Rhebo

a Landis+Gyr company

CYBERSECURITY MADE IN EUROPE™

Initiated by ECSO. Issued by eurobits e.V.

Die aktuelle Lage der OT-Sicherheit – Warum Made in Germany Lösungen relevanter werden

itsa 365 IT Security Talk: OT-Security, 29. April 2025, Dr. Frank Stummer

Die Quellen zu den in den folgenden Folien zitierten Daten und weiteres Material finden Sie im Rhebo-Whitepaper “Die Lage der OT-Security 2024/2025”.

Link zum Download:

https://www.rhebo.com/de/downloads/die-lage-der-ot-cybersicherheit-2024-2025---metriken-und-trends-global-und-lokal

Schlaglichter aus der globalen Sicht auf die OT-Sicherheit

76 Berichte über spezifische OT-Cyberangriffe

57% betreffen kritische Infrastrukturen

437 ICS-Advisories (nur CISA)

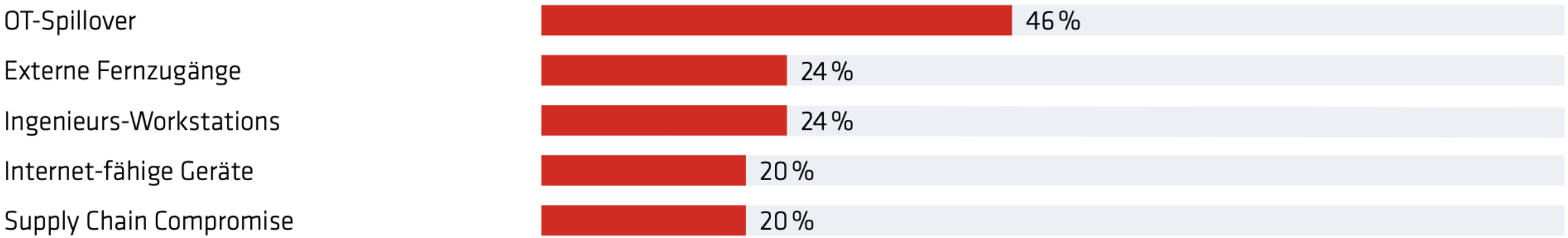
45% hatten/ befürchten Betriebsstörungen, 70% haben Fachkräftemangel


CYBER CRIME
CYBER CRIME
CYBER CRIME

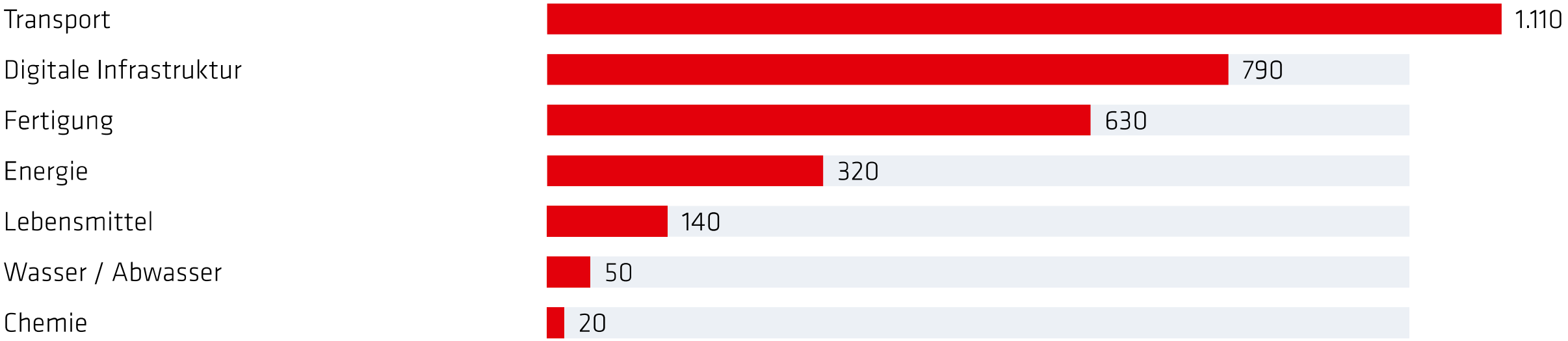

Cyber Dominance


CYBER WAR

Top 5 der initialen Angriffsvektoren auf Industrieanlagen



Von Cyberangriffen betroffene Sektoren in der EU



Schlaglichter aus deutscher Sicht

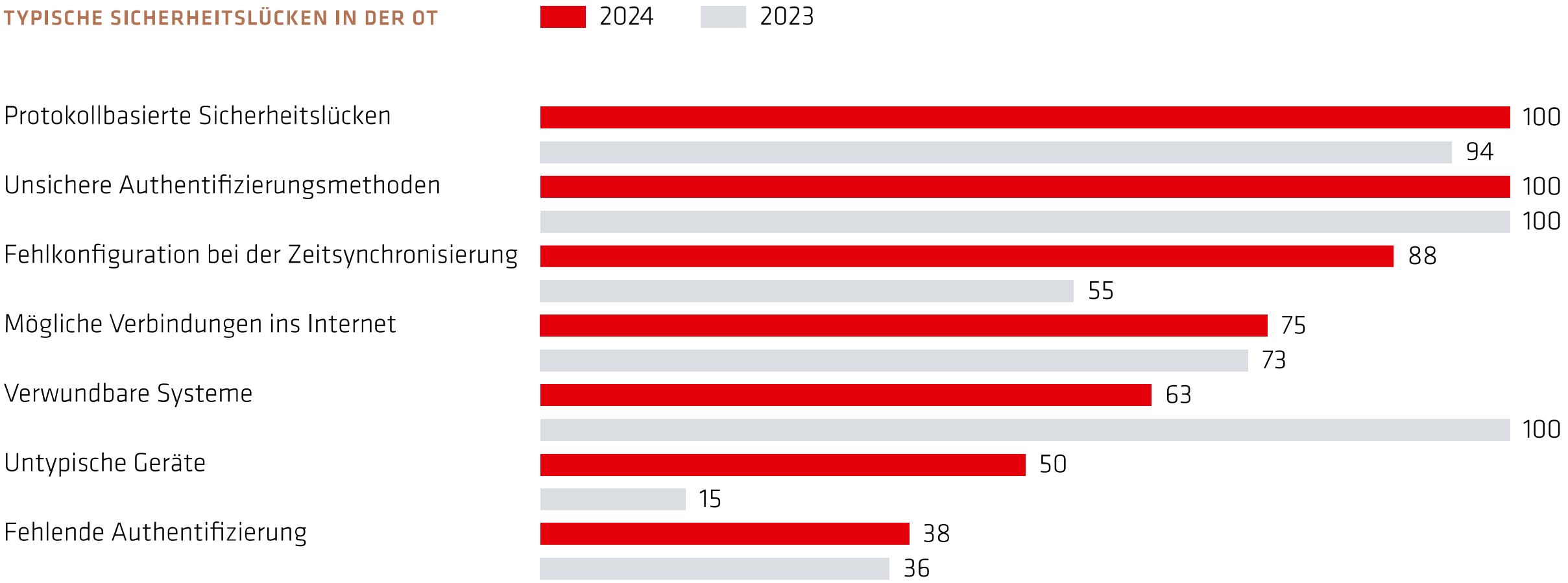
Nr. 2 der angegriffenen Länder weltweit

144 Akteure mit Deutschland als Ziel

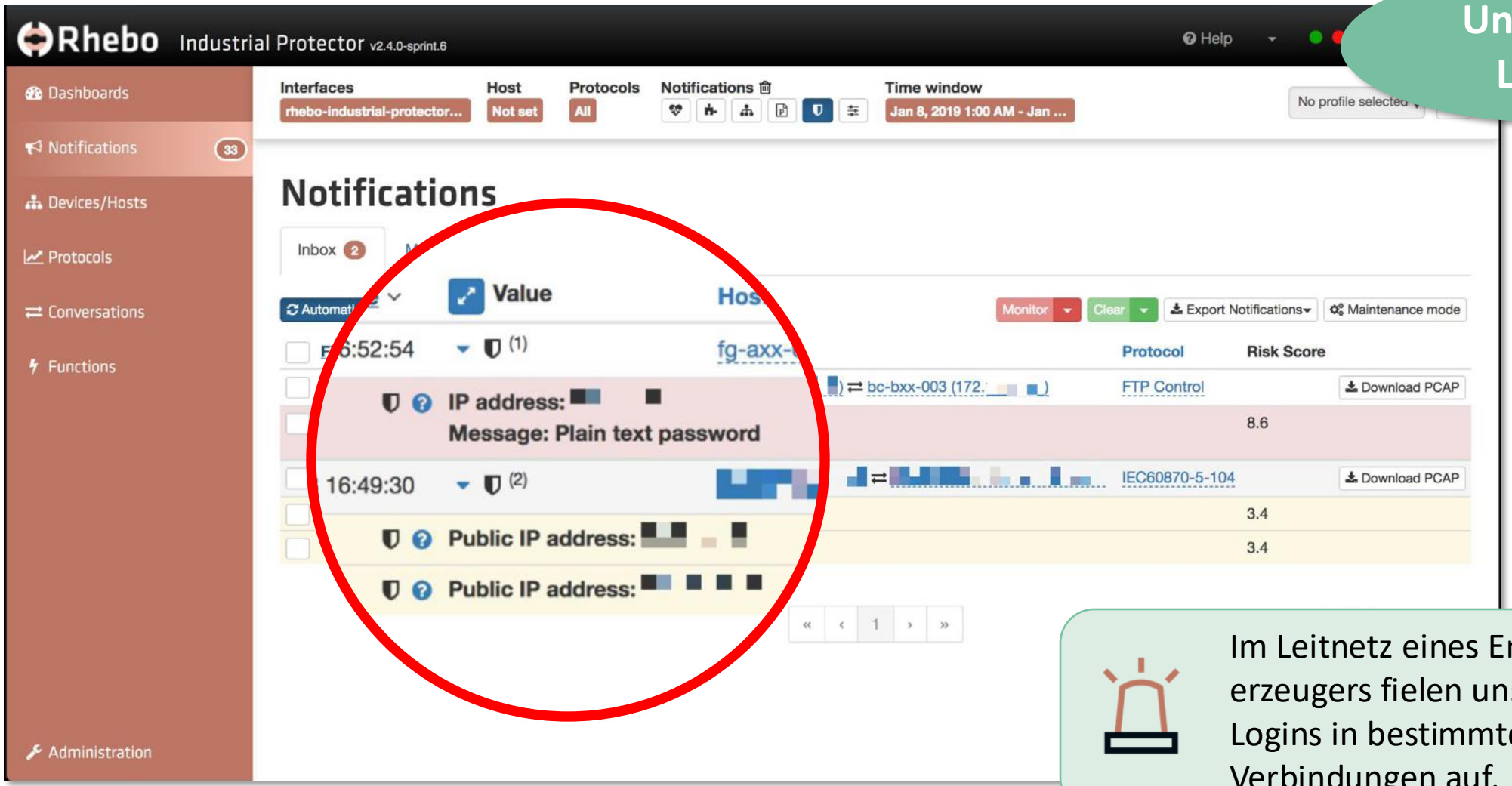
140 von 671 KRITIS konnten ihr ISMS verbessern

69% haben noch nicht alle MUSS-Anforderungen an ein SzA umgesetzt

Ergebnisse aus Rhebo Sicherheits- und Stabilitätsreports



Unsichere Logins



Im Leitnetz eines Energieerzeugers fielen unsichere Logins in bestimmten Verbindungen auf.

Schwachstellen

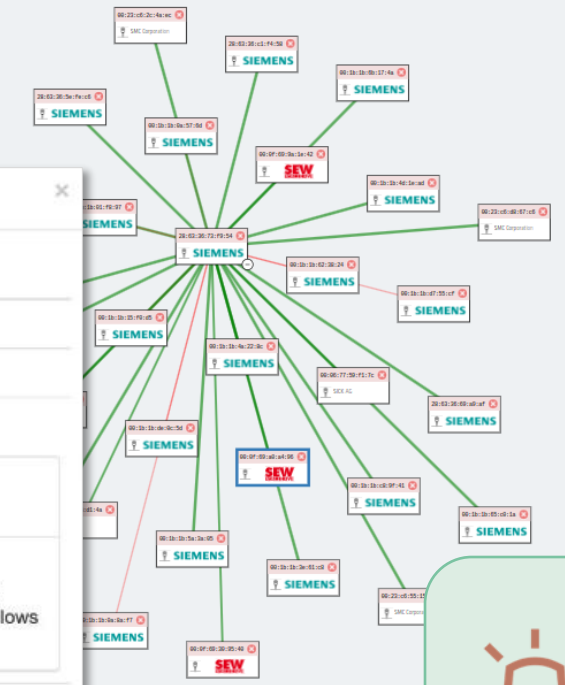
Rhebo
a Landis+Gyr company

Industrial Protector v3.5.0 rhebo-controller

Events | Interfaces: All | Host: Not set | Protocols: All | Notifications | Time window: Mar 27, 2024, 3:16 PM - Mar 27, 2024, 3:20 PM

- Dashboards
- Inbox 32
- Devices/Hosts
  - List
  - Conversation Map
  - Network Map
  - Vendors

Group by device | Group by host | Display network quality



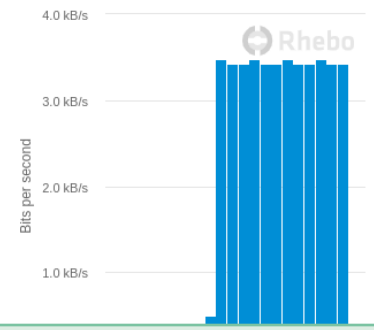
9.1

00:0f:69:a0:a4:96

IP address	MAC address
-	00:0f:69:a0:a4:96
Vendor	**Device Type**
SEW Eurodrive GmbH & Co. KG	-

Top protoc… | Throughput | Unique in… | Recurring …

Top protocols



Anwendungs- Und Bedrohungsdatenbank

Name	Typ	Gefährdungsniveau	Ports	Protokolle
Back Orifice	Bedrohung	Mittel	31337	TCP, UDP
trojans	Bedrohung	Mittel	31337	TCP, UDP
SSL	Schwachstelle	Gering	31337	TCP, UDP

CVE	Schwere	Angriffswert	Gewichtung
CVE-2003-0719	Hoch	10	6.4

Beschreibung

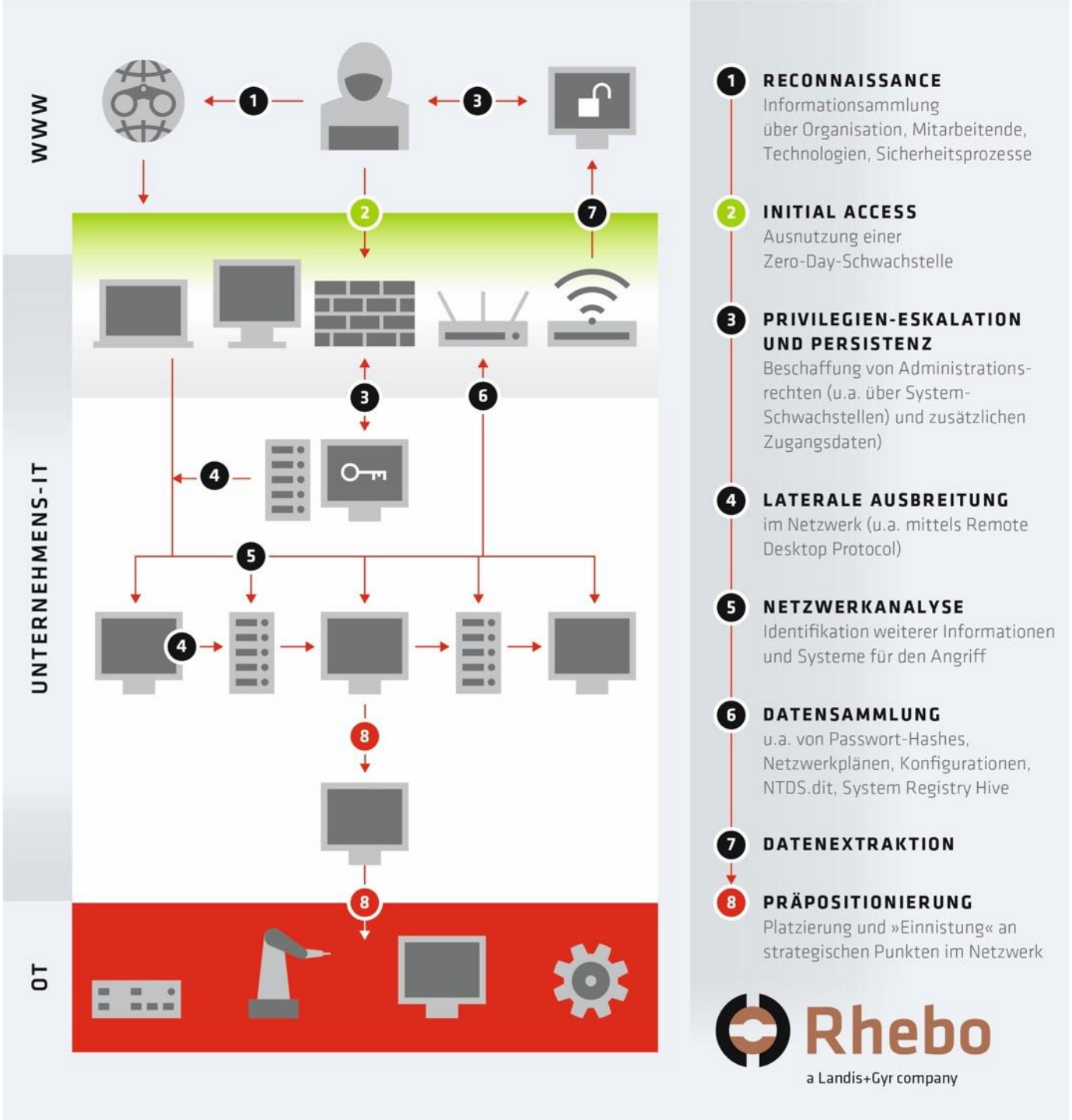
Buffer overflow in the Private Communications Transport (PCT) protocol implementation in the Microsoft SSL library, as used in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via PCT 1.0 handshake packets.

aMSN	Schwachstelle	Gering	31337	TCP, UDP
.Net Remoting	Anwendung	Keines	31337	TCP, UDP
Terraria	Anwendung	Keines	31337	TCP, UDP

Eine Schadsoftware hat eine Backdoor geöffnet. Die Schwachstelle war der CVE-Datenbank bekannt.

Beispiel Volt Typhoon und LOTL

“Living-off-the-Land-Angriffe” werden für zielgerichtete Angriffe zum Einnisten, Ausspähen und ggf. Übernehmen oder Abschalten von kritischen Infrastrukturen genutzt.



RHEBO STABILITÄTS- & SICHERHEITSASSESSMENT

- **Identifikation** aller OT-Geräte & Systeme
- Schwachstellen-Identifikation nach CVE
- Identifikation von Gefährdungen, **Sicherheitslücken** & technischer Fehlerzustände
- **Handlungsempfehlungen** mit Abschlussbericht & Workshop

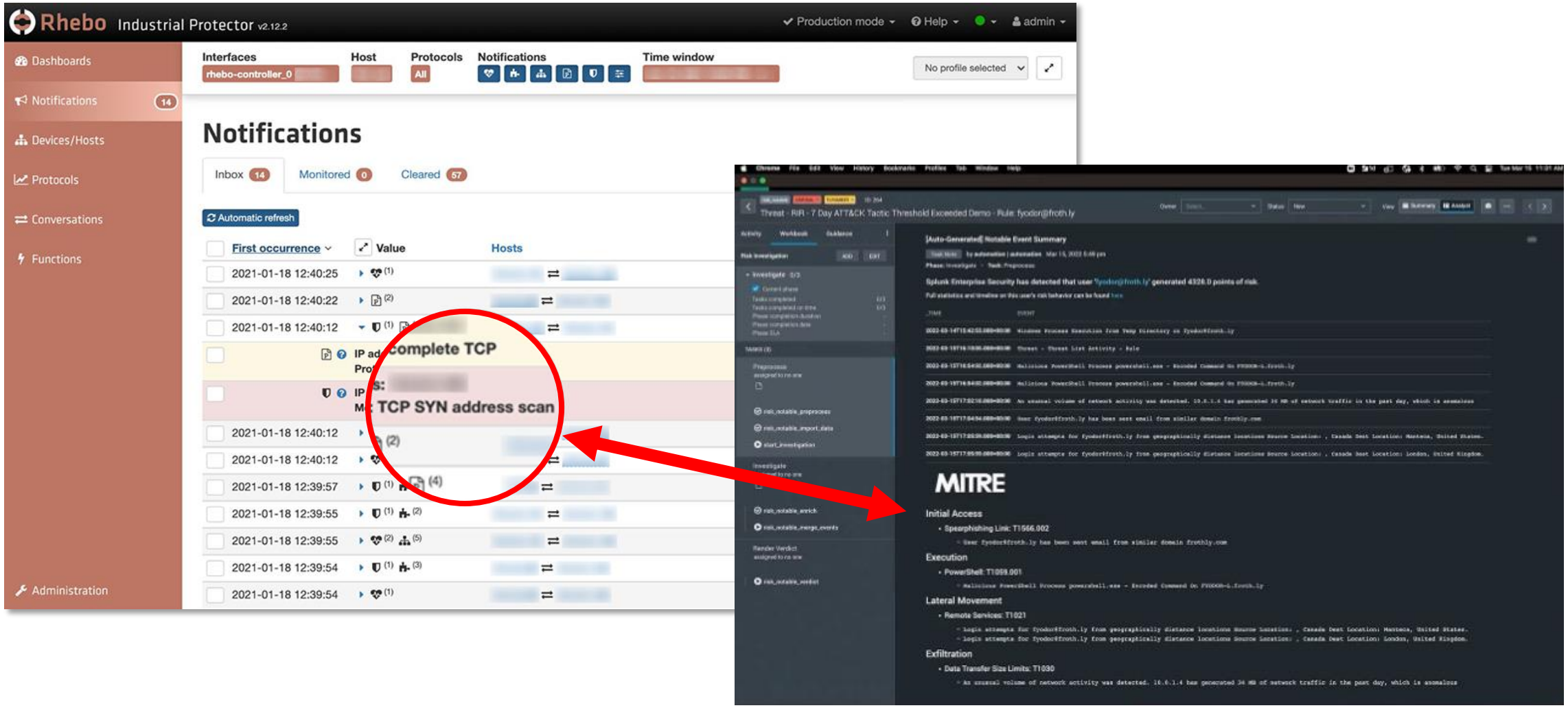
RHEBO INDUSTRIAL PROTECTOR

- **Echtzeitübersicht** über das Kommunikationsverhalten aller OT- und IIoT-Assets
- Echtzeitmeldung und –lokalisierung von Vorgängen (Anomalien)
- frühzeitige **Identifikation** von Angriffen über **Backdoors**, bislang unbekannte Schwachstellen und Innentätern

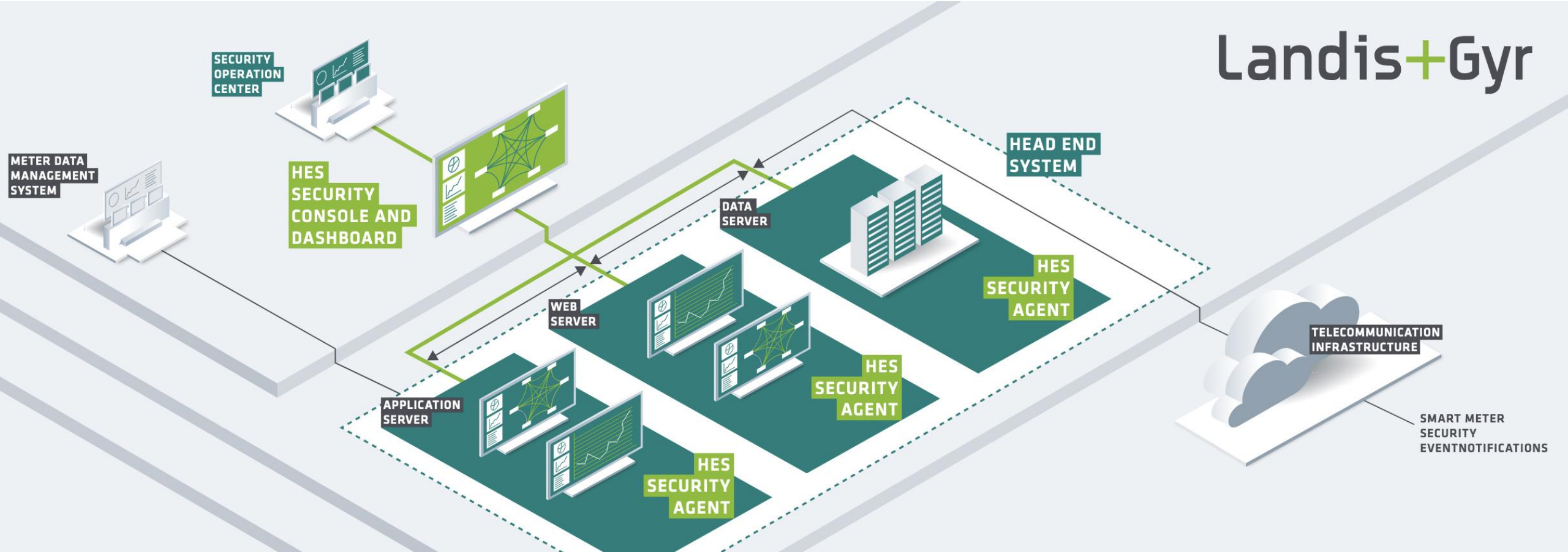
MANAGED PROTECTION

- Expert:innen-Unterstützung beim Betrieb des OT-Sicherheitsmonitorings
- schnelle **forensische Analyse** und Aufklärung von Anomalien in der OT
- **regelmäßige** OT-Risiko- und **Schwachstellenanalyse** für kontinuierliche Verbesserung

Direkte Meldung als Techniken und Taktiken nach MITRE



Praxisbeispiel: Integrierte Sicherheit in Head-End-Systemen



OT Security Made Simple

Klaus Mochalski

★ 4,0 (4) · TECHNOLOGIE · ZWEIWÖCHENTLICH

OT Security Made Simple is about OT security from practice for practice, hosted by Rhebo CEO Klaus Mochalski. The podcast invites experts from the forefront of OT security at energy suppliers, ... MEHR

▶ Neueste Folge

+ Folgen ···

Folgen >

VOR 2 TAGEN

Die Rolle des CISO in der OT | OT Security Made Simple

Eileen Walther, General Manager von Northwave Cyber Security, und Klaus Mochalski gehen der Frage auf den Grund, wie sich die Rolle des CISO in der OT-Security verändert hat und was KMUs daraus lernen können.

22 Min. ···

27. MÄRZ

ISO 27001 für OT: Mehrwert oder Overhead? | OT Security Made Simple

Klaus Kilvinger, Managing Director bei den Sicherheitsexperten von Opexa Advisory, berichtet aus seinen vielfältigen Erfahrungen zur ISO 27001. Während diese in der IT bereits ein alter Hut ist, wird sie in industriellen Umgebungen - der OT - häufig mit einer Mischung aus Argwohn und Überforderungen begrüßt. Im Podcast kommen wir dem Mehrwert auf die Spur.

24 Min. ···

11. MÄRZ

Aus dem Tagebuch eines OT-Pentesters | OT Security Made Simple

Patrick Latus berichtet als passionierter Pentester von vorderster Front der OT-Sicherheit. Von fehlendem Bewusstsein und Expertise bei Herstellern, Anwendenden und Auditor:innen bis zur Frage, ob OT-Sicherheitsvorfälle nur deshalb nicht publik werden, weil sie schlichtweg nicht gesehen werden.

22 Min. ···

27. FEB.

How do you secure the smart grid infrastructure? | OT Security Made Simple

In this episode of OT Security Made Simple, Zeek Muratovic, Director of Security Solutions for the Landis+Gyr group talks about the challenges and shortcomings of energy distributors, and the first steps to secure the growing and ever more complex smart grid infrastructure from the distribution network to the edge like smart meters and EV charging stations.

19 Min. ···

Rhebo

a Landis+Gyr company

Dr. Frank Stummer

Business Development

frank.stummer@rhebo.com

+49 341 3937 90-0