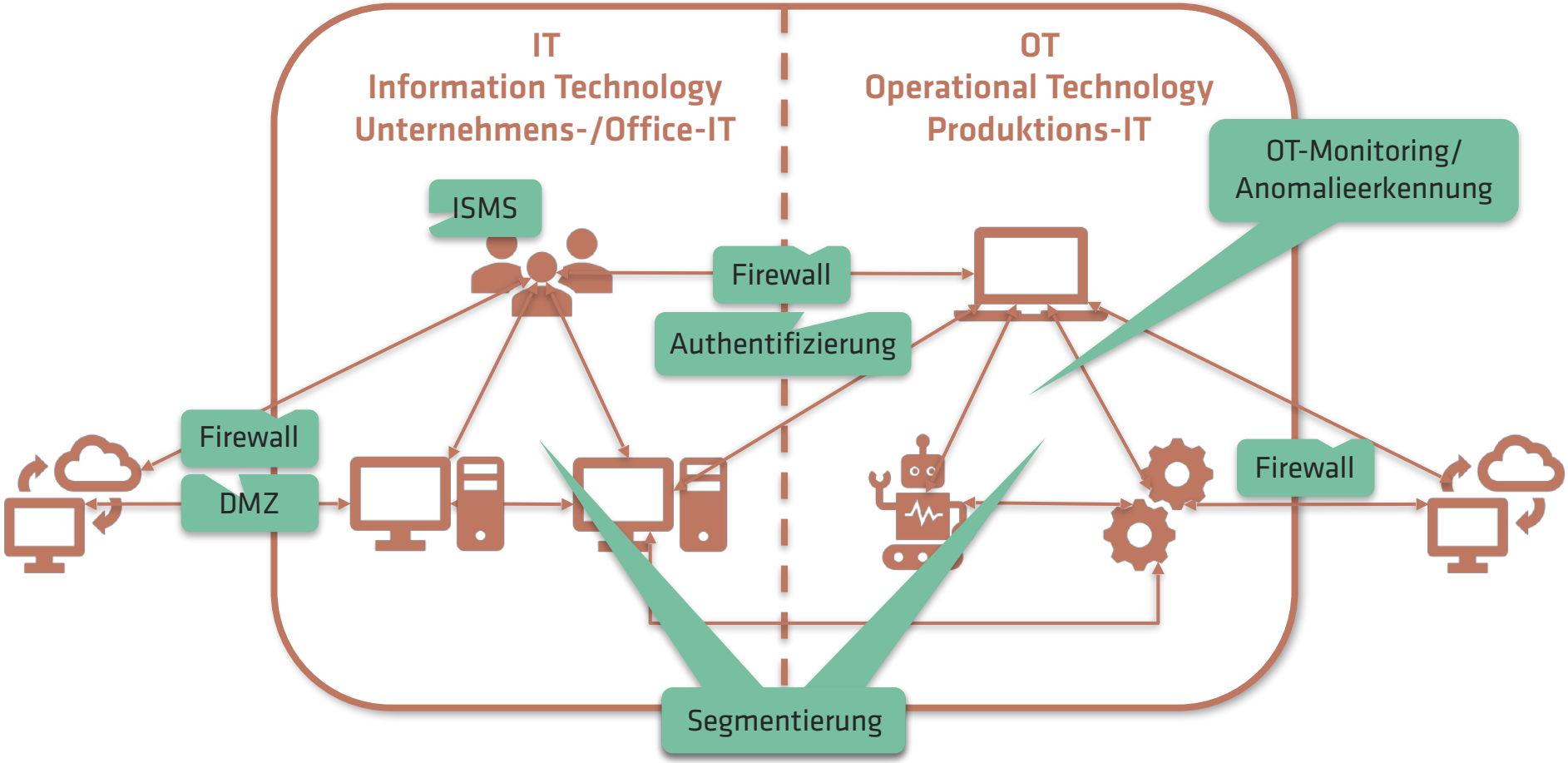
# Allgemeine Konzepte (General Concepts)



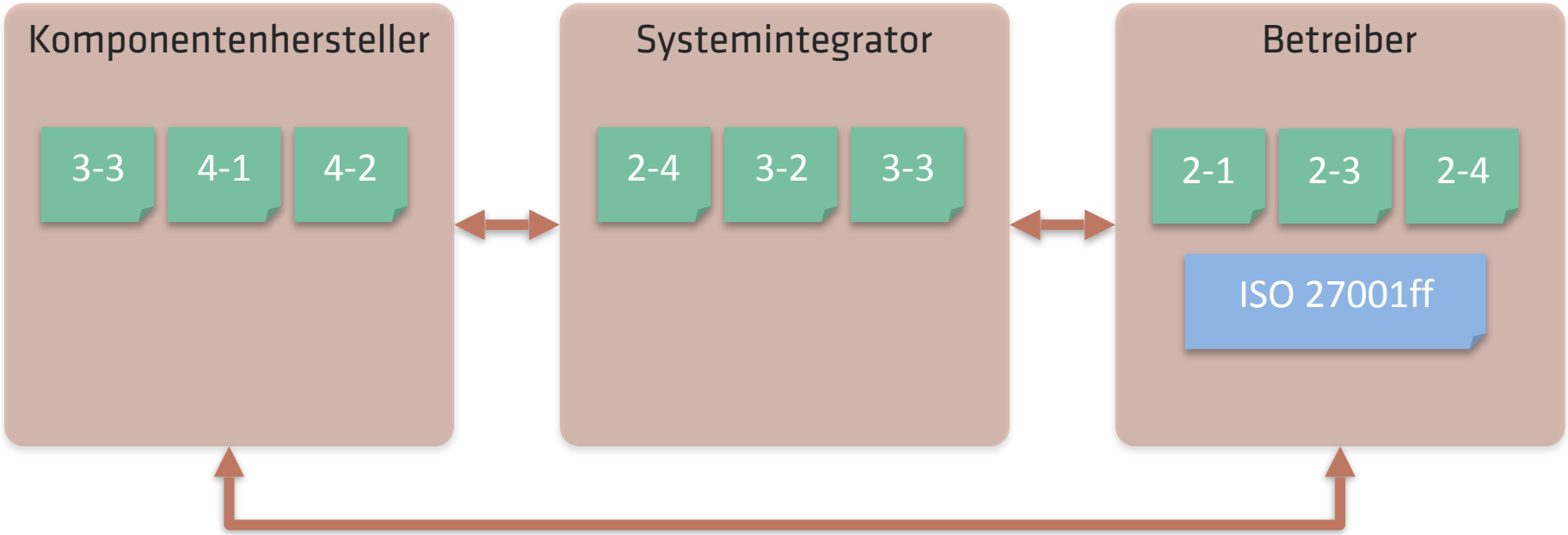
# Defence in Depth



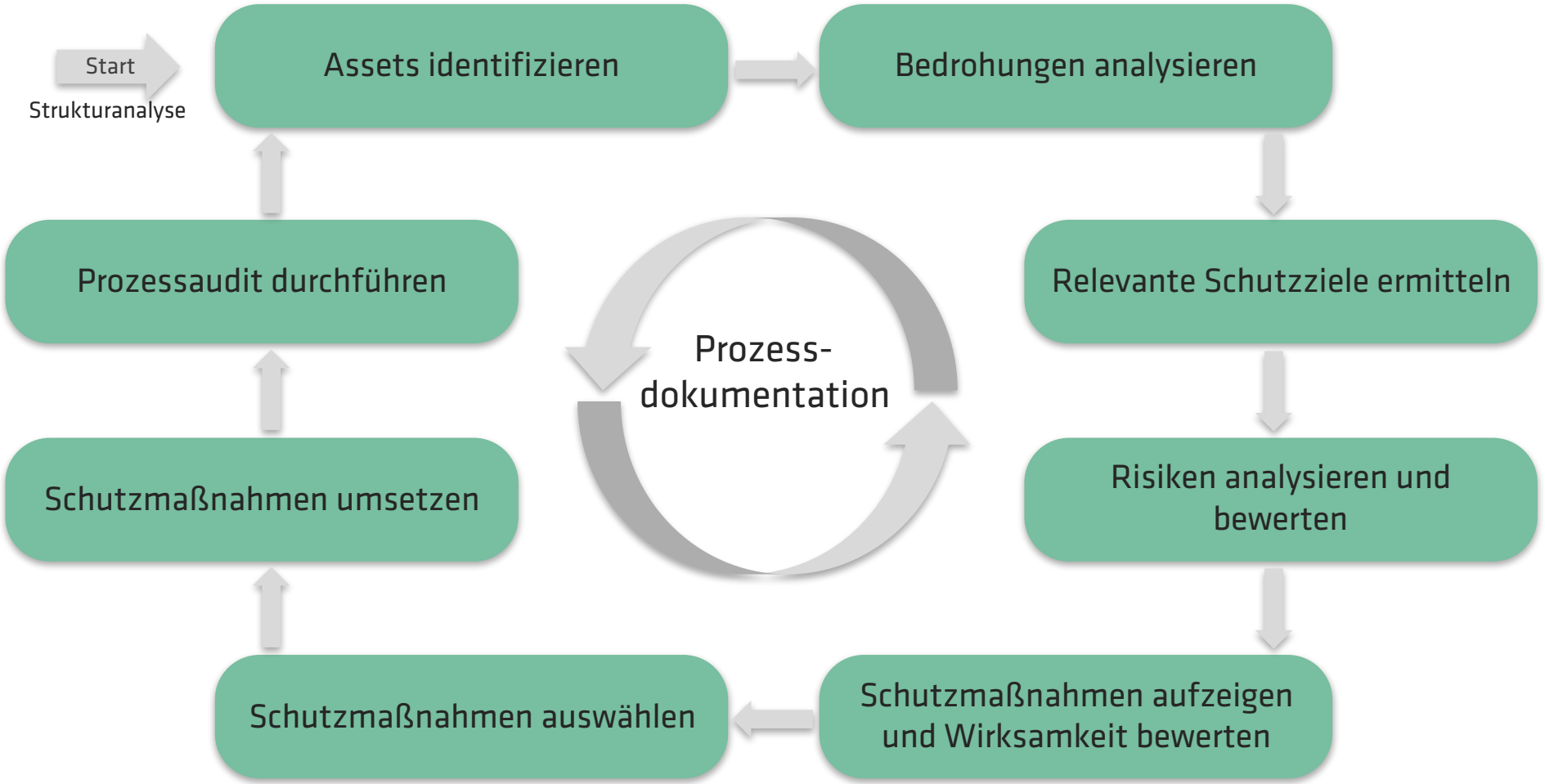
# Defence in Depth im Unternehmen



# Zusammenspiel der Rollen im Security-Lebenszyklus



# PDCA-Vorgehensmodell

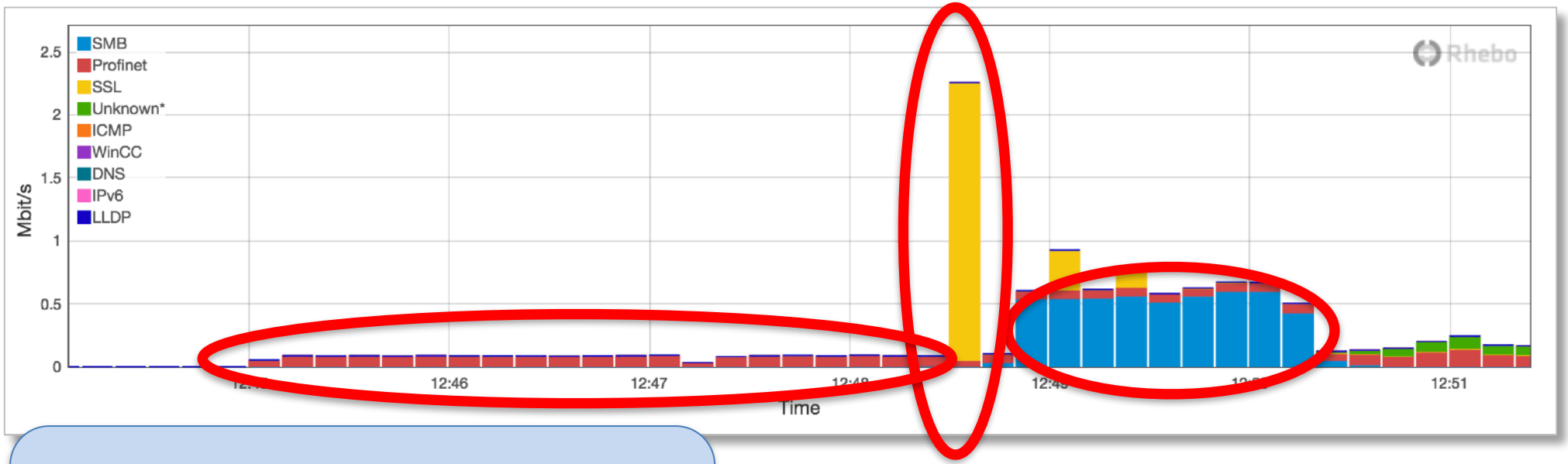



Vorgehensmodell nach VDI_2182_1

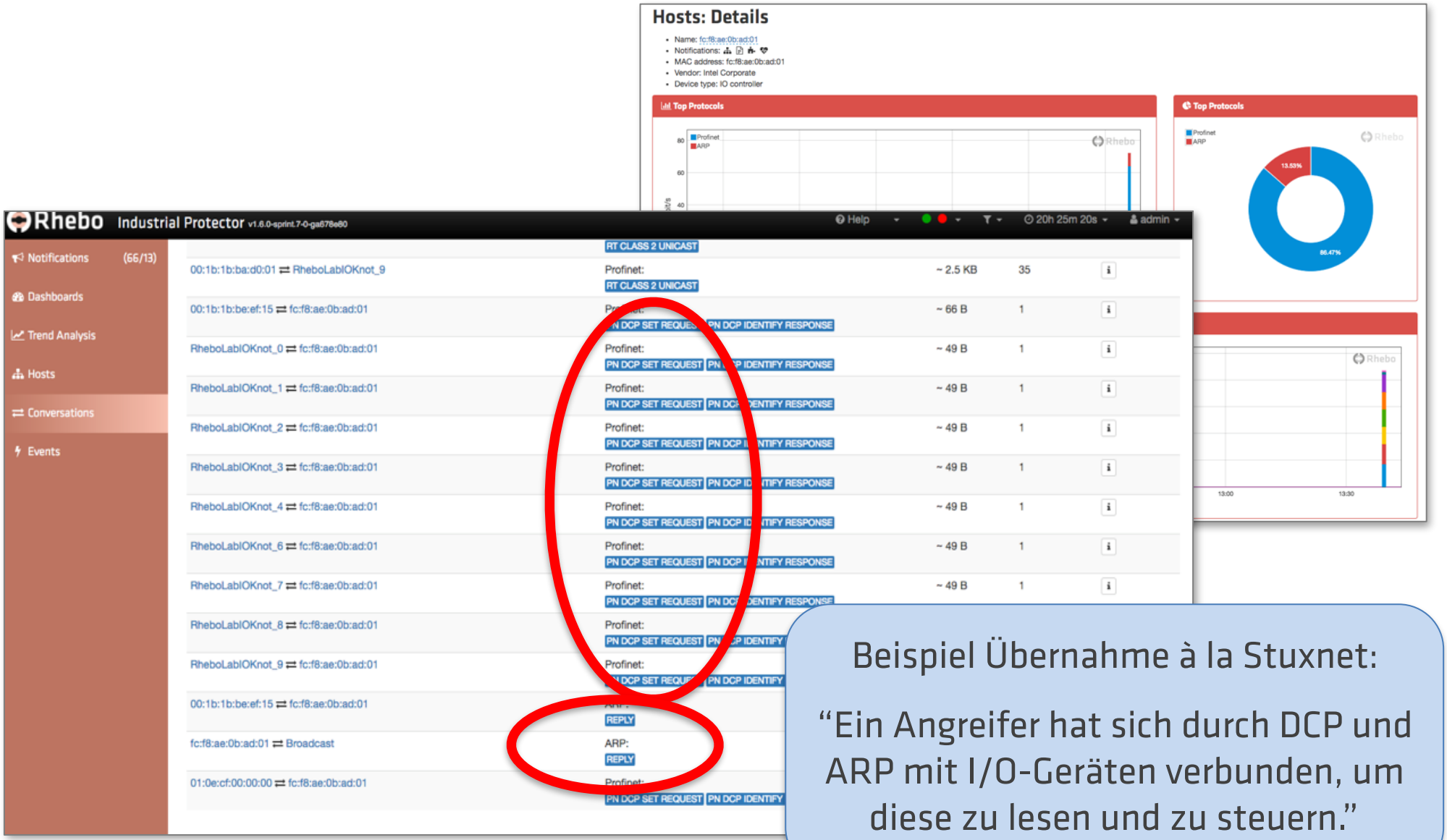
Vernetzte Produktion
Standards
**Reale Beispiele**


Beispiel WannaCry:

“WannaCry hat sich rasend schnell ausgebreitet. … ”

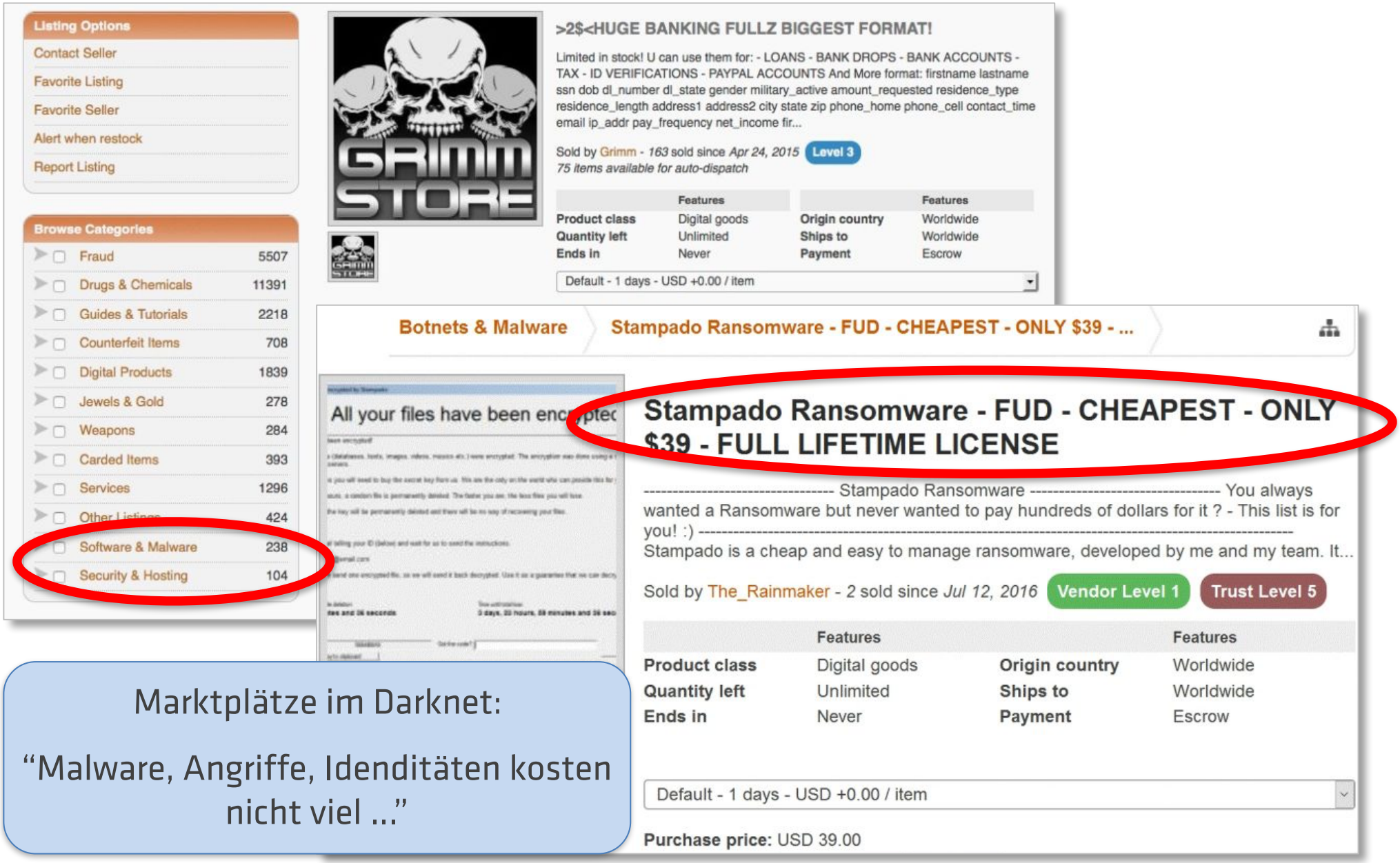



"... Normaler Profinetverkehr, valides Datenbankupdate über SSL – aber anormal hoher SMB-Verkehr."




Beispiel Übernahme à la Stuxnet:

“Ein Angreifer hat sich durch DCP und ARP mit I/O-Geräten verbunden, um diese zu lesen und zu steuern.”




Marktplätze im Darknet:

“Malware, Angriffe, Idenditäten kosten nicht viel …”

# Millionen ICS sind aus dem Internet erreichbar

z.B. www.shodan.io


## XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

## PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

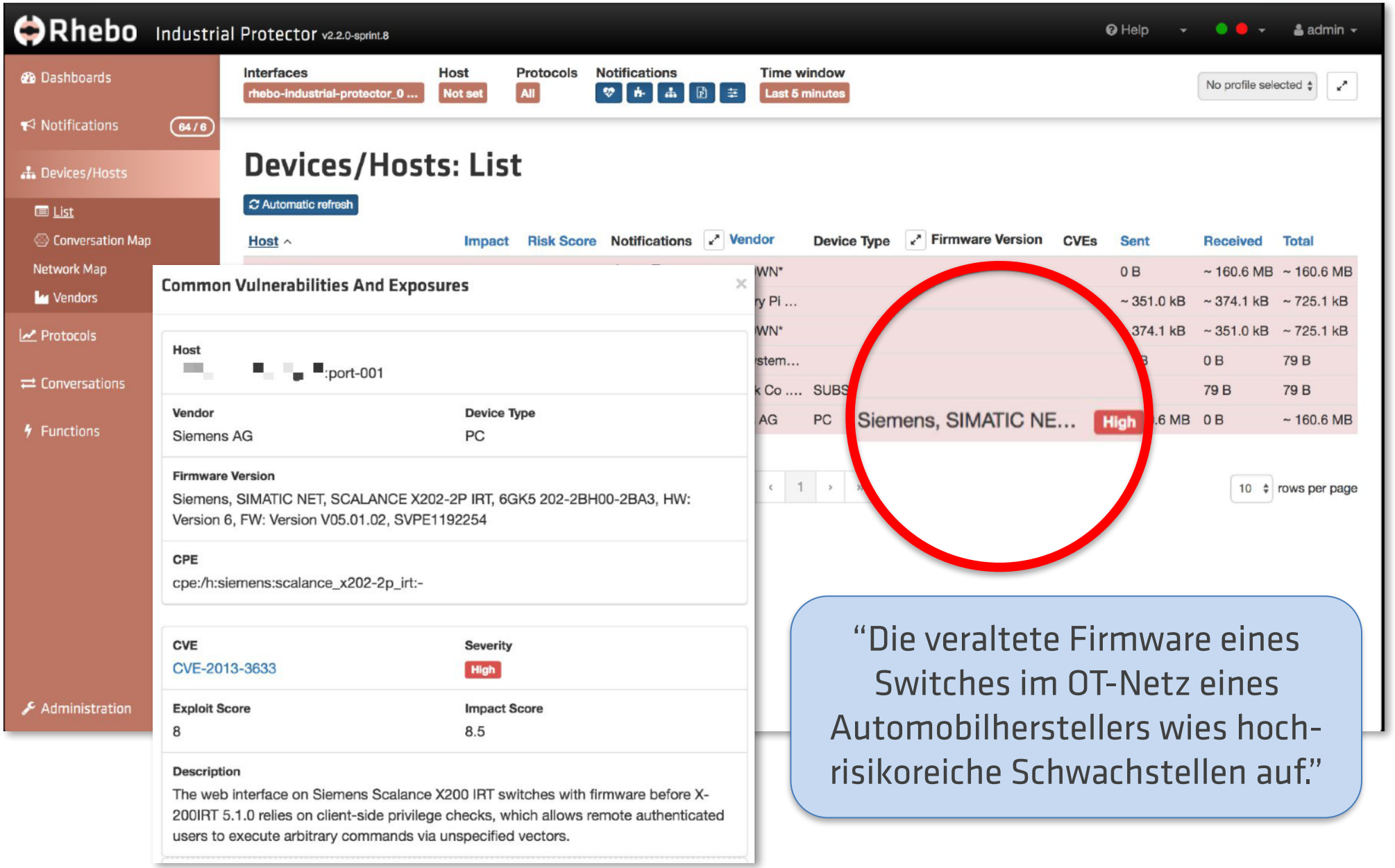
Explore

**The search engine for Power Plants**

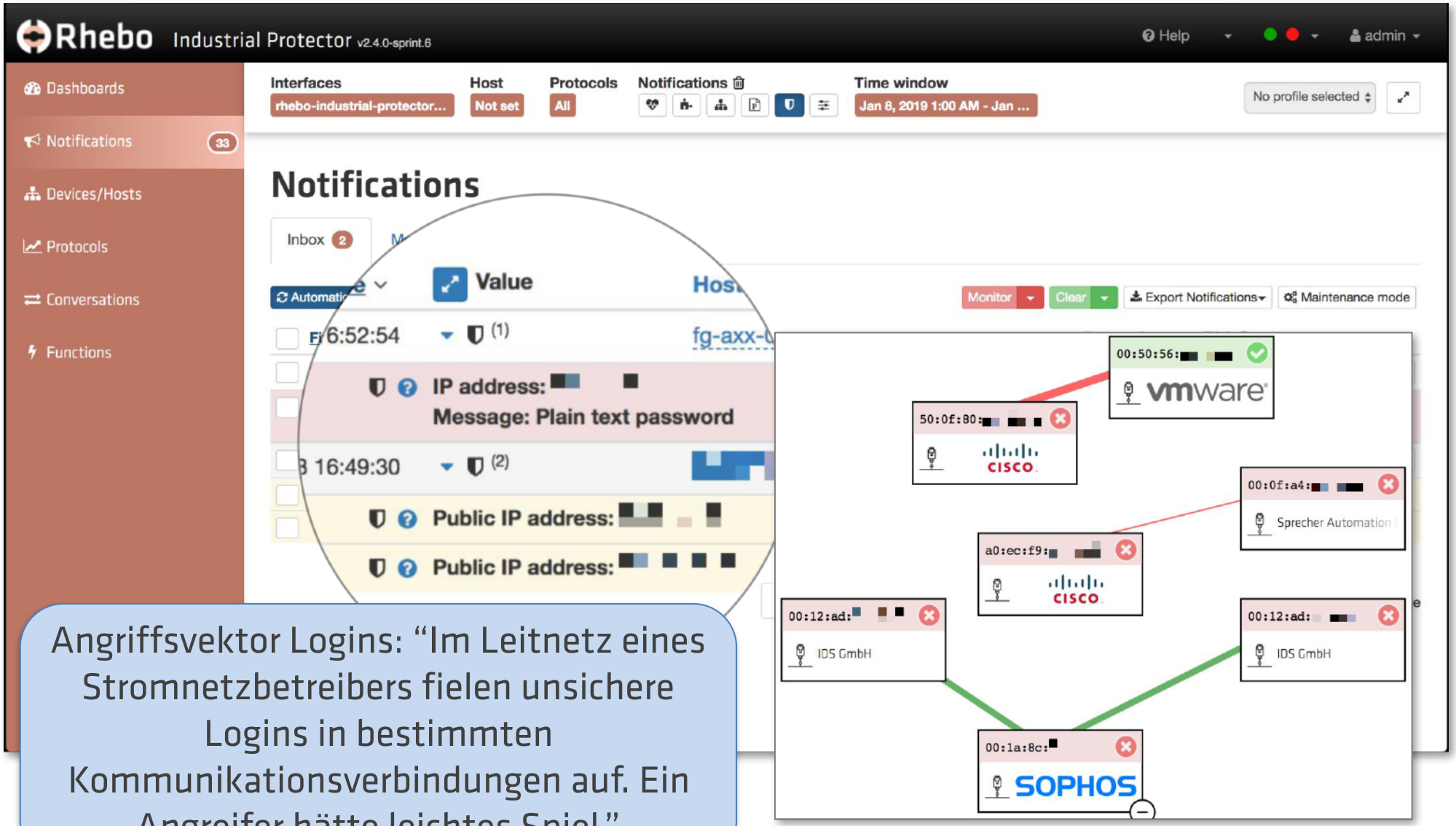
**The search engine for Buildings**

**The search engine for the Internet of Things**

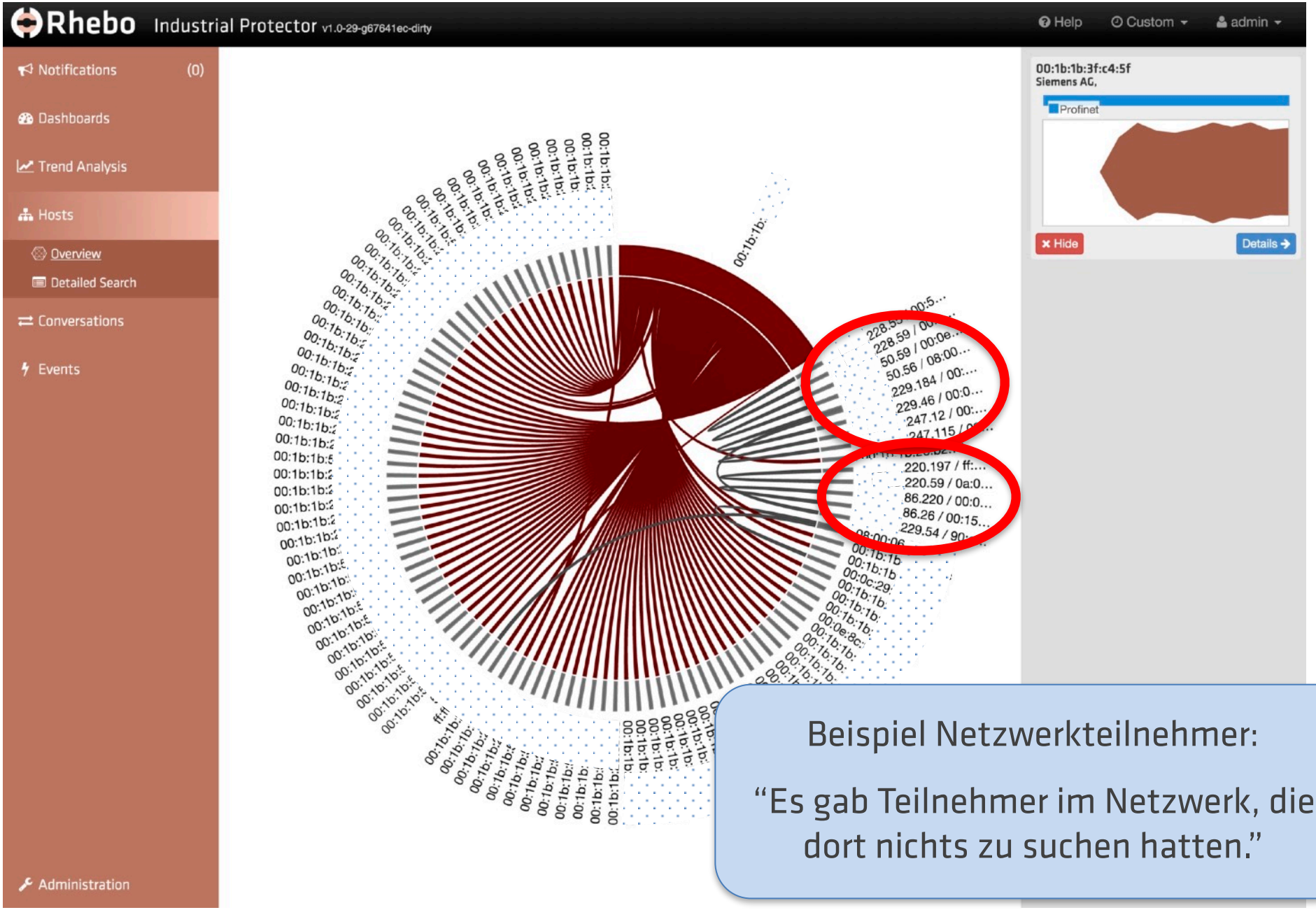
**The search engine for Refrigerators**

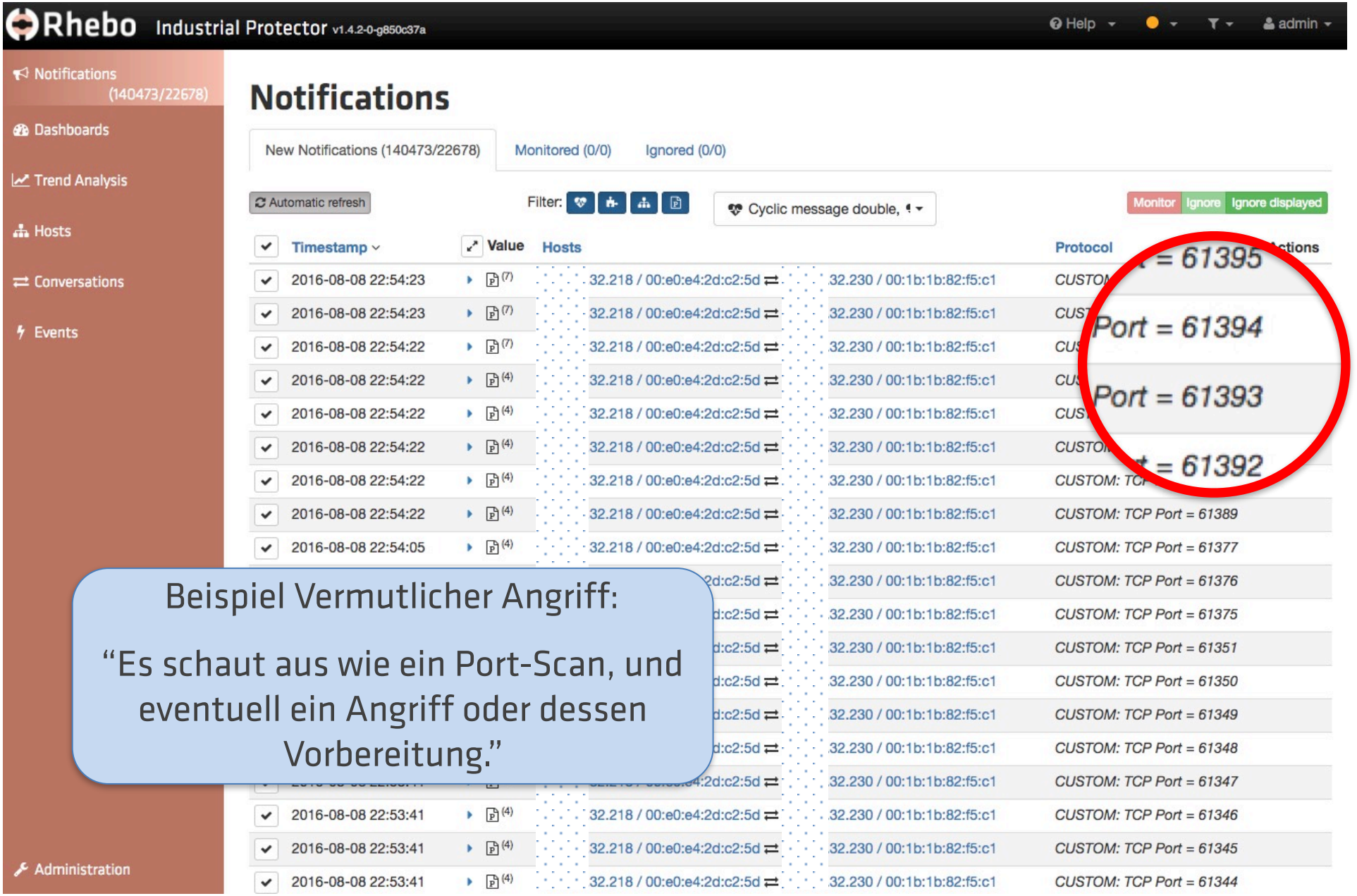



"Die veraltete Firmware eines Switches im OT-Netz eines Automobilherstellers wies hoch-risikoreiche Schwachstellen auf."



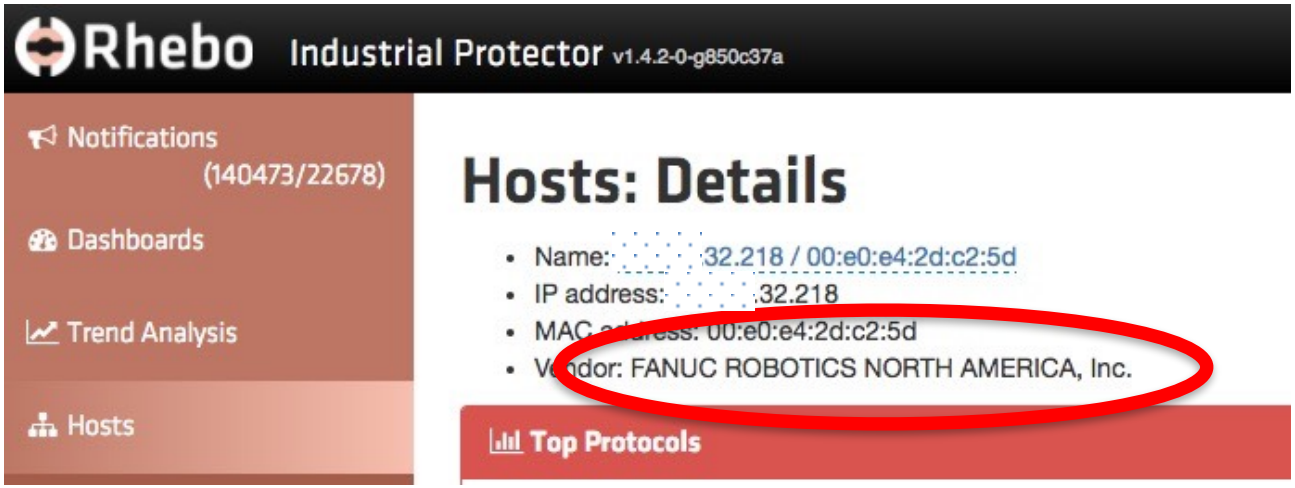

Angriffsvektor Logins: “Im Leitnetz eines Stromnetzbetreibers fielen unsichere Logins in bestimmten Kommunikationsverbindungen auf. Ein Angreifer hätte leichtes Spiel.”


Rhebo Industrial Protector v1.0-29-g67641ec-dirty
Help
Custom
admin
Notifications (0)
Dashboards
Trend Analysis
Hosts
Overview
Detailed Search
Conversations
Events
Administration
00:1b:1b:3f:c4:5f
Siemens AG,
Profinet
Hide
Details
Beispiel Netzwerkteilnehmer:
"Es gab Teilnehmer im Netzwerk, die dort nichts zu suchen hatten."




Beispiel Vermutlicher Angriff:

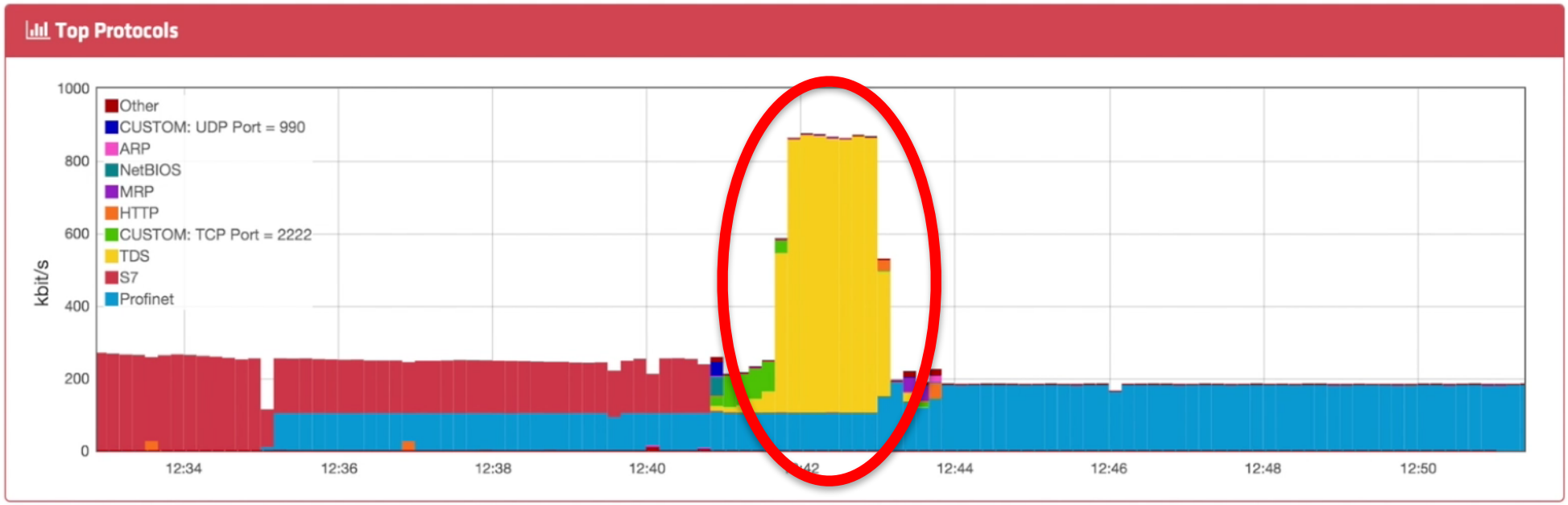
"Es schaut aus wie ein Port-Scan, und eventuell ein Angriff oder dessen Vorbereitung."

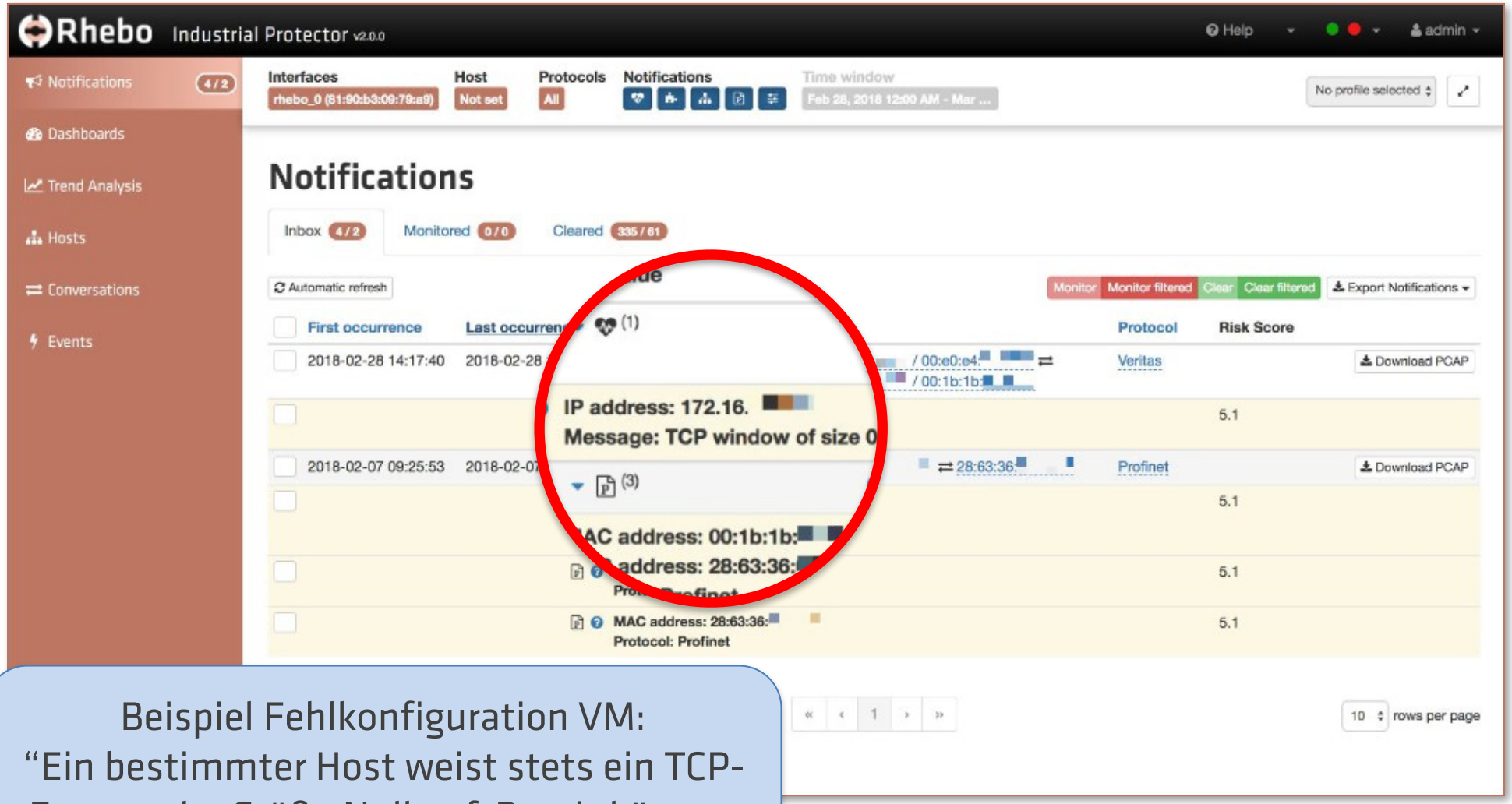



"... Es war aber die regelkonforme Steuerkommunikation eines eingesetzten Roboters."

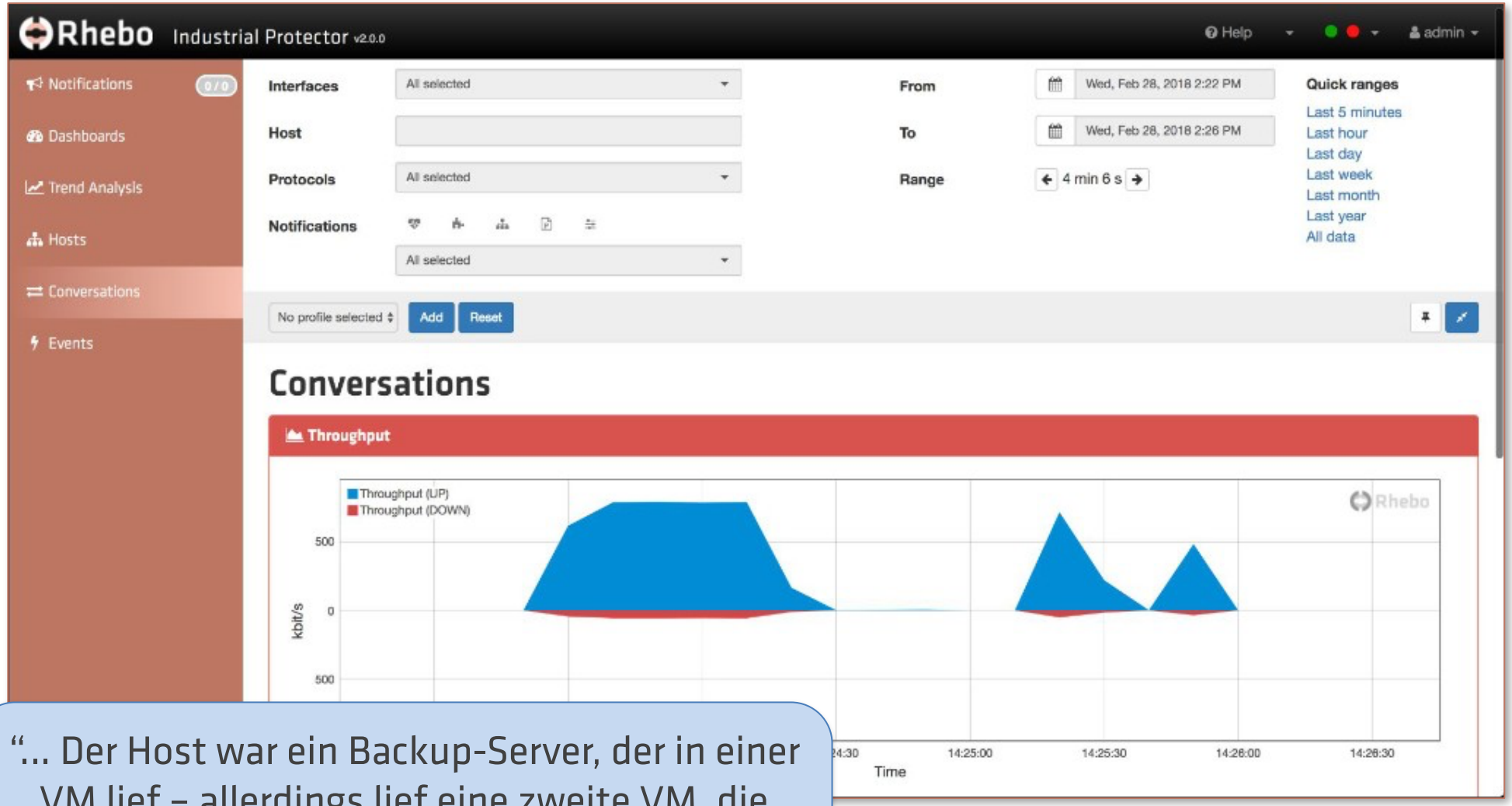
Beispiel Datenbankabfragen:
“Die Netzwerkbelastung durch periodische Datenbankabfragen muss in die Planung der Netzinfrastruktur einberechnet werden.”

## Trend Analysis

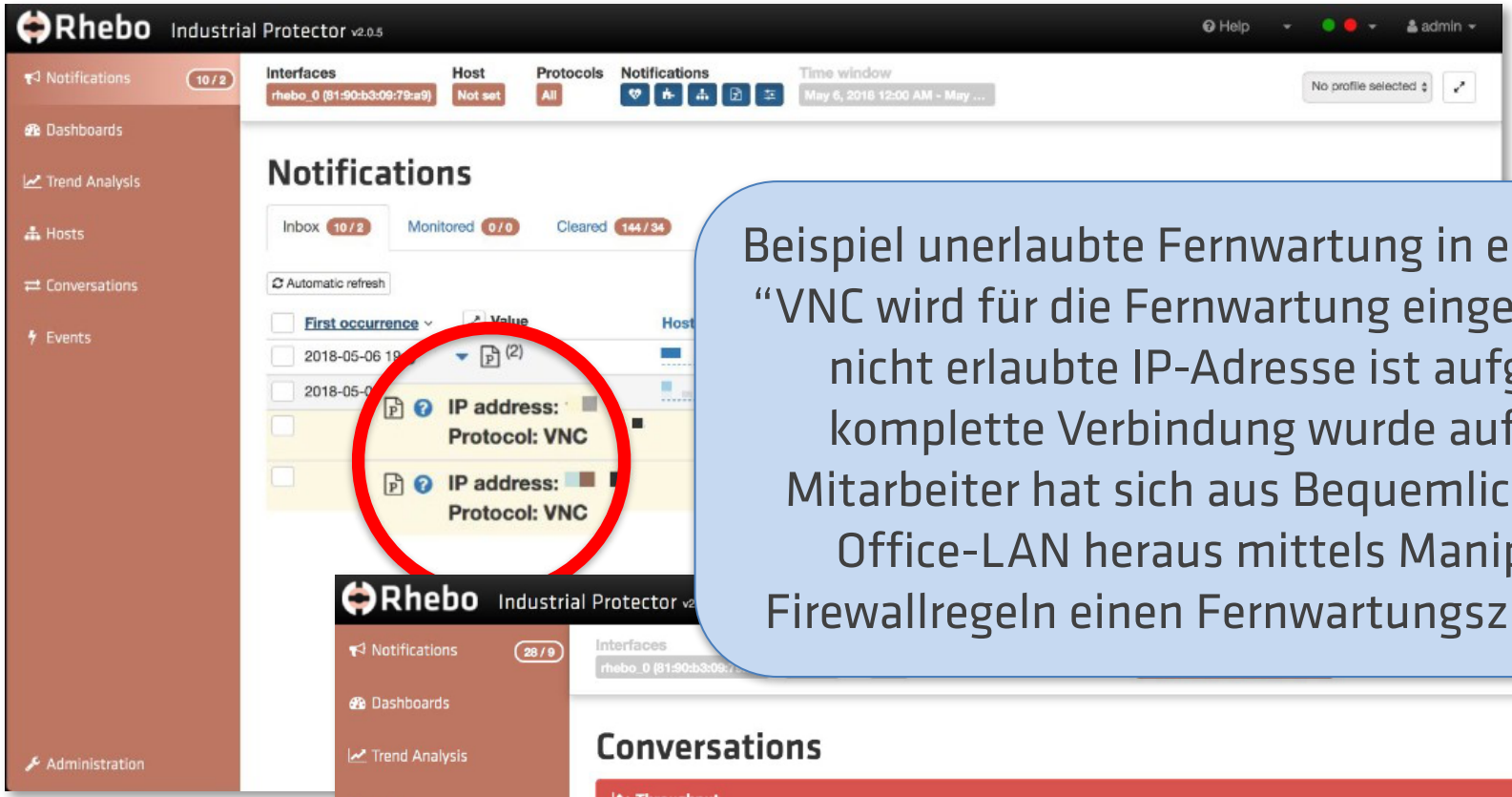




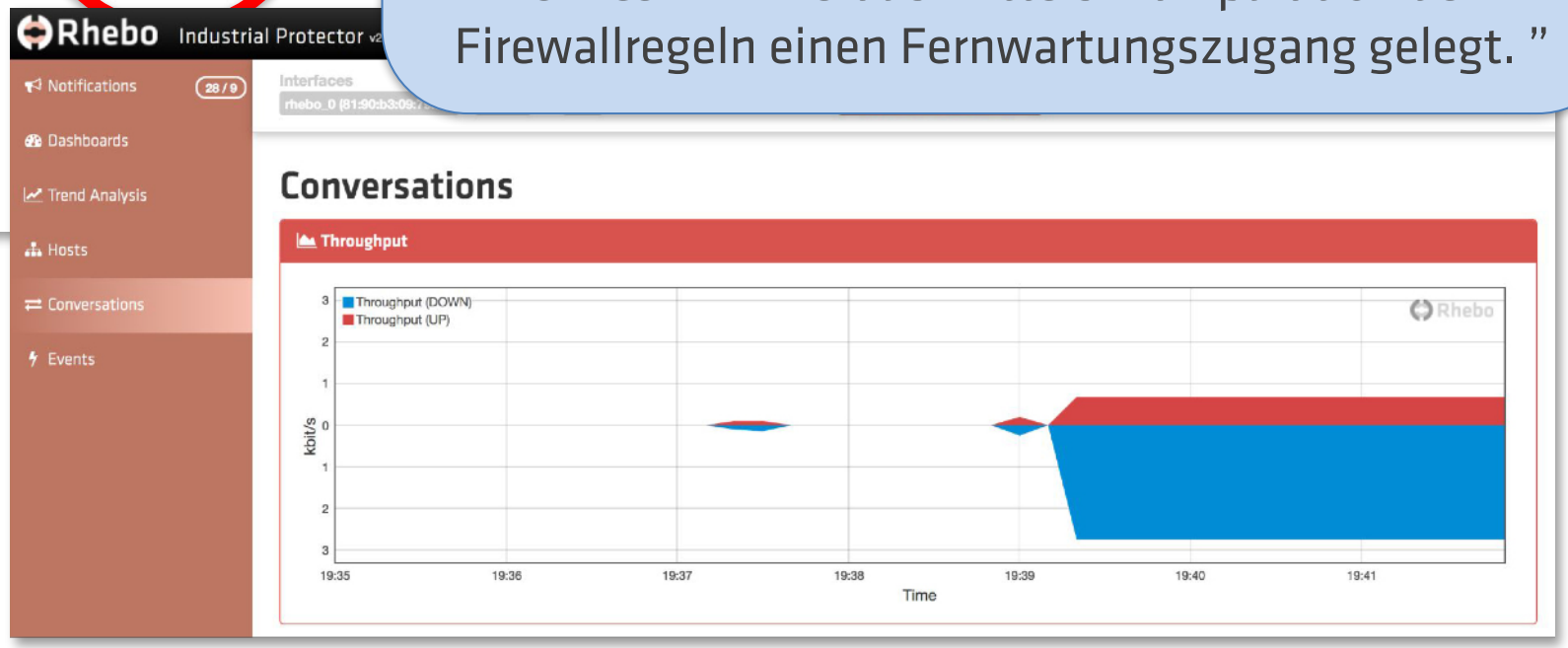

Beispiel Fehlkonfiguration VM:
“Ein bestimmter Host weist stets ein TCP-Fenster der Größe Null auf. Damit können keine Daten empfangen werden. ...”

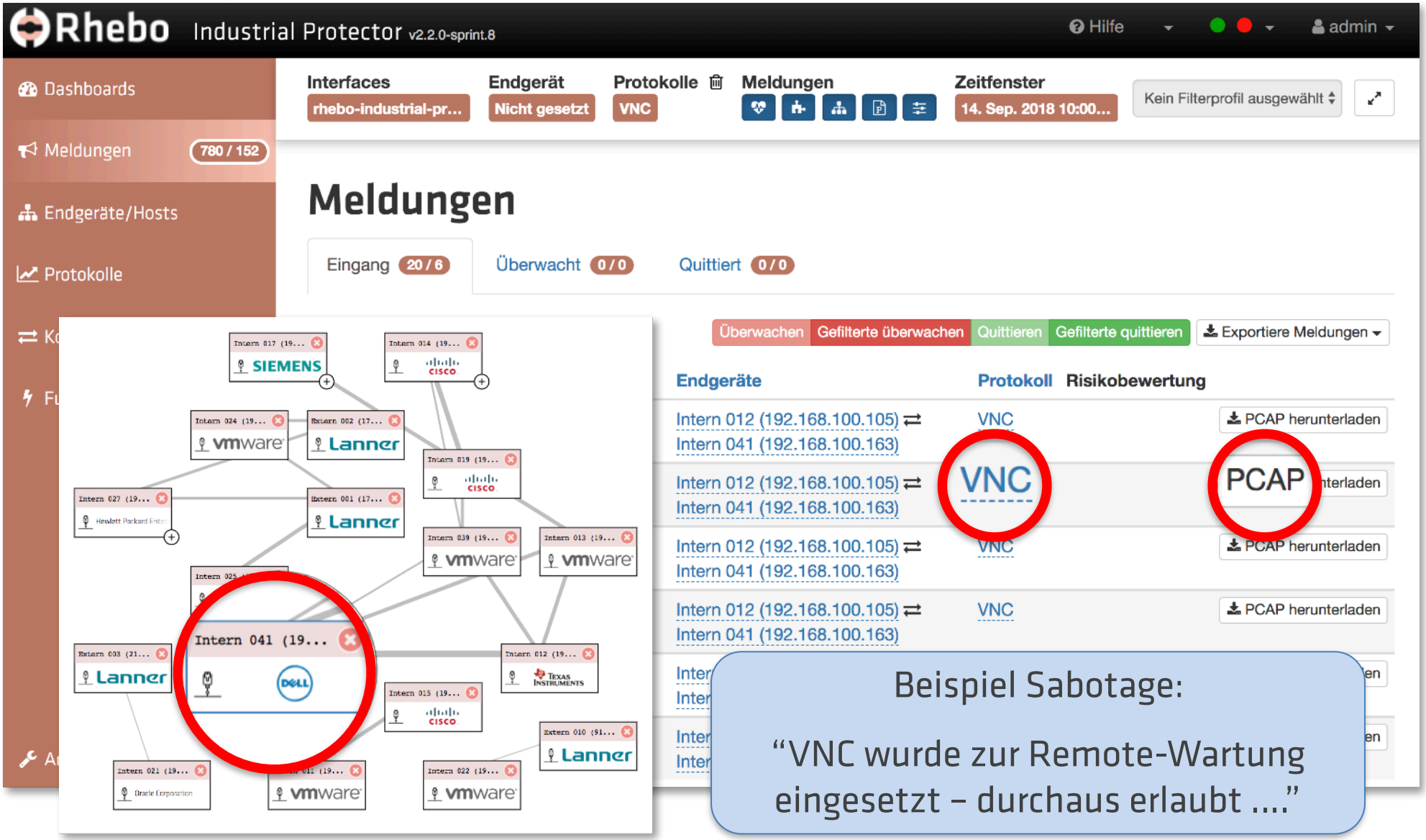



"... Der Host war ein Backup-Server, der in einer VM lief – allerdings lief eine zweite VM, die aufgrund einer Fehlkonfiguration die Ressourcen vollständig beansprucht hat."




Beispiel unerlaubte Fernwartung in einem Kraftwerk: “VNC wird für die Fernwartung eingesetzt, aber eine nicht erlaubte IP-Adresse ist aufgefallen. Die komplette Verbindung wurde aufgezeigt. Ein Mitarbeiter hat sich aus Bequemlichkeit aus dem Office-LAN heraus mittels Manipulation der Firewallregeln einen Fernwartungszugang gelegt. ”




Rhebo Industrial Protector v2.2.0-sprint.8
Hilfe
admin
Dashboards
Meldungen 780 / 152
Endgeräte/Hosts
Protokolle
Interfaces
rhebo-industrial-pr...
Endgerät
Nicht gesetzt
Protokolle
VNC
Meldungen
Zeitfenster
14. Sep. 2018 10:00...
Kein Filterprofil ausgewählt
Meldungen
Eingang 20 / 6
Überwacht 0 / 0
Quittiert 0 / 0
Überwachen
Gefilterte überwachen
Quittieren
Gefilterte quittieren
Exportiere Meldungen
Endgeräte
Protokoll
Risikobewertung
Intern 012 (192.168.100.105)
Intern 041 (192.168.100.163)
VNC
PCAP herunterladen
Intern 041 (19...
SIEMENS
CISCO
vmware
Lanner
DELL
Texas Instruments
Beispiel Sabotage:
“VNC wurde zur Remote-Wartung eingesetzt – durchaus erlaubt ....”

```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import sys
import binascii
from scapy.all import sniff, TCP, Raw


VNC_CODES = {'ff08': 'Backspace',
             'ff09': 'Tab',
             'ff0d': 'Return/Enter',
             'ff1b': 'Escape',
             'ff63': 'Insert',
             'ffff': 'Delete',
             'ff50': 'Home',
             'ff57': 'End',
             'ff55': 'Page-Up',
             'ff56': 'Page-Down',
             'ff51': 'Left',
             'ff52': 'Up',
             'ff53': 'Right',
             'ff54': 'Down'}

PORT_RANGE_TCP = list(range(5901, 5999))
PORT_RANGE_HTTP = list(range(5801, 5899))


def parse_vnc(raw_payload):

        decoded = binascii.hexlify(raw_payload).dec

        if len(decoded) == 16 and decoded[1] == '4'
            try:
                if decoded[-4:] in VNC_CODES:
                    key_stroke = VNC_CODES[decoded[
                    print('_{0}'.format(key_stroke)
                else:
                    key_stroke = binascii.unhexlify
                    print(key_stroke, end='', flush

            except UnicodeDecodeError:
                print('\\n')


def callback(rawPacket):

    if rawPacket.haslayer(TCP):
        srcPort = rawPacket.getlayer(TCP).sport
        dstPort = rawPacket.getlayer(TCP).dport

        if (srcPort in PORT_RANGE_TCP
                or dstPort in PORT_RANGE_TCP):

            if rawPacket.haslayer(Raw):
                parse_vnc(rawPacket.getlayer(Raw).load)


sniff(offline=sys.argv[1], store=0, prn=callback)
```

```python
def parse_vnc(raw_payload):

        decoded = binascii.hexlify(raw_payload).decode('latin-1')

        if len(decoded) == 16 and decoded[1] == '4' and decoded[3] == '0':
            try:
                if decoded[-4:] in VNC_CODES:
                    key_stroke = VNC_CODES[decoded[-4:]]
                    print('_{0}'.format(key_stroke))
                else:
                    key_stroke = binascii.unhexlify(decoded[-8:]).decode('utf-8')[-1]
                    print(key_stroke, end='', flush=True)

            except UnicodeDecodeError:
                print('\\n')

def callback(rawPacket):
```

```
ppppppppppppp---
---
sshhuuttddoowwnn   --hh    nooww_Return/Enter
 Return/Enter
```

"... Es war jedoch der Sabotageangriff eines Innentäters, der (nachweislich) gezielt und konzertiert Geräte heruntergefahren hat."


Dr. Frank Stummer
frank.stummer@rhebo.com
www.rhebo.com