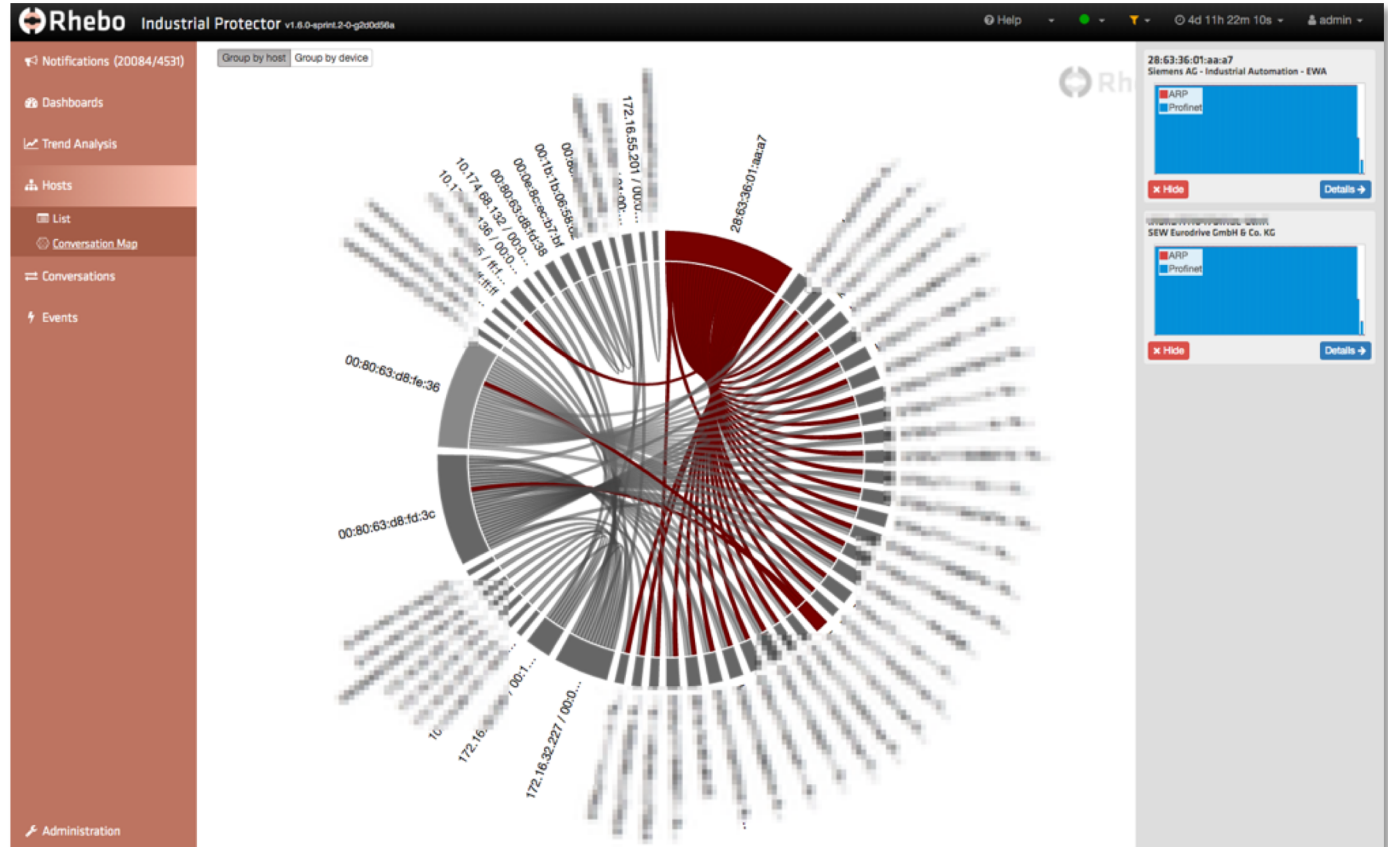


**GEFAHREN IN
INDUSTRIESTEUERUNGSANLAGEN
SCHNELL ERKENNEN UND
PRODUKTIVITÄT ERHÖHEN**

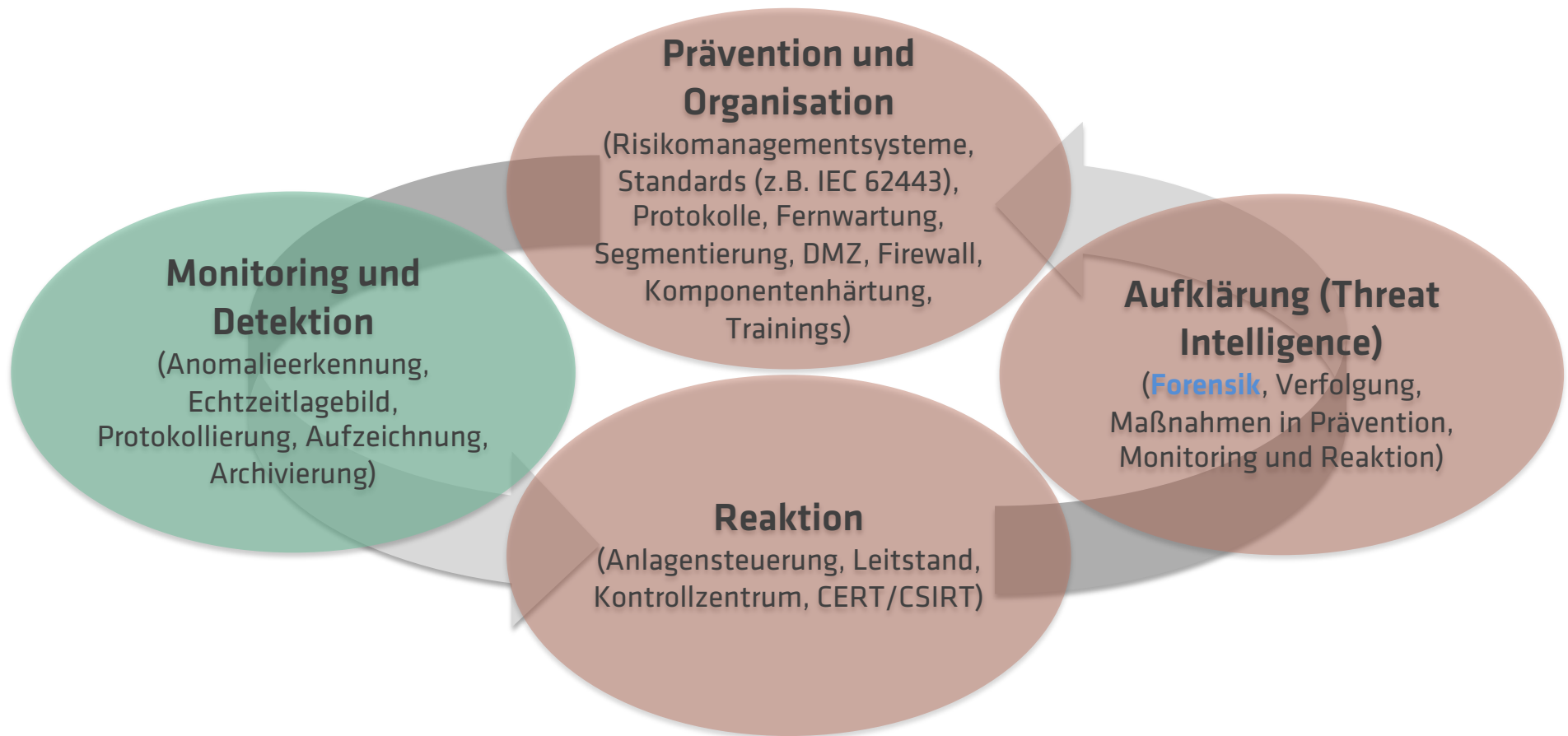
Der Vernetzungsgrad steigt immer weiter

Eine typische Zelle heute:

- Dutzende bis hunderte Komponenten
- Zunehmende Verbreitung von Ethernet
- Ein Fehler, dutzende verschiedene Punkte für Auswirkungen
- ...



Sicherheit und Verfügbarkeit in der Produktion



Dashboards

Notifications

105 / 32

Devices/Hosts

Protocols

Conversations

Functions

Interfaces

rhebo-industrial-protect_0 ...

Host

Not set

Protocols

All

Notifications

[Icons: Heart, Plus, User, Document, List]

Time window

Last 5 minutes

No profile selected

Notifications

Inbox

105 / 32

Monitored

3 / 3

Cleared

0 / 0

Automatic refresh

Clear

Clear filtered

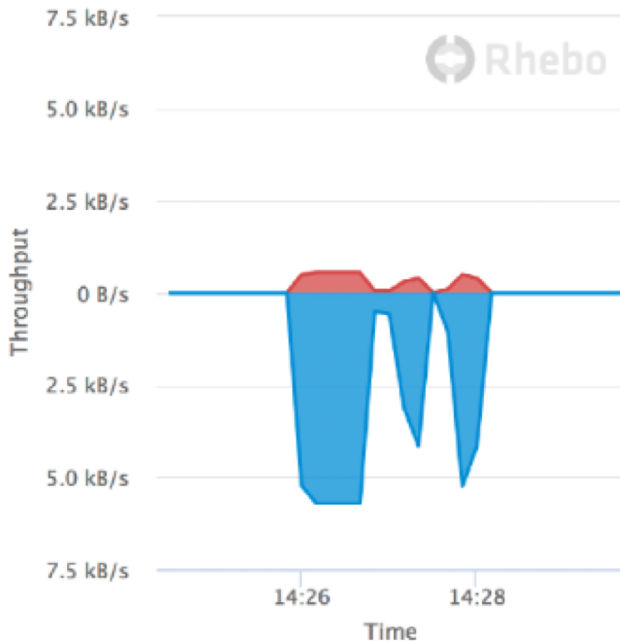
Export Notifications

☐	First occurrence	Last occurrence	☒ Value	Hosts	Protocol	Count	Risk Score	
☐	2018-11-14 14:26:01	2018-11-14 14:28:08	☒ (1)	192.168.1.100	HTTP	53	5.1	Download PCAP
	IP address: 192.168.1.100 Message: TCP checksum error							
☐	2018-11-14 14:26:01	2018-11-14 14:28:08	☒ (1)	192.168.1.100	HTTP	21	5.1	Download PCAP
	IP address: 192.168.1.100 Message: Duplicate TCP Acknowledgement							
☐	2018-11-14 14:26:01	2018-11-14 14:28:08	☒ (1)	192.168.1.100	HTTP	53	5.1	Download PCAP
	IP address: 192.168.1.100 Message: TCP Retransmission							

10 rows per page

Beispiel defekter Switch im Produktionsnetz eines Autobauers:
 "TCP-Prüfsummenfehler und erneute Übertragungsversuche
 häufen sich zu gewissen Zeiten und sind damit ein Hinweis auf
 fehlerhafte Übertragungen."

Throughput



● Throughput (DOWN) ● Throughput (UP)

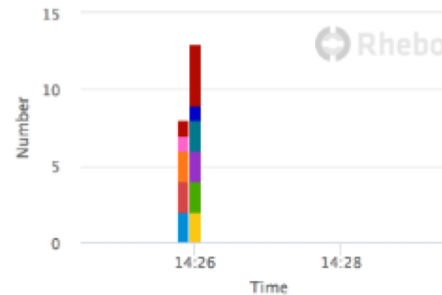
Notifications

Time window

Last 5 minutes

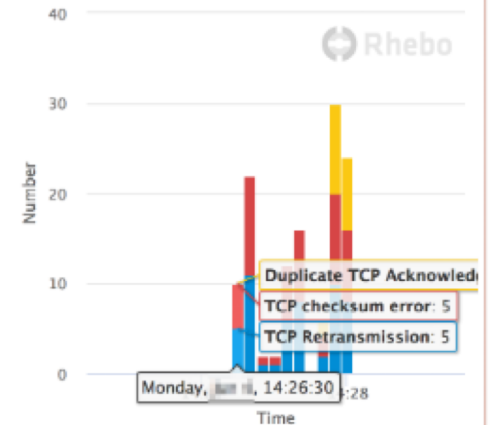
No profile selected

Unique inbox notifications by type



- IP
- IP and MAC
- IP and function
- IP and protocol
- MAC
- MAC and function
- MAC and protocol
- IP pair
- IP pair and function
- Other

Recurring monitored notifications by



- TCP Retransmission
- TCP checksum error
- Duplicate TCP Acknowledgement

Protocol

Sent

Received

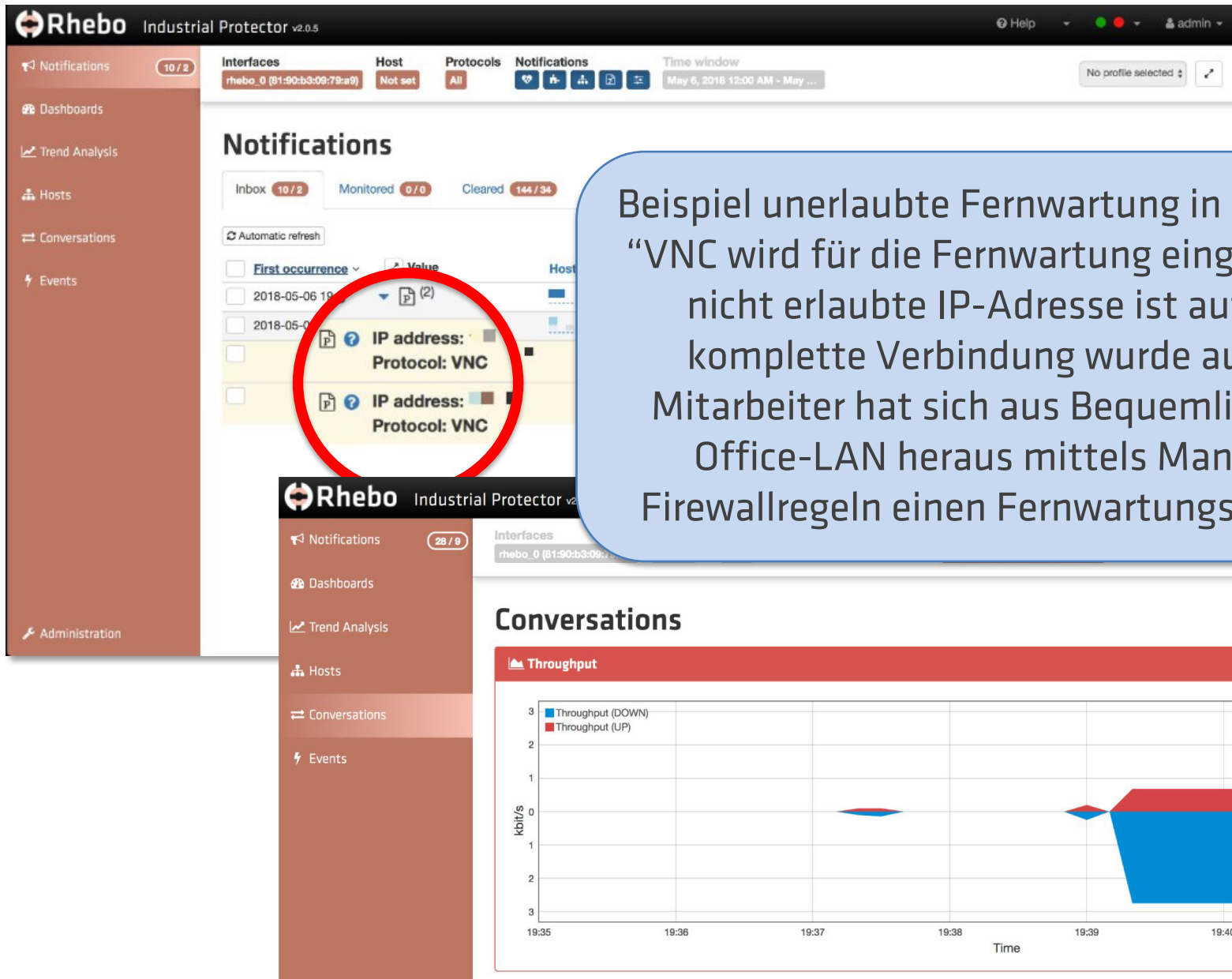
Total

Details

~ 64.2 kB

i

“... Die wiederkehrenden Vorgänge konnten auf einen Wartungsrechner eingegrenzt werden. Offenbar war ein Switch im Kommunikationsweg defekt. Dieser wurde ausgetauscht. Das Problem ist behoben.”



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

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.

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...		B	0 B	79 B
k Co SUBS			79 B	79 B
AG PC	Siemens, SIMATIC NE...	High	0.6 MB	0 B
			~ 160.6 MB	

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

Anlagenverfügbarkeit

Stabilität

Cybersicherheit

Steuernetzüberwachung & -analyse

- ✓ Vollständige digitale Transparenz
- ✓ Echtzeiterkennung von (Sicherheits-)Anomalien
- ✓ Forensische Analyse und Compliance



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



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