



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

Unternehmern
 Leipzig
 die alleiniger
 ipoque 2014
 arbeitete
 beide
 Stummern
 Institut
 ist
 u. a. liegt
 Frankfurter
 Vertrieb
 Digital
 akquiriert
 mehrere
 Konzern
 e. von 2006
 CEO
 GmbH
 Fraunhofer
 sowie
 Uhd
 Business
 Mitgründer
 Industrie
 Systems
 Adyton
 wurden
 zuvor
 Forensics
 IT-Sicherheit
 Grosskonzerne
 studierte



DIGITAL FORENSICS

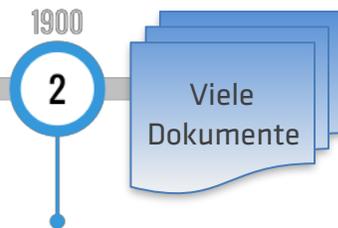


Vernetzte Produktion
Standards
Reale Beispiele

Kommunikationstechnologie in Industrie 4.0

Mechanisierung

- Dampfmaschine
- Webstuhl
- Treibriemenanlage

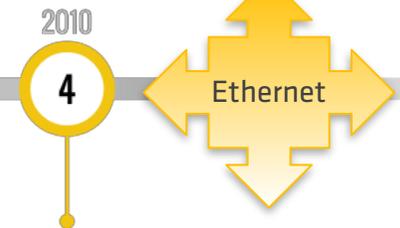
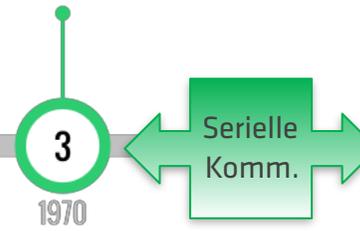


Massenproduktion

- Fließband
- Elektrizität
- Verkehrsmöglichkeiten

Automatisierung

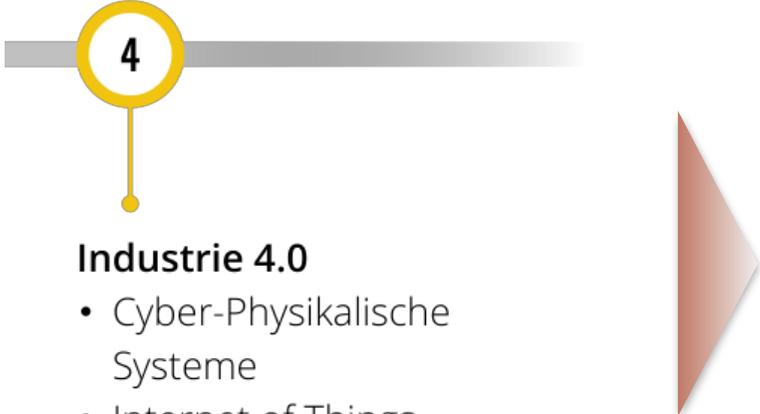
- Computer
- Roboter
- Sensoren



Industrie 4.0

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

Vorteile und Herausforderungen der Industrie 4.0



4

Industrie 4.0

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

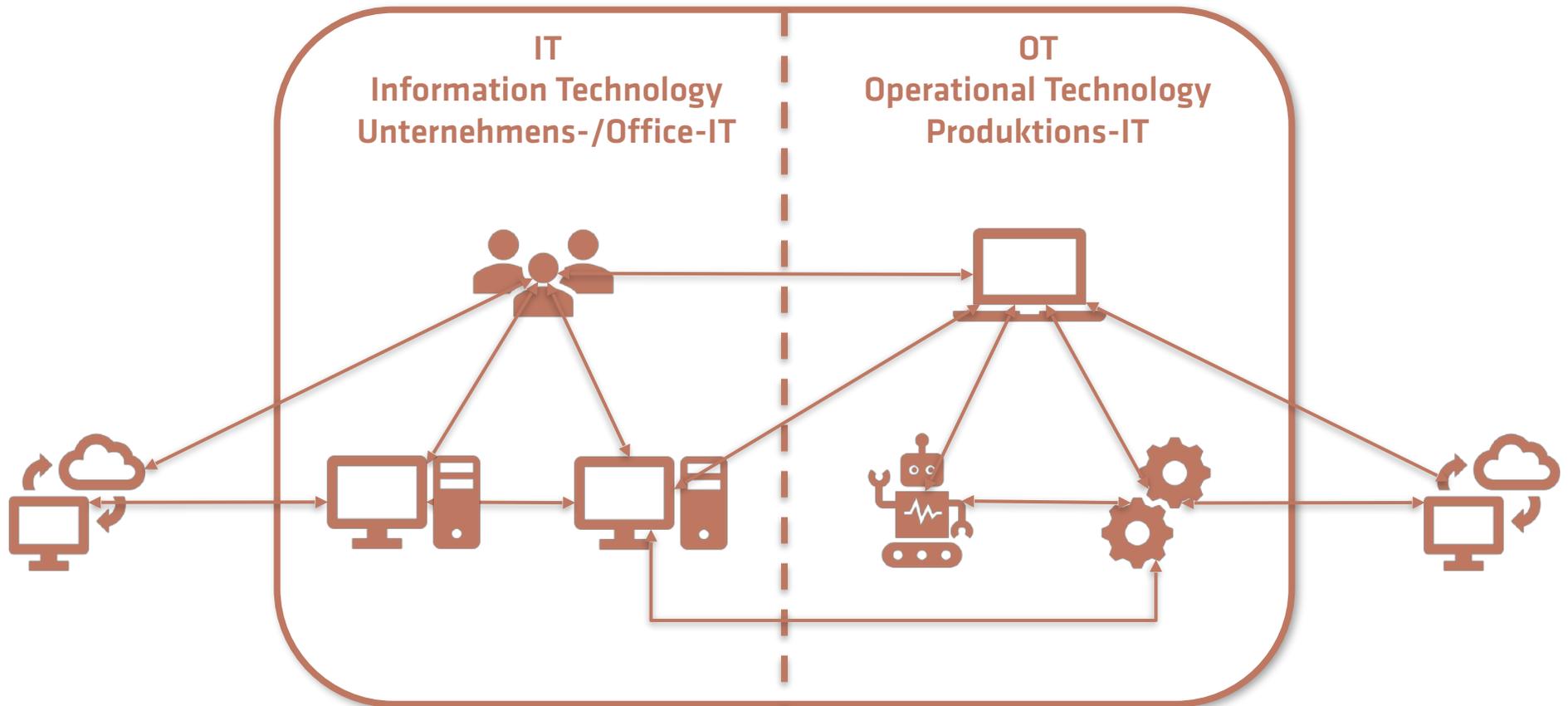
Höhere Flexibilität und Effizienz der industriellen Produktion durch:

- 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



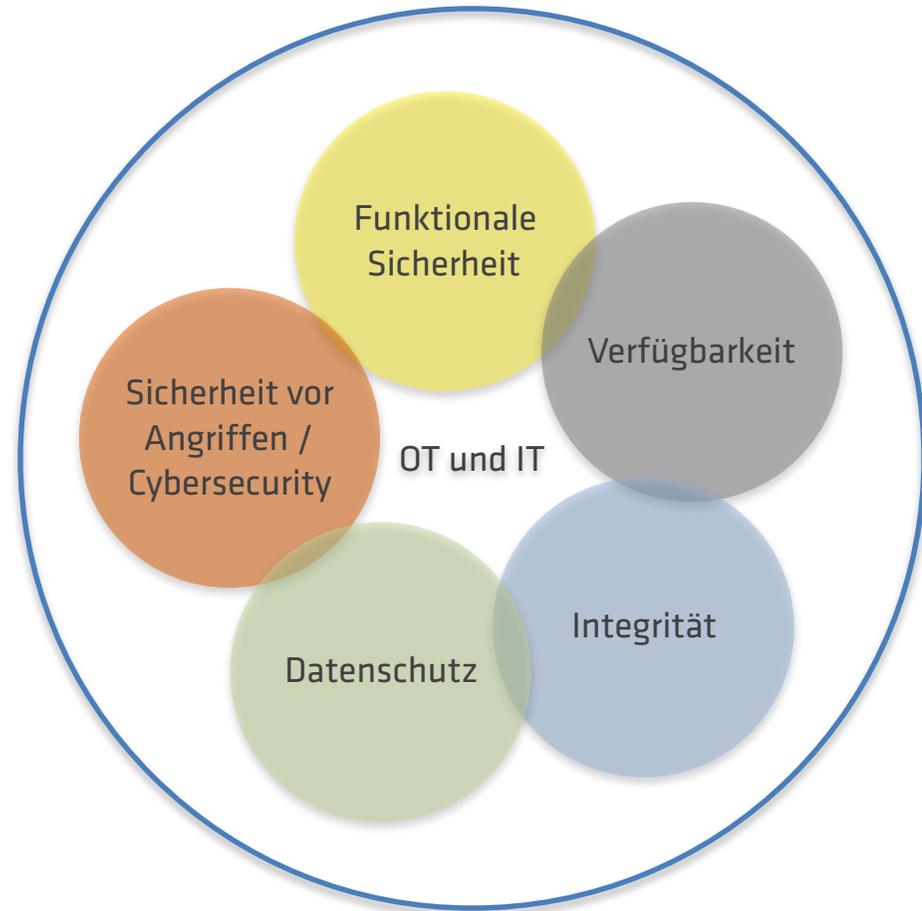
Die Ziele der OT und der IT vereinheitlichen sich

Produktion/ OT:

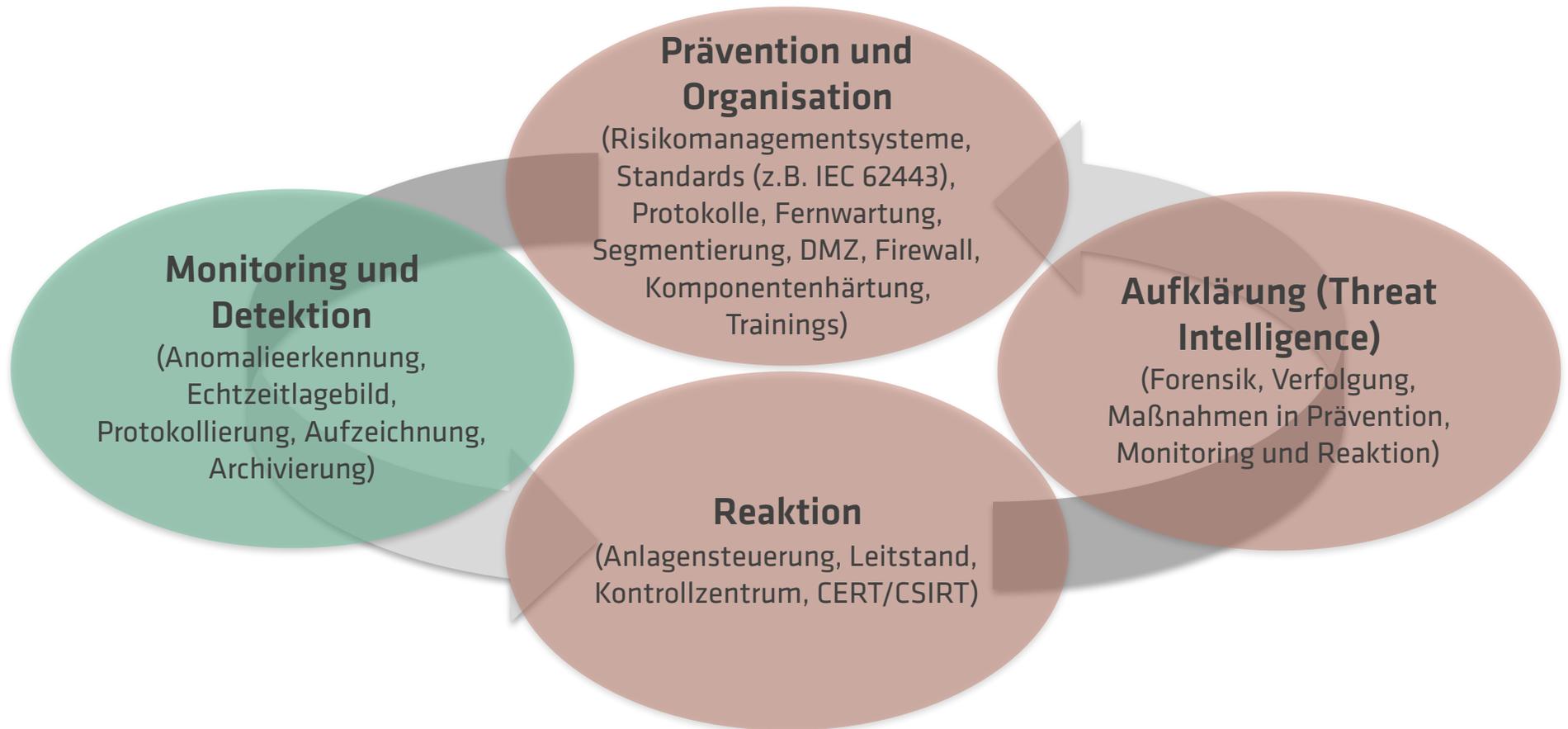
1. Funktionale Sicherheit
2. Verfügbarkeit
3. Integrität
4. Sicherheit for Angriffen

IT Systeme:

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



Sicherheit (und Verfügbarkeit) in der Produktion

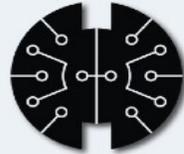


Industrial DPI Decoding Engine

I-DPI State Machine	API Callback 0
Protocol Identifier	Flow Tracker
	Content Decoder



Learning and Analytics Engine



Workflow and Report Center



SIEM and Ticket Systems

ERP and MES

Existing Dashboard / Leitstand

EXTERNAL CONNECTORS

Asset monitoring and Control Systems

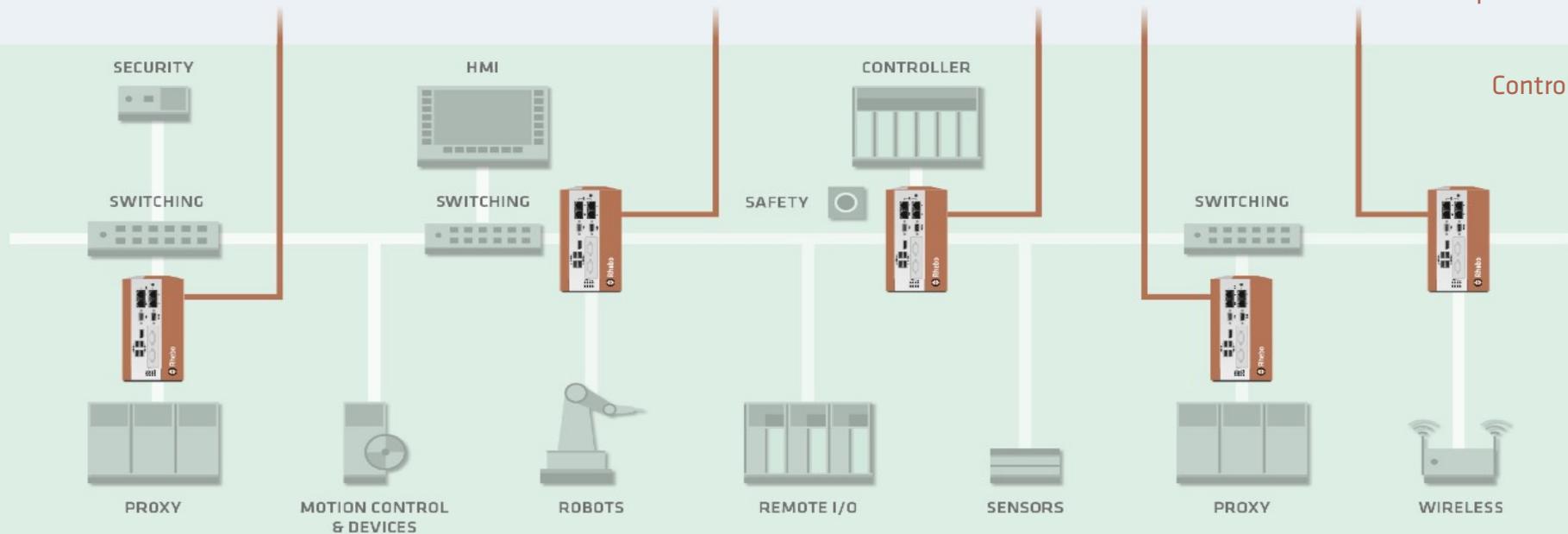
Big Data

RHEBO CONTROLLER



Supervisory Network

Control Network



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...

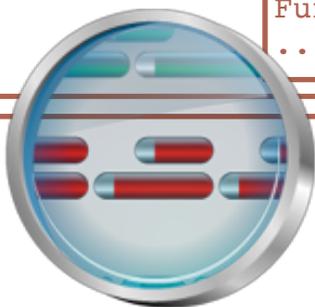
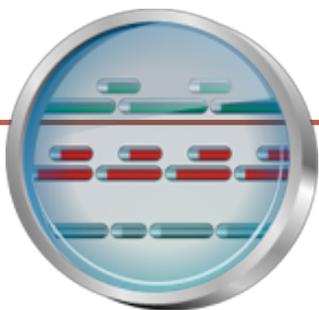
```
Proto=Profinet  
Funct=DCP_Set  
Proto=EtherCAT  
Funct=LogicalWrite  
Proto=DHCP  
Proto=HTTP  
Proto=FTP
```

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

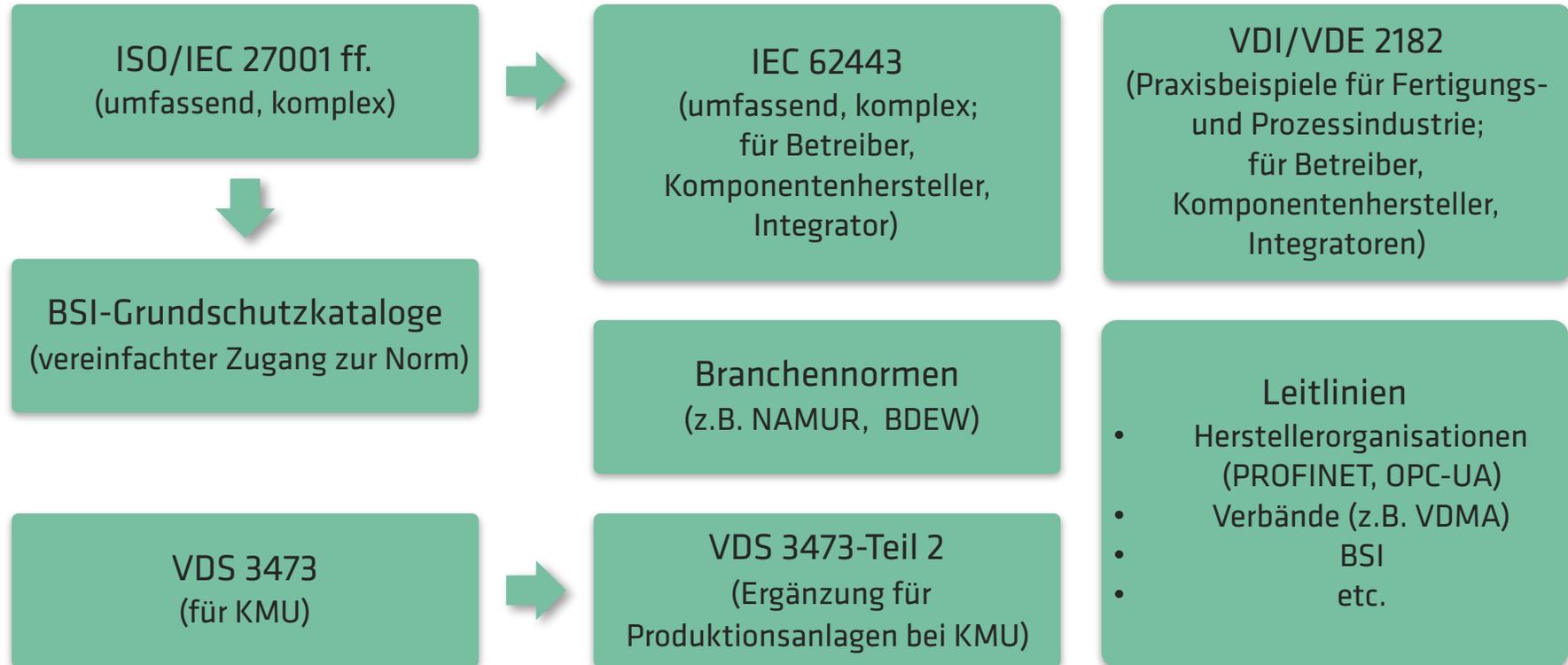
Acronis Backup
Adobe Server
ARP
AXIS Camera
Management
Canon BJNP
CDP
CGMP
Cisco
Cisco DCE
COTP
DCE/RPC
DEC
DHCP
DNS
DTP
ECTP
EGP
EIGRP
FTP Control
FTP Data
HP
HP DTC
HP Extended LLC
HP Probe
HSR
HSRP
HTTP
HTTPS
ICMP
IGMP
IPv6
Kerberos
LDAP
LLC
LLDP
LLMNR
McAfee ePO
mDNS
NetBIOS
NFS
NTP
OSPF
PIM
PTP
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

Office Bereich

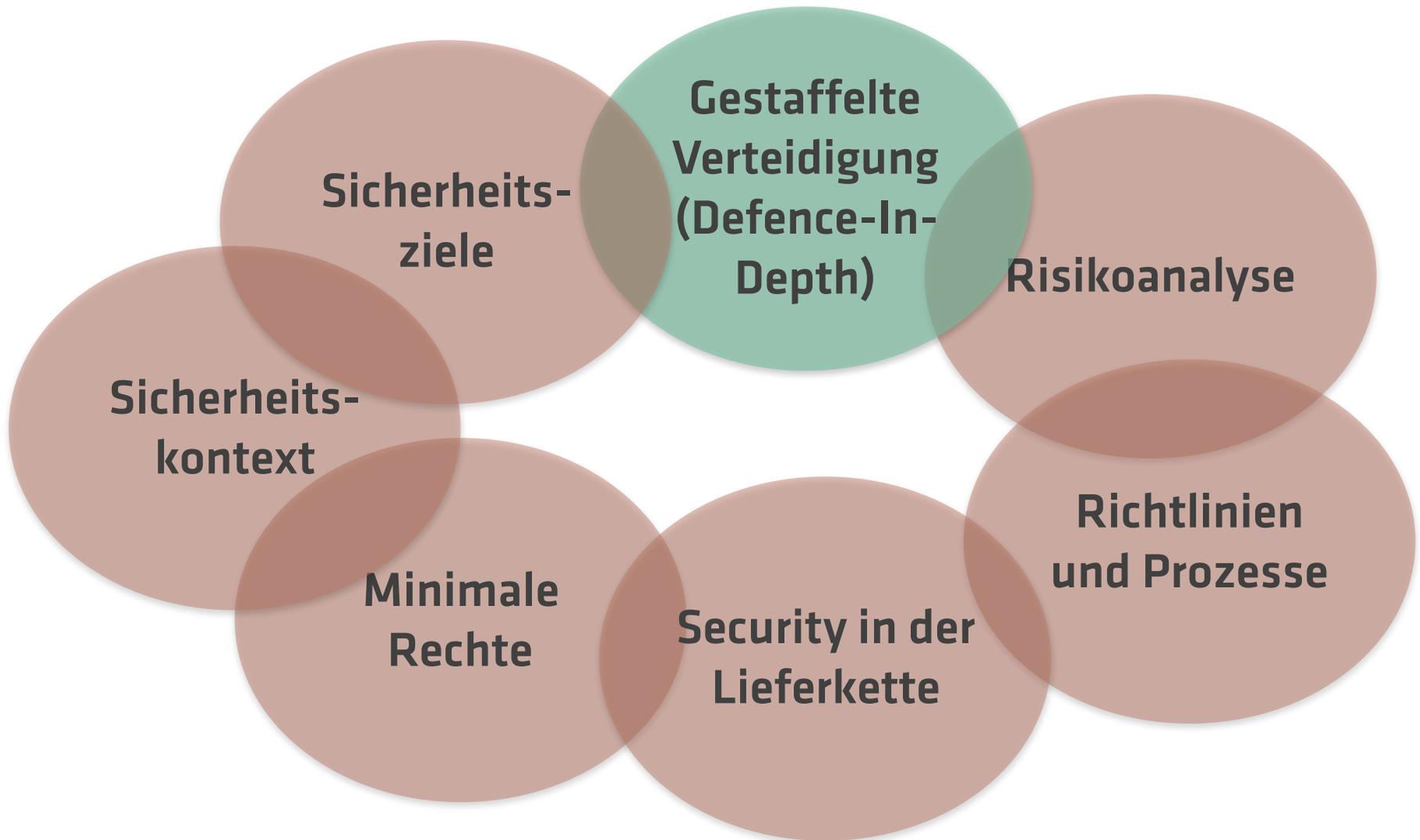
Produktionsbereich



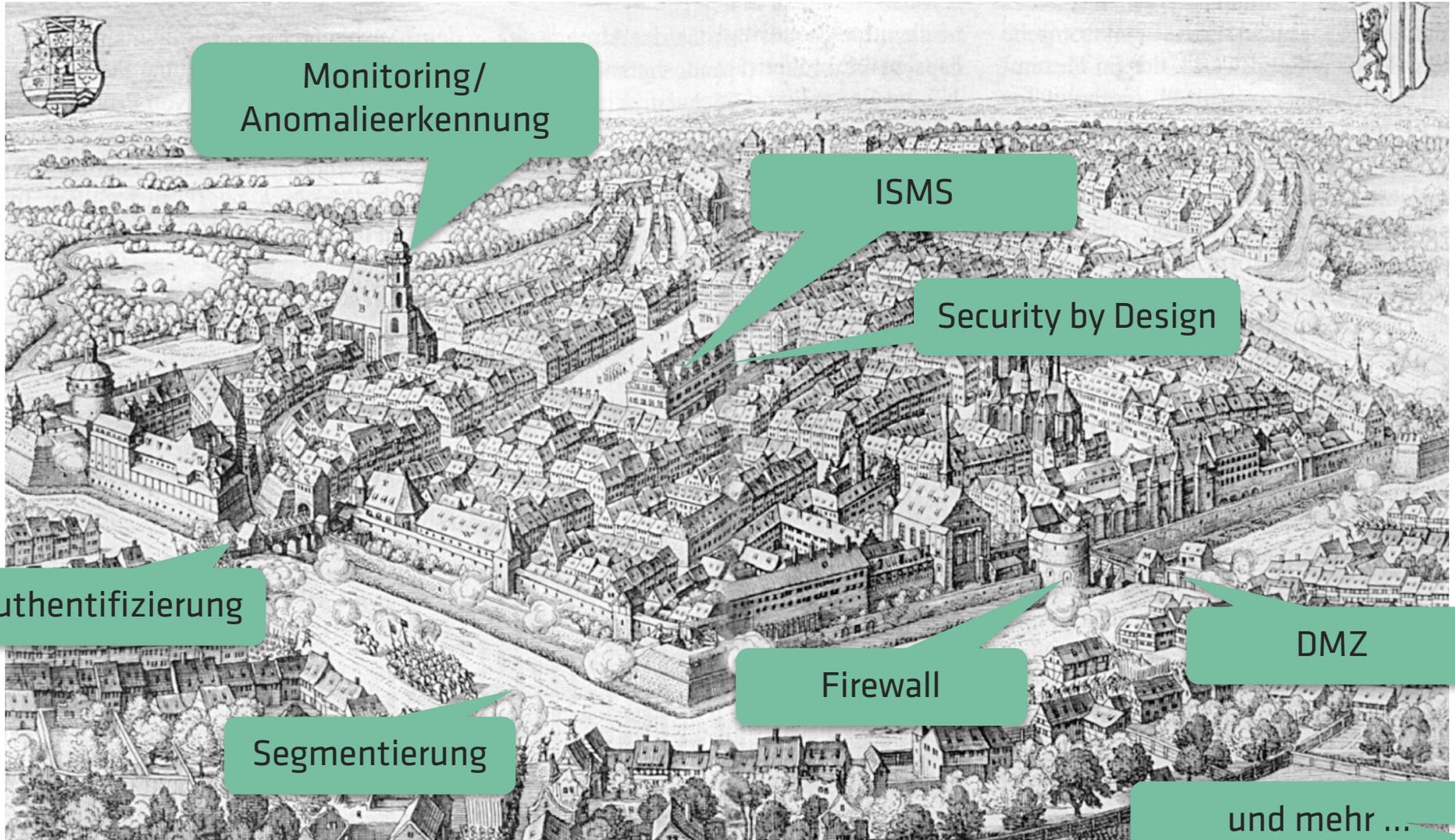
Der (grobe) Weg durch die IEC62443



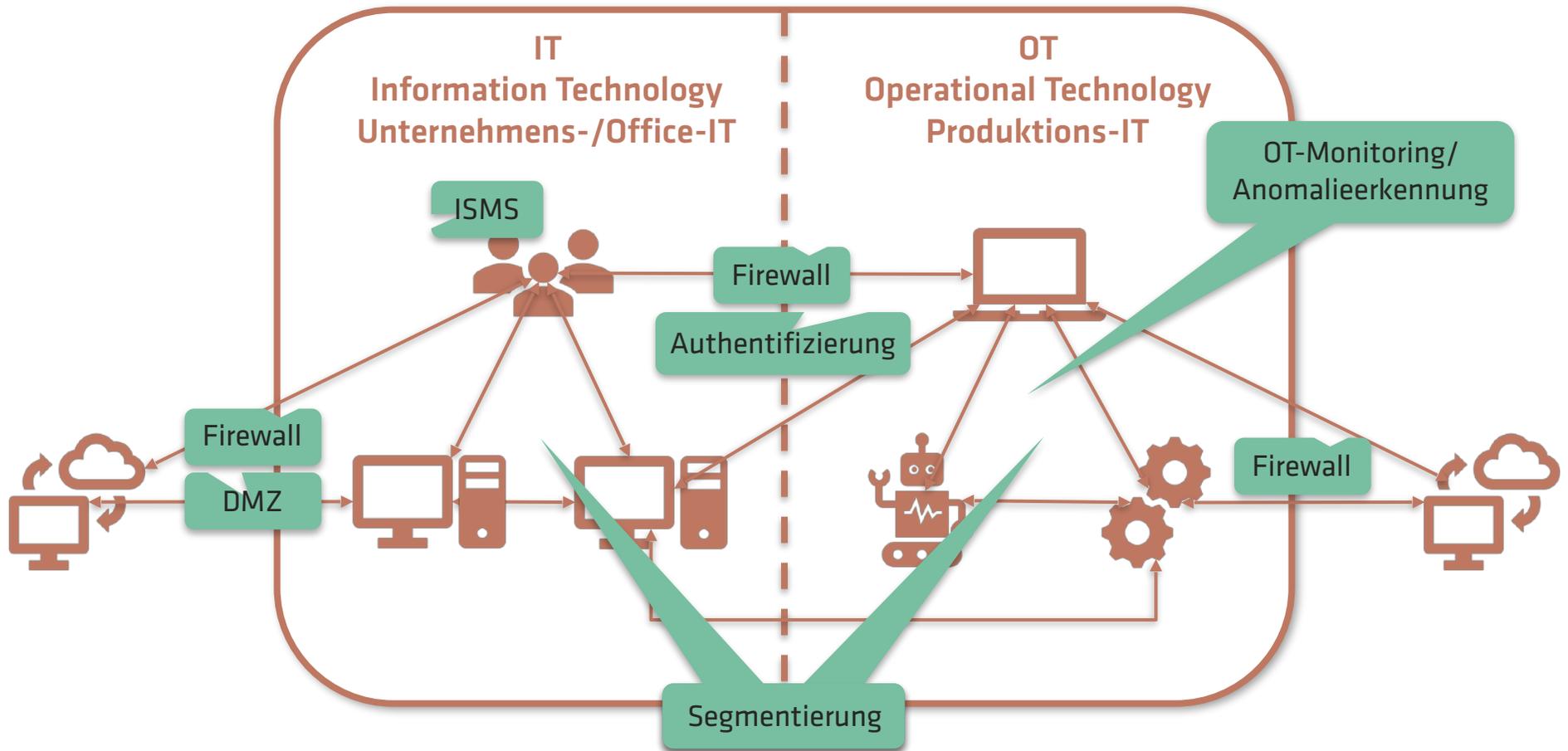
Allgemeine Konzepte (General Concepts)



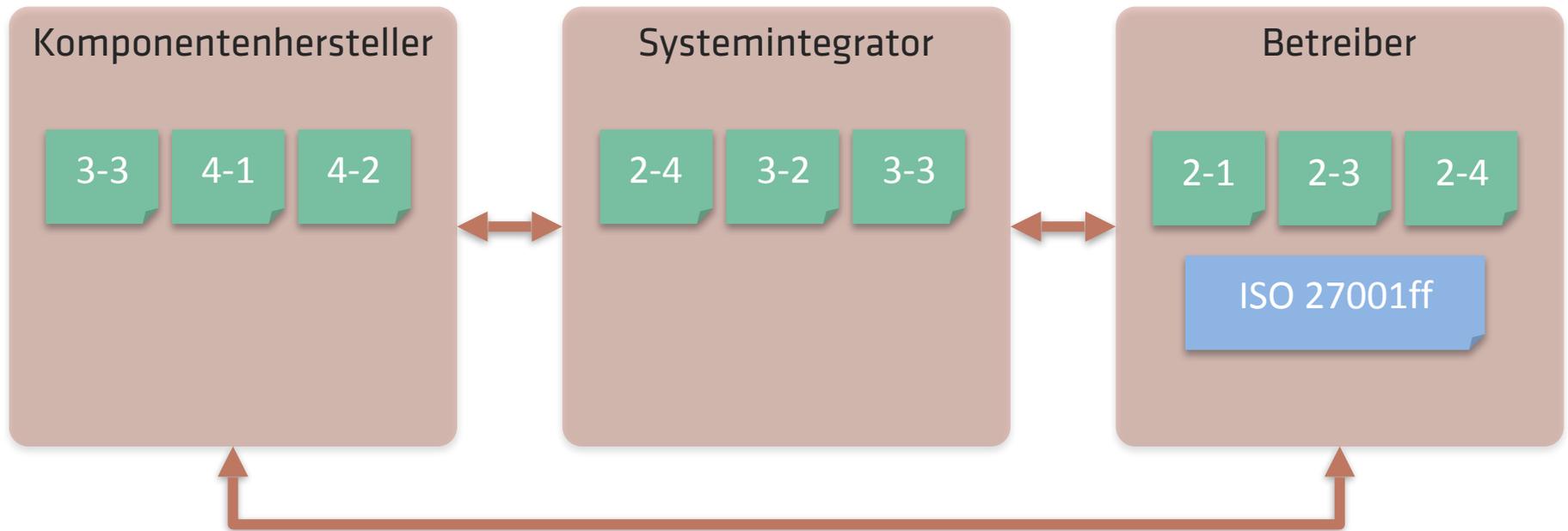
Defence in Depth



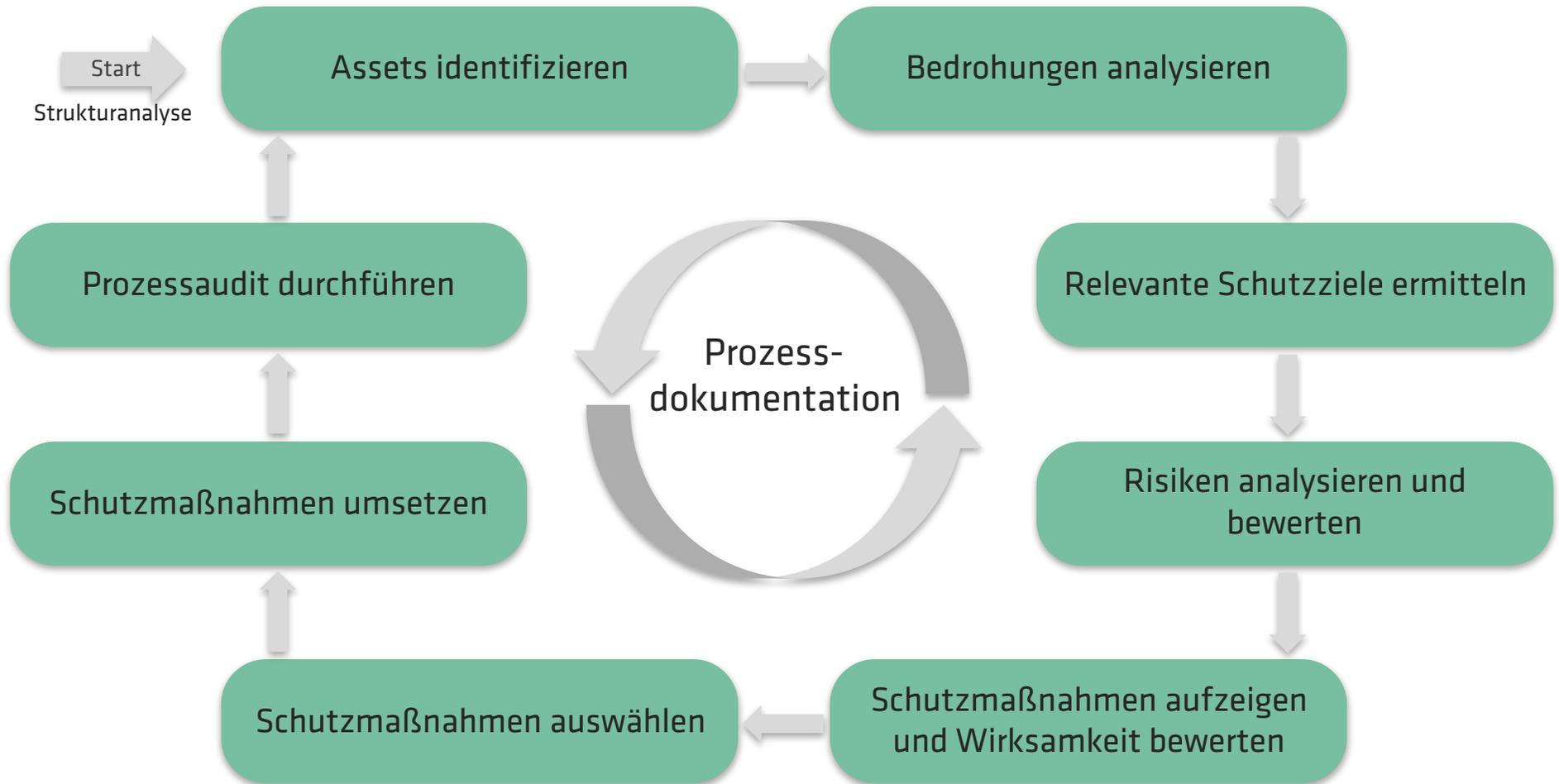
Defence in Depth im Unternehmen



Zusammenspiel der Rollen im Security-Lebenszyklus



PDCA-Vorgehensmodell



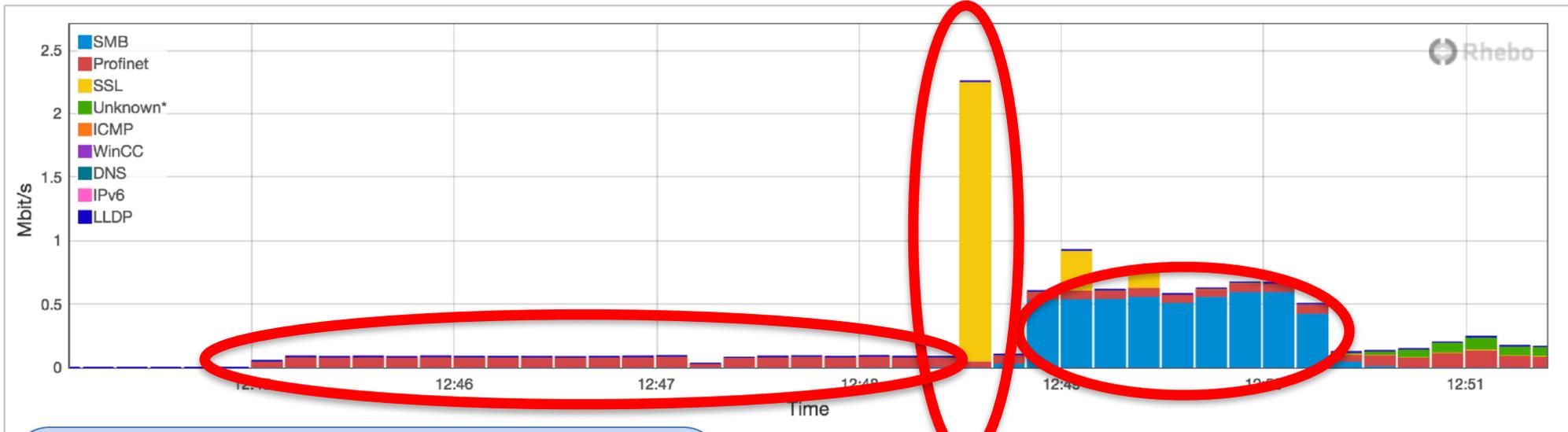
Vorgehensmodell nach VDI_2182_1

Vernetzte Produktion
Standards
Reale Beispiele



Beispiel WannaCry:

“WannaCry hat sich rasend schnell ausgebreitet. ...”



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

Rhebo Industrial Protector v1.6.0-apr1nt.7-0-ga578e90

Notifications (56/13) | Dashboards | Trend Analysis | Hosts | Conversations | Events

Source	Destination	Protocol	Size	Count
00:1b:1b:ba:d0:01	RheboLablOKnot_9	RT CLASS 2 UNICAST	Profinet:	~ 2.5 KB 35
00:1b:1b:be:ef:15	fc:f8:ae:0b:ad:01	RT CLASS 2 UNICAST	Profinet:	~ 66 B 1
RheboLablOKnot_0	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_1	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_2	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_3	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_4	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_6	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_7	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_8	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
RheboLablOKnot_9	fc:f8:ae:0b:ad:01	PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1
00:1b:1b:be:ef:15	fc:f8:ae:0b:ad:01	ARP	Profinet:	~ 49 B 1
fc:f8:ae:0b:ad:01	Broadcast	REPLY	Profinet:	~ 49 B 1
01:0e:cf:00:00:00	fc:f8:ae:0b:ad:01	ARP	Profinet:	~ 49 B 1
		REPLY	Profinet:	~ 49 B 1
		PN DCP SET REQUEST PN DCP IDENTIFY RESPONSE	Profinet:	~ 49 B 1

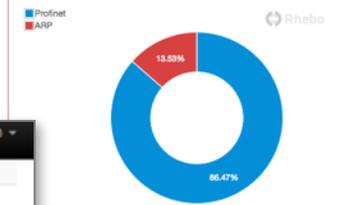
Hosts: Details

- Name: fc:f8:ae:0b:ad:01
- Notifications: 📢 🛡️ 🏠
- MAC address: fc:f8:ae:0b:ad:01
- Vendor: Intel Corporate
- Device type: IO controller

Top Protocols



Top Protocols



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.”

Millionen ICS sind aus dem Internet erreichbar



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

z.B. www.shodan.io

The search engine for **Power Plants**

The search engine for **Buildings**

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

The search engine for **Refrigerators**

Dashboards

Notifications 64 / 6

Devices/Hosts

List

Conversation Map

Network Map

Vendors

Protocols

Conversations

Functions

Administration

Interfaces

rhebo-industrial-protector_0 ...

Host

Not set

Protocols

All

Notifications

🔔 📄 📧 📧 📧

Time window

Last 5 minutes

No profile selected

Devices/Hosts: List

Automatic refresh

Host ^

Impact

Risk Score

Notifications

Vendor

Device Type

Firmware Version

CVEs

Sent

Received

Total

Common Vulnerabilities And Exposures

Host

port-001

Vendor

Siemens AG

Device Type

PC

Firmware Version

Siemens, SIMATIC NET, SCALANCE X202-2P IRT, 6GK5 202-2BH00-2BA3, HW: Version 6, FW: Version V05.01.02, SVPE1192254

CPE

cpe:/h:siemens:scalance_x202-2p_irt:-

CVE

CVE-2013-3633

Severity

High

Exploit Score

8

Impact Score

8.5

Description

The web interface on Siemens Scalance X200 IRT switches with firmware before X-200IRT 5.1.0 relies on client-side privilege checks, which allows remote authenticated users to execute arbitrary commands via unspecified vectors.

Host	Device Type	Firmware Version	CVEs	Sent	Received	Total
WN*				0 B	~ 160.6 MB	~ 160.6 MB
ry Pi ...				~ 351.0 kB	~ 374.1 kB	~ 725.1 kB
WN*				374.1 kB	~ 351.0 kB	~ 725.1 kB
stem...				0 B	79 B	79 B
k Co ...	SUBS			79 B	79 B	79 B
AG PC	PC	Siemens, SIMATIC NE...	High	~ 160.6 MB	0 B	~ 160.6 MB

“Die veraltete Firmware eines Switches im OT-Netz eines Automobilherstellers wies hochrisikoreiche Schwachstellen auf.”

Dashboards

Notifications 33

Devices/Hosts

Protocols

Conversations

Functions

Interfaces

rhebo-industrial-protector...

Host

Not set

Protocols

All

Notifications

Time window

Jan 8, 2019 1:00 AM - Jan ...

No profile selected

Notifications

Inbox 2

Automatically Value Hosts

6:52:54 (1) fg-axx-0

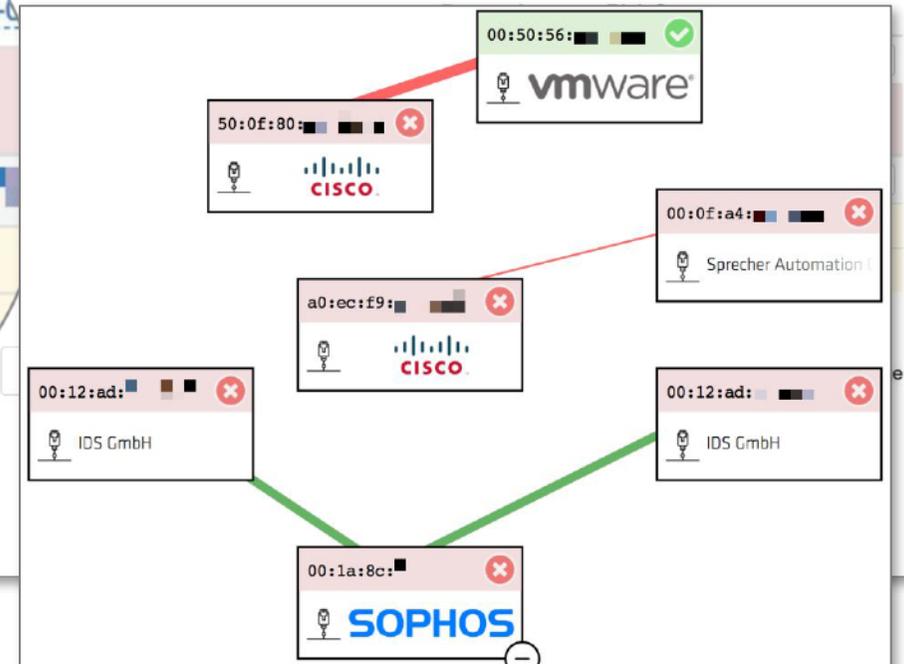
IP address: [redacted]
Message: Plain text password

16:49:30 (2)

Public IP address: [redacted]

Public IP address: [redacted]

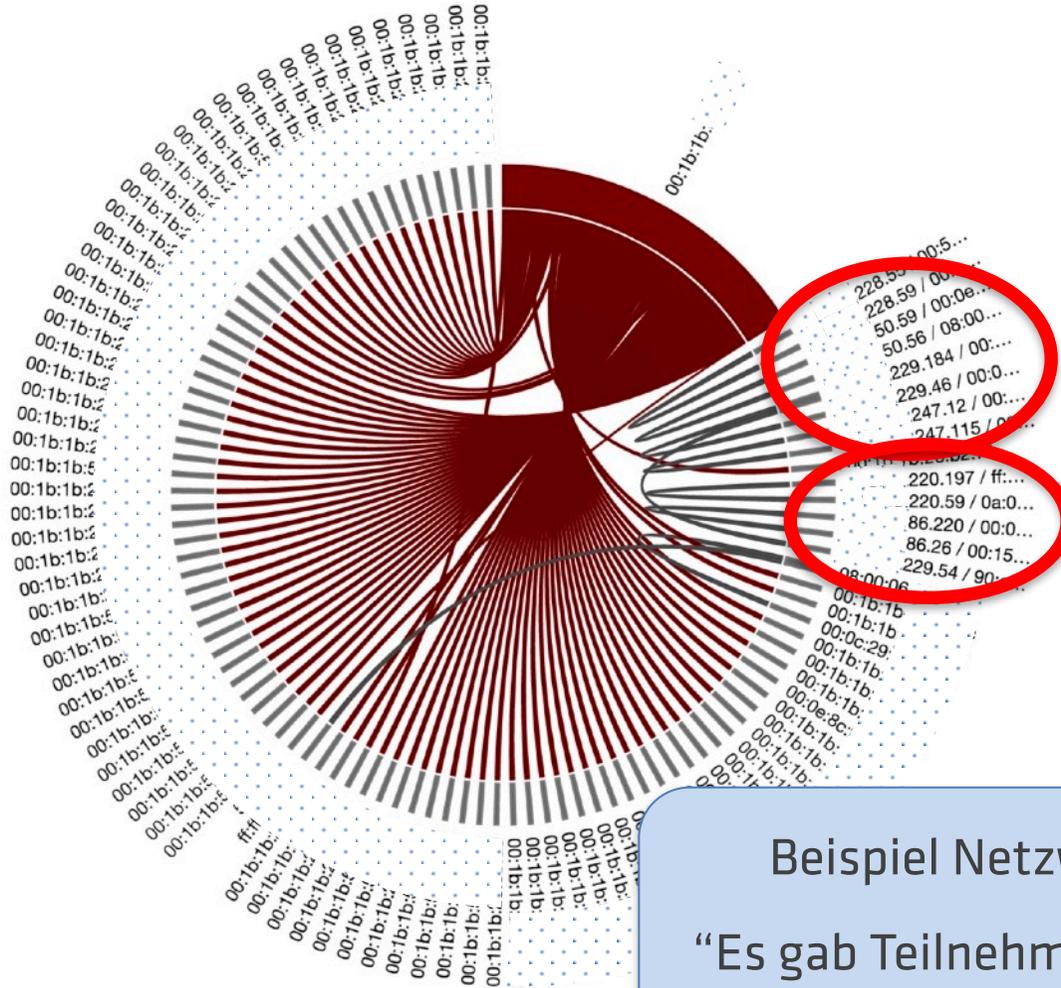
Monitor Clear Export Notifications Maintenance mode



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

- 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."

Notifications (140473/22678)

Dashboards

Trend Analysis

Hosts

Conversations

Events

Administration

Notifications

New Notifications (140473/22678)

Monitored (0/0)

Ignored (0/0)

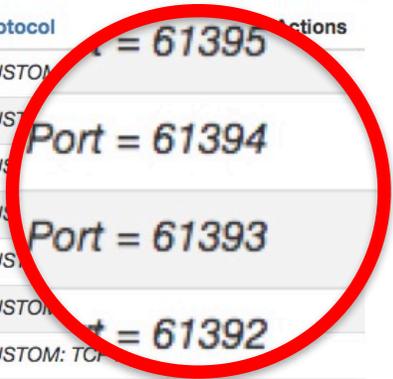
Automatic refresh

Filter: [Icons]

Cyclic message double, [Dropdown]

Monitor Ignore Ignore displayed

Timestamp	Value	Hosts	Protocol	Actions
2016-08-08 22:54:23	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61395	
2016-08-08 22:54:23	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61394	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61393	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61392	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61389	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61377	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61376	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61375	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61351	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61350	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61349	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61348	
2016-08-08 22:54:22	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61347	
2016-08-08 22:53:41	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61346	
2016-08-08 22:53:41	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61345	
2016-08-08 22:53:41	[Icon]	32.218 / 00:e0:e4:2d:c2:5d	CUSTOM: TCP Port = 61344	



Beispiel Vermutlicher Angriff:
 “Es schaut aus wie ein Port-Scan, und
 eventuell ein Angriff oder dessen
 Vorbereitung.”

Rhebo Industrial Protector v1.4.2-0-g850c37a

Notifications (140473/22678)

Dashboards

Trend Analysis

Hosts

Hosts: Details

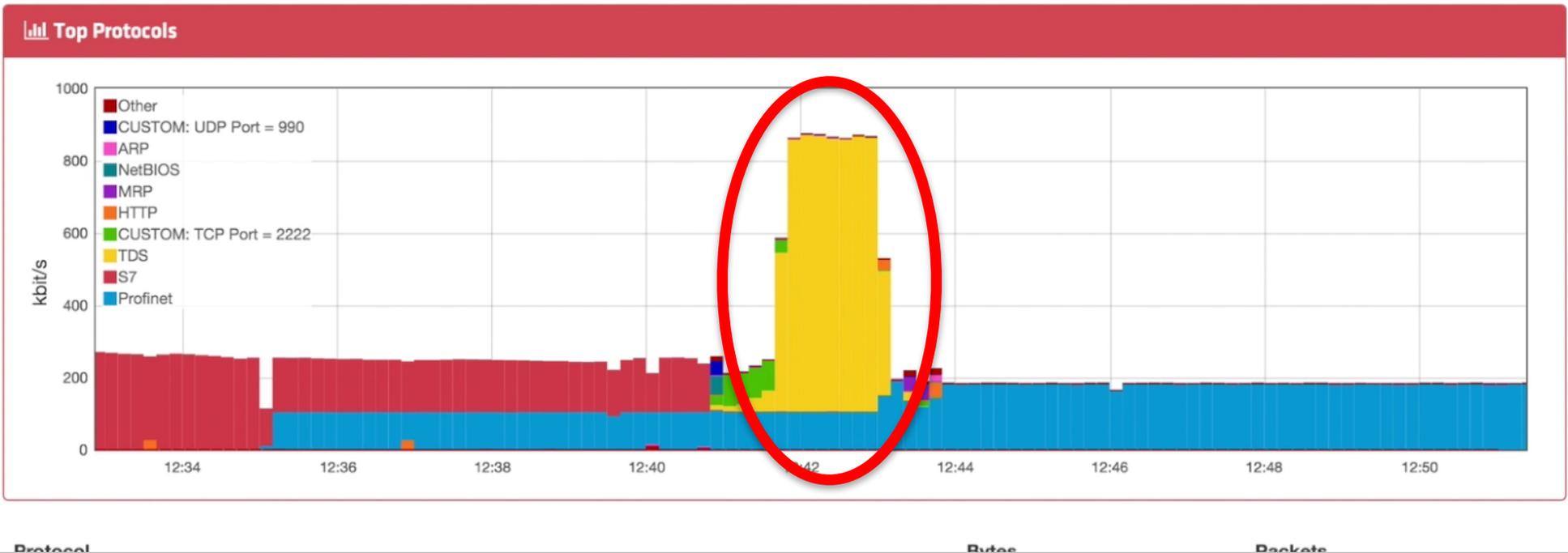
- Name: 192.168.1.32.218 / 00:e0:e4:2d:c2:5d
- IP address: 192.168.1.32.218
- MAC address: 00:e0:e4:2d:c2:5d
- Vendor: FANUC ROBOTICS NORTH AMERICA, Inc.

Top Protocols

“... 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



Rhebo Industrial Protector v2.0.0

Help admin

Notifications 4/2

Interfaces: rhebo_0 (81:90:b3:09:79:a9) Host: Not set Protocols: All Notifications: Time window: Feb 28, 2018 12:00 AM - Mar ...

Notifications

Inbox 4/2 Monitored 0/0 Cleared 335/61

Automatic refresh

Monitor Monitor filtered Clear Clear filtered Export Notifications

First occurrence	Last occurrence	Protocol	Risk Score
2018-02-28 14:17:40	2018-02-28	Veritas	5.1
2018-02-07 09:25:53	2018-02-07	Profinet	5.1
			5.1
			5.1
			5.1

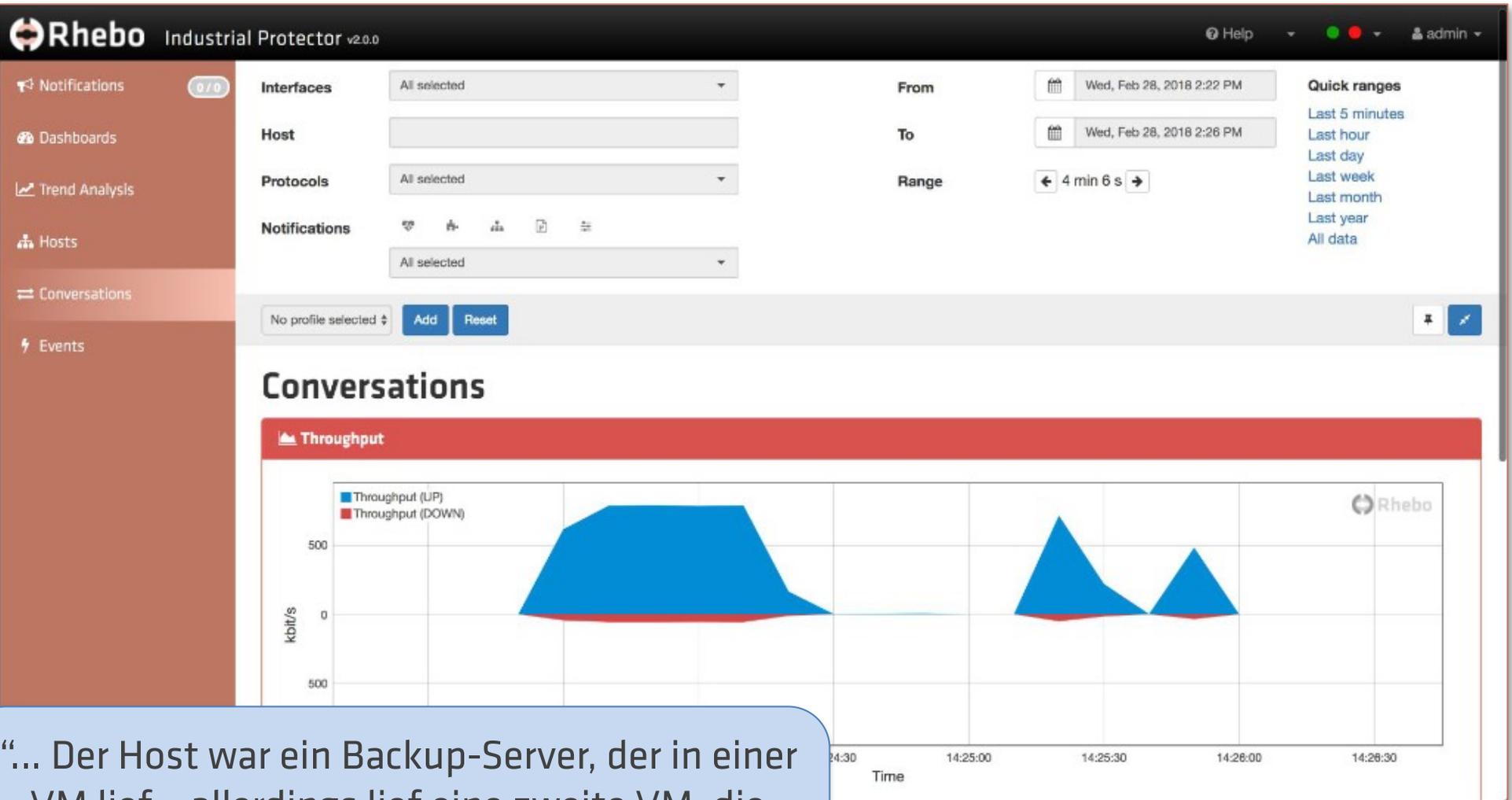
IP address: 172.16. Message: TCP window of size 0

MAC address: 00:1b:1b: address: 28:63:36: Protocol: Profinet

MAC address: 28:63:36: Protocol: Profinet

10 rows per page

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.”

Dashboards

Meldungen 780 / 152

Endgeräte/Hosts

Protokolle

Interfaces

rhebo-industrial-pr...

Endgerät

Nicht gesetzt

Protokolle

VNC

Meldungen

Icons for various actions

Zeitfenster

14. Sep. 2018 10:00...

Kein Filterprofil ausgewählt

Meldungen

Eingang 20 / 6

Überwacht 0 / 0

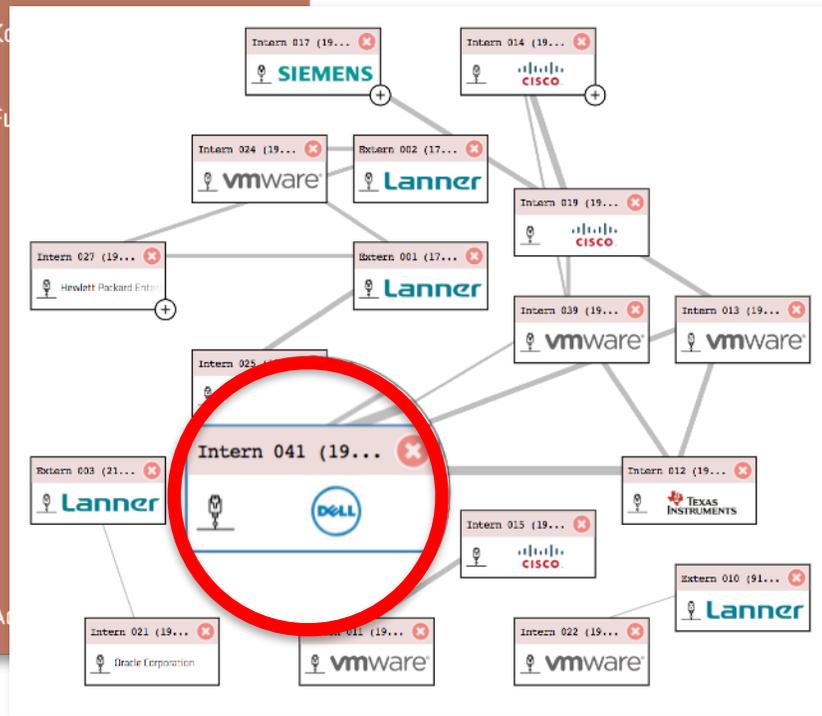
Quittiert 0 / 0

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 012 (192.168.100.105) Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
Intern 012 (192.168.100.105) Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
Intern 012 (192.168.100.105) Intern 041 (192.168.100.163)	VNC	PCAP herunterladen



Beispiel Sabotage:
 "VNC wurde zur Remote-Wartung eingesetzt – durchaus erlaubt ..."

```
1 #!/usr/bin/env python3
2 # -*- coding: utf-8 -*-
3
4 import sys
5 import binascii
6 from scapy.all import sniff, TCP, Raw
7
8
9 VNC_CODES = {'ff08': 'Backspace',
10             'ff09': 'Tab',
11             'ff0d': 'Return/Enter',
12             'ff1b': 'Escape',
13             'ff63': 'Insert',
14             'ffff': 'Delete',
15             'ff50': 'Home',
16             'ff57': 'End',
17             'ff55': 'Page-Up',
18             'ff56': 'Page-Down',
19             'ff51': 'Left',
20             'ff52': 'Up',
21             'ff53': 'Right',
22             'ff54': 'Down'}
23
24 PORT_RANGE_TCP = list(range(5981, 5999))
25 PORT_RANGE_HTTP = list(range(5801, 5899))
26
27
28 def parse_vnc(raw_payload):
29
30     decoded = binascii.hexlify(raw_payload).dec
31
32     if len(decoded) == 16 and decoded[1] == '4':
33         try:
34             if decoded[-4:] in VNC_CODES:
35                 key_stroke = VNC_CODES[decoded[-4:]]
36                 print('{0}'.format(key_stroke))
37             else:
38                 key_stroke = binascii.unhexlify
39                 print(key_stroke, end='', flush
40
41         except UnicodeDecodeError:
42             print('!-!')
43
44
45 def callback(rawPacket):
46
47     if rawPacket.haslayer(TCP):
48         srcPort = rawPacket.getlayer(TCP).sport
49         dstPort = rawPacket.getlayer(TCP).dport
50
51         if (srcPort in PORT_RANGE_TCP
52             or dstPort in PORT_RANGE_TCP):
53
54             if rawPacket.haslayer(Raw):
55                 parse_vnc(rawPacket.getlayer(Raw).load)
56
57
58 sniff(offline=sys.argv[1], store=0, prn=callback)
```

```
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):
```

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

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



**WISSEN SIE, WER SICH
IN IHRER INFRASTRUKTUR
HERUMTREIBT?**



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