WEBINAR

LEITSYSTEM-KERNZONE NACH IT-SIG 2.0 SCHÜTZEN

Rhebo
a Landis+Gyr company

PSI

09. MÄRZ - 11.00-12.00

OT SECURITY
Made in Germany

Agenda

11:00 Uhr	**Begrüßung**
11:10 Uhr	**"Angriffsvektoren in Leitsystemen: Ergebnisse aus Rhebo Industrial Security Assessments bei deutschen Energieversorgungsunternehmen"** Klaus Mochalski, Gründer und Geschäftsführer, Rhebo
11:25 Uhr	**"Leitsysteme für das IT-SIG 2.0 fit machen: PSI-Kernzone schützen und Energieversorgung sichern"** Marco Bachmann,Vertriebsleiter Stadtwerke, PSI
11:40 Uhr	**"Bis zum 1 Mai 2023 Reifegrad 3 bis 4 für industrielle Cybersicherheit erreichen: Geht das?“** Klaus Mochalski, Gründer und Geschäftsführer, Rhebo
11:50 Uhr	**FAQ & Verabschiedung**

Rhebo

a Landis+Gyr company

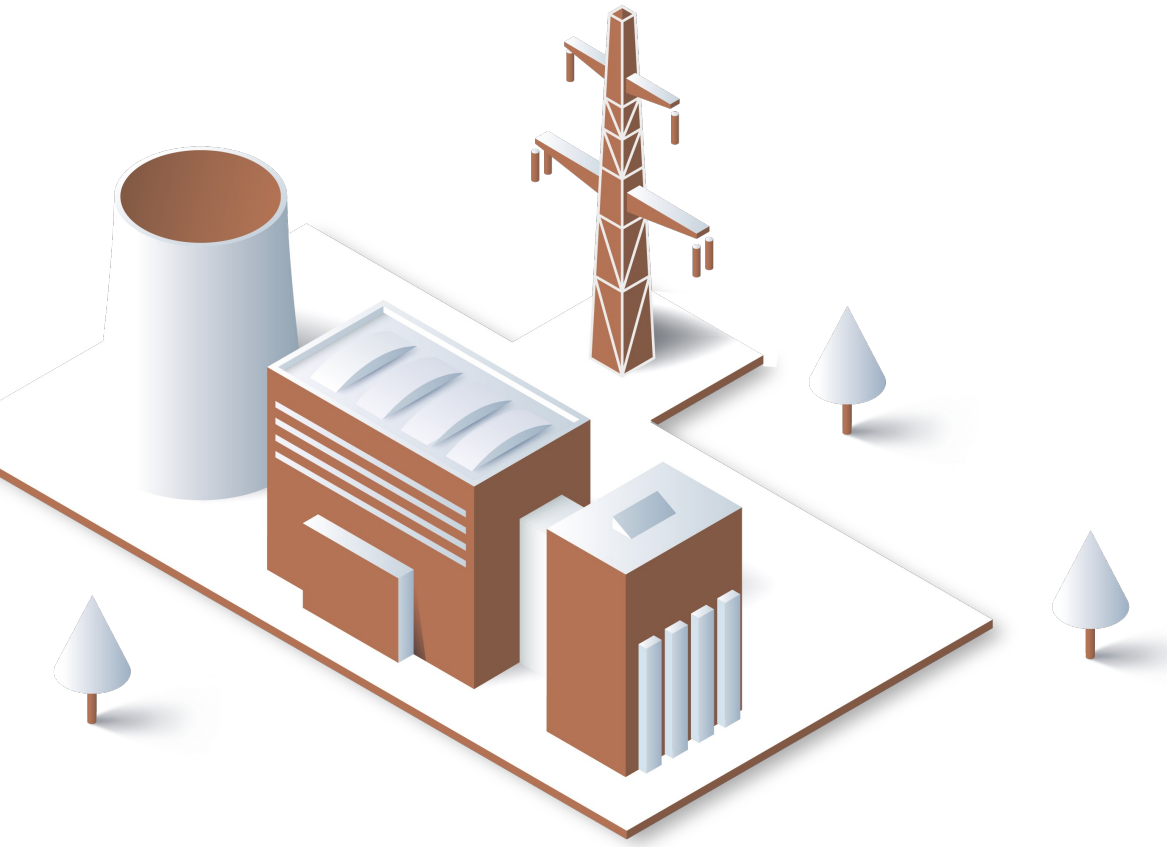
PSI

Leitsystem-Kernzone nach IT-SiG 2.0 schützen

Klaus Mochalski, CEO
km@rhebo.com

Marco Bachmann
Vertriebsleiter für Stadtwerke

Cybersicherheit & Verfügbarkeit für OT & IoT in Kritischen Infrastrukturen seit 2014

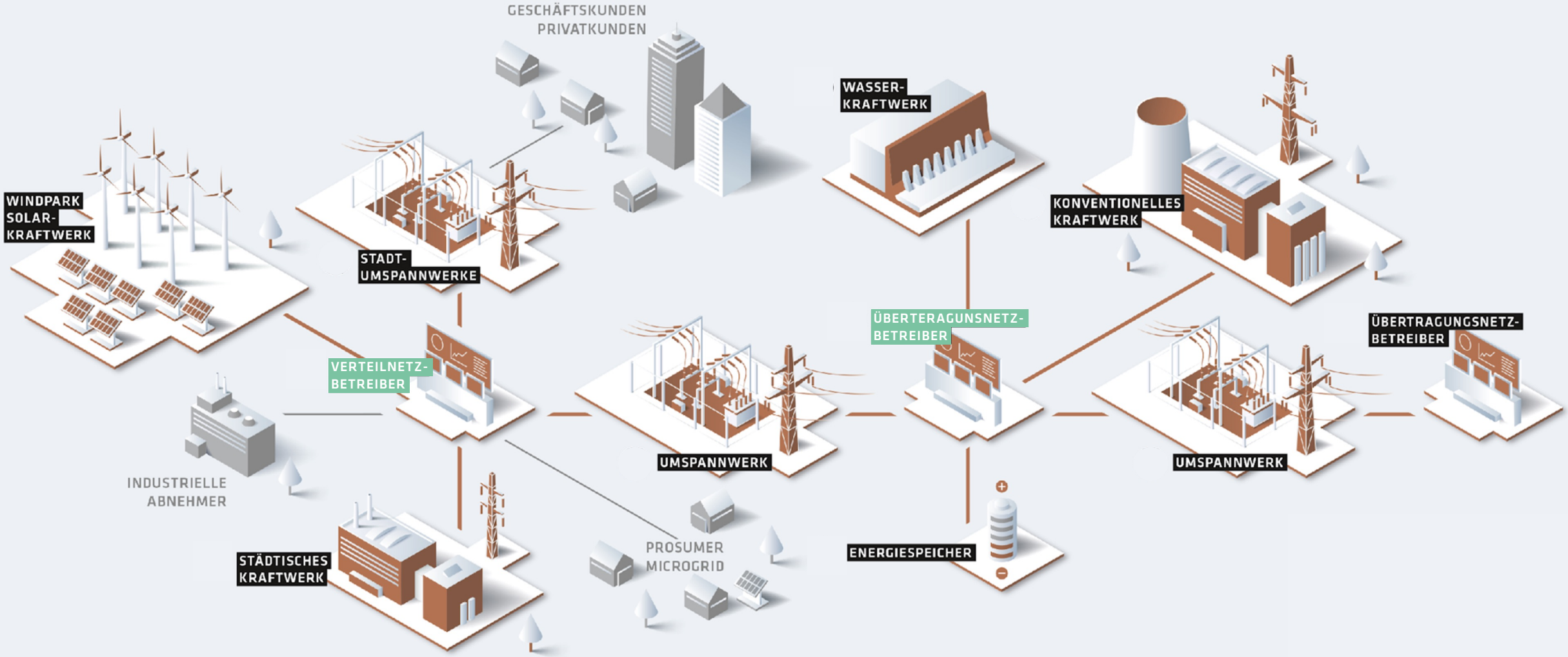


- >65k Installationen des Rhebo Industrial Protectors weltweit
- >33% des deutschen Stromnetzes abgesichert
- Erfahrung im Energiesektor durch Landis+Gyr seit 1896

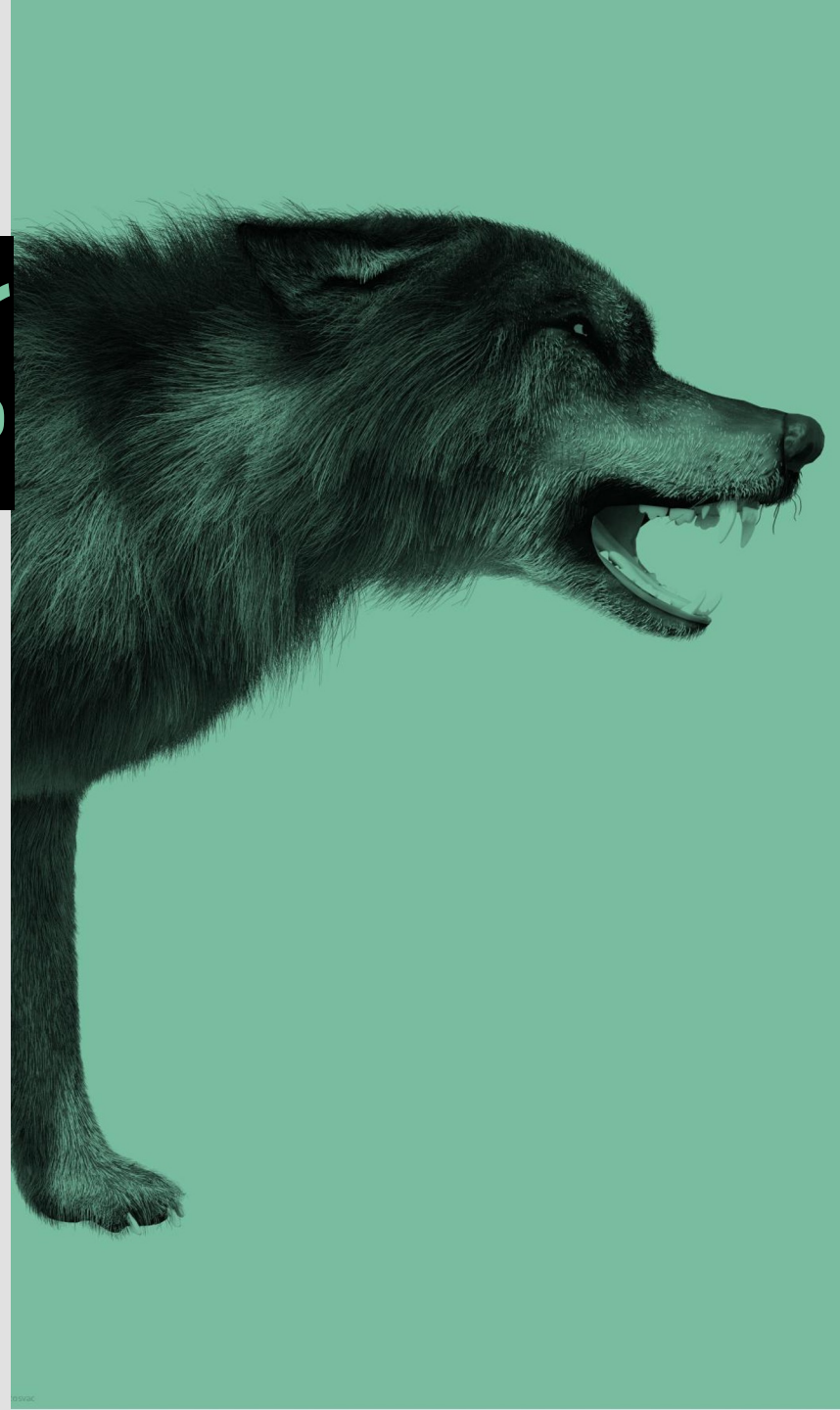
Rhebo
a Landis+Gyr company

Angriffsvektoren in Leitsystemen:
Ergebnisse aus Rhebo Industrial Security Assessments bei deutschen Energieversorgungsunternehmen

Kritische Infrastrukturen werden immer komplexer – in Betrieb und Überwachung



Wissen Sie, wer sich in Ihrer Infrastruktur herumtreibt?



Top-5 der Auffälligkeiten bei 50+ Rhebo-Kunden

68% nicht benötigte Protokolle & Dienste

66% verwundbare Hardware und Software

56% Lastspitzen und Bandbreitenschwankungen

47% unsichere Authentifizierungsmethoden

47% mögliche Schadsoftware

Rhebo
a Landis+Gyr company

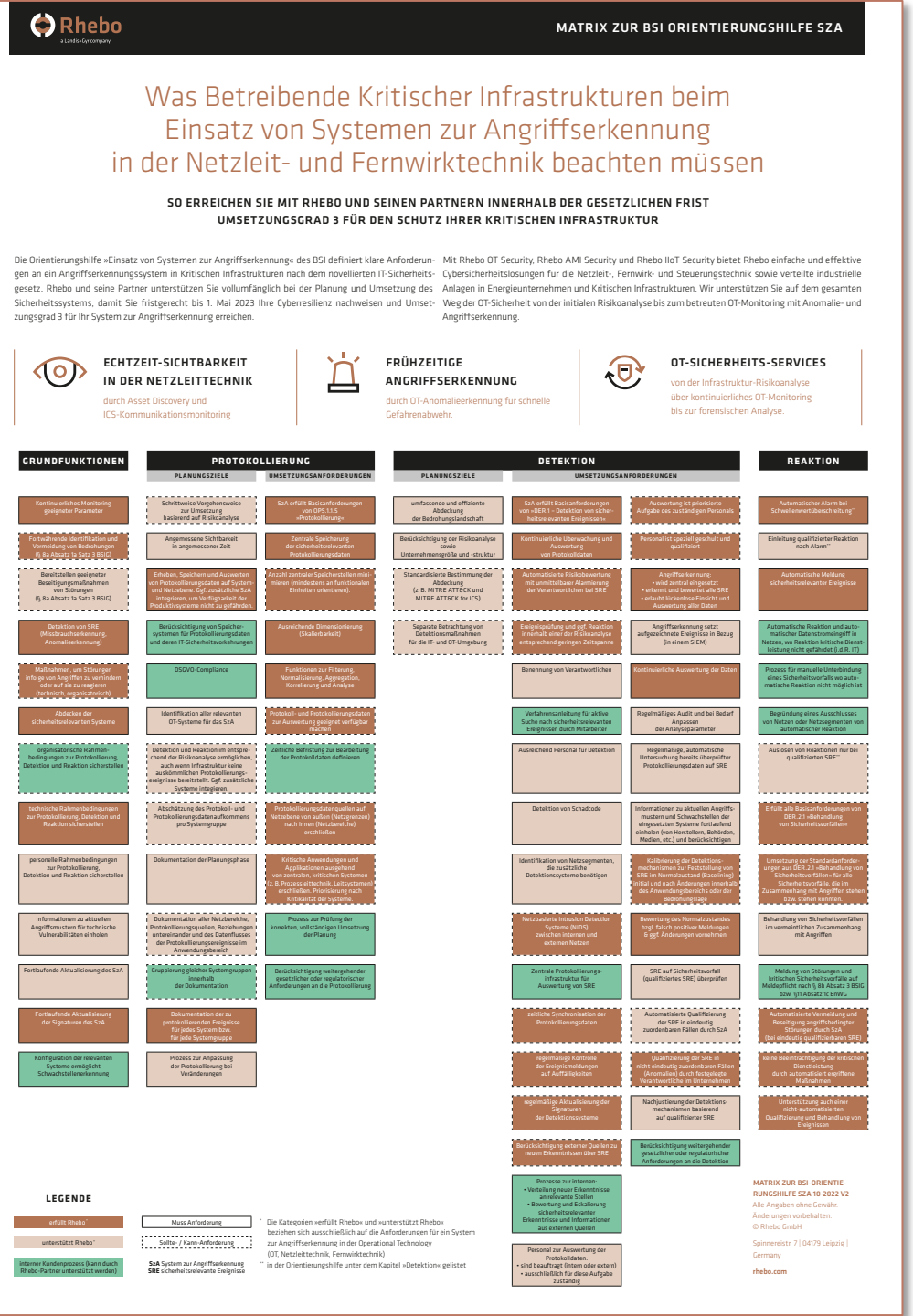
Bis zum 1 Mai 2023 Reifegrad 3 bis 4 für industrielle Cybersicherheit erreichen: Geht das?

Übersicht BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Inhalt

1 Überblick
Zielsetzung und Adressatenkreis der Orientierungshilfe
Aufbau der Orientierungshilfe
Weiterführende Informationen
2 Grundlagen
Gesetzlicher Hintergrund
Systeme zur Angriffserkennung und ihr branchenspezifischer Einsatz
3 Anforderungen
Protokollierung
Planung der Protokollierung
Umsetzung der Protokollierung
Detektion
Planung der Detektion
Umsetzung der Detektion
Reaktion
4 Nachweis von Systemen zur Angriffserkennung
Das Umsetzungsgradmodell
Nachweiserbringung
5 Glossar

Anforderungen an Systeme zur Angriffserkennung (SzA) und an deren Einsatz (siehe Matrix)



Rhebo
a Landis+Gyr company

MATRIX ZUR BSI ORIENTIERUNGSHILFE SZA

Was Betreibende Kritischer Infrastrukturen beim Einsatz von Systemen zur Angriffserkennung in der Netzleit- und Fernwirktechnik beachten müssen

SO ERREICHEN SIE MIT RHEBO UND SEINEN PARTNERN INNERHALB DER GESETZLICHEN FRIST UMSETZUNGSGRAD 3 FÜR DEN SCHUTZ IHRER KRITISCHEN INFRASTRUKTUR

Die Orientierungshilfe »Einsatz von Systemen zur Angriffserkennung« des BSI definiert klare Anforderungen an ein Angriffserkennungssystem in Kritischen Infrastrukturen nach dem novellierten IT-Sicherheitsgesetz. Rhebo und seine Partner unterstützen Sie vollumfänglich bei der Planung und Umsetzung des Sicherheitssystems, damit Sie fristgerecht bis 1. Mai 2023 Ihre Cyberresilienz nachweisen und Umsetzungsgrad 3 für Ihr System zur Angriffserkennung erreichen.

Mit Rhebo OT Security, Rhebo AMI Security und Rhebo IIoT Security bietet Rhebo einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen und Kritischen Infrastrukturen. Wir unterstützen Sie auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung.

ECHTZEIT-SICHTBARKEIT IN DER NETZLEITTECHNIK
durch Asset Discovery und ICS-Kommunikationsmonitoring

FRÜHZEITIGE ANGRIFFSERKENNUNG
durch OT-Anomalieerkennung für schnelle Gefahrenabwehr.

OT-SICHERHEITS-SERVICES
von der Infrastruktur-Risikoanalyse über kontinuierliches OT-Monitoring bis zur forensischen Analyse.

GRUNDFUNKTIONEN	PROTOKOLLIERUNG		DETEKTION			REAKTION
	PLANUNGSZIELE	UMSETZUNGSANFORDERUNGEN	PLANUNGSZIELE	UMSETZUNGSANFORDERUNGEN		
Kontinuierliches Monitoring geeigneter Parameter	Schrittweise Vorgehensweise zur Umsetzung basierend auf Risikoanalyse	SzA erfüllt Basisanforderungen von OPS.1.1.5 »Protokollierung«	umfassende und effiziente Abdeckung der Bedrohungslandschaft	SzA erfüllt Basisanforderungen von »DER.1 - Detektion von sicherheitsrelevanten Ereignissen«	Auswertung ist priorisierte Aufgabe des zuständigen Personals	Automatischer Alarm bei Schwellenwertüberschreitung*
Fortwährende Identifikation und Vermeidung von Bedrohungen (§ 8a Absatz 1a Satz 3 BSIG)	Angemessene Sichtbarkeit in angemessener Zeit	Zentrale Speicherung der sicherheitsrelevanten Protokollierungsdaten	Berücksichtigung der Risikoanalyse sowie Unternehmensgröße und -struktur	Kontinuierliche Überwachung und Auswertung von Protokolldaten	Personal ist speziell geschult und qualifiziert	Einleitung qualifizierter Reaktion nach Alarm*
Bereitstellen geeigneter Beseitigungsmaßnahmen von Störungen (§ 8a Absatz 1a Satz 3 BSIG)	Erheben, Speichern und Auswerten von Protokollierungsdaten auf System- und Netzebene. Ggf. zusätzliche SzA integrieren, um Verfügbarkeit der Produktivsysteme nicht zu gefährden.	Daten sollten so granular wie möglich (mindestens an funktionalen Einheiten orientieren).	Standardisierte Bestimmung der Abdeckung (z. B. MITRE ATT&CK und MITRE ATT&CK for ICS)	Automatisierte Detektionsmeldung mit unmittelbarer Alarmierung der Verantwortlichen bei SRE	Angriffserkennung: • wird zentral eingesetzt • erkennt und bewertet alle SRE • erlaubt lückenlose Einsicht und Auswertung aller Daten	Automatische Meldung sicherheitsrelevanter Ereignisse
Detektion von SRE (Missbrauchserkennung, Anomalieerkennung)	Berücksichtigung von Speichersystemen für Protokollierungsdaten und deren IT-Sicherheitsvorkehrungen	Ausreichende Dimensionierung (Skalierbarkeit)	Separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung	Eingrenzung und ggf. Kontrolle innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne	Angriffserkennung setzt aufgezeichnete Ereignisse in Bezug (in einem SIEM)	Automatische Reaktion und automatischer Datenstromeingriff in Netzen, wo Reaktion kritische Dienstleistung nicht gefährdet (z.d.R. IT)
Maßnahmen, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (technisch, organisatorisch)	DSGVO-Compliance	Funktionen zur Filterung, Normalisierung, Aggregation, Korrelierung und Analyse		Benennung von Verantwortlichen	Kontinuierliche Auswertung der Daten	Prozess für manuelle Unterbindung eines Sicherheitsvorfalls wo automatische Reaktion nicht möglich ist
Abdecken der sicherheitsrelevanten Systeme	Identifikation aller relevanten OT-Systeme für das SzA	Protokoll- und Protokollierungsdaten zur Auswertung geeignet verfügbar machen		Verfahrensanleitung für aktive Suche nach sicherheitsrelevanten Ereignissen durch Mitarbeiter	Regelmäßiges Audit und bei Bedarf Anpassen der Analyseparameter	Begründung eines Ausschlusses von Netzen oder Netzsegmenten von automatischer Reaktion
organisatorische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Detektion und Reaktion im entsprechend der Risikoanalyse ermöglichen, auch wenn Infrastruktur keine ausnömmlichen Protokollierungs-ereignisse bereitstellt. Ggf. zusätzliche Systeme integrieren.	Zeitliche Befristung zur Bearbeitung der Protokolldaten definieren		Ausreichend Personal für Detektion	Regelmäßige, automatische Untersuchung bereits überprüfter Protokollierungsdaten auf SRE	Auslösen von Reaktionen nur bei qualifizierten SRE*
technische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Abschätzung des Protokoll- und Protokollierungsdatenaufkommens pro Systemgruppe	Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschließen		Detektion von Schadcode	Informationen zu aktuellen Angriffsmustern und Schwachstellen der eingesetzten Systeme fortlaufend einholen (von Herstellern, Behörden, Medien, etc.) und berücksichtigen	Erfüllt alle Basisanforderungen von DER.2.1 »Behandlung von Sicherheitsvorfällen«
personelle Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Dokumentation der Planungsphase	Kritische Anwendungen und Applikationen ausgehend von zentralen, kritischen Systemen (z. B. Prozessleittechnik, Leitsysteme) erschließen. Priorisierung nach Kritikalität der Systeme.		Identifikation von Netzsegmenten, die zusätzliche Detektionssysteme benötigen	Kalibrierung der Detektionsmechanismen zur Feststellung von SRE im Normalzustand (Baselining) initial und nach Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage	Umsetzung der Standardanforderungen aus DER.2.1 »Behandlung von Sicherheitsvorfällen« für alle Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.
Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten einholen	Dokumentation aller Netzbereiche, Protokollierungsquellen, Beziehungen untereinander und des Datenflusses der Protokollierungsereignisse im Anwendungsbereich	Prozess zur Prüfung der korrekten, vollständigen Umsetzung der Planung		Netzbasierte Intrusion Detection Systeme (NIDS) zwischen internen und externen Netzen	Bewertung des Normalzustandes bzgl. falsch positiver Meldungen & ggf. Änderungen vornehmen	Behandlung von Sicherheitsvorfällen im vermeintlichen Zusammenhang mit Angriffen
Fortlaufende Aktualisierung des SzA	Kapselung gleicher Systemgruppen innerhalb der Dokumentation	Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Protokollierung		Zentrale Protokollierungsinfrastruktur für Auswertung von SRE	SRE auf Sicherheitsvorfall (qualifiziertes SRE) überprüfen	Meldung von Störungen und kritischen Sicherheitsvorfälle auf Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG.
Fortlaufende Aktualisierung der Signaturen des SzA	Dokumentation der zu protokollierenden Ereignisse für jedes System bzw. für jede Systemgruppe			zeitliche Synchronisation der Protokollierungsdaten	Automatisierte Qualifizierung der SRE in eindeutig zuordenbaren Fällen durch SzA	Automatisierte Vermeidung und Beseitigung angriffsbedingter Störungen durch SzA (bei eindeutig Qualifizierung SRE)
Konfiguration der relevanten Systeme ermöglicht Schwachstellenerkennung	Prozess zur Anpassung der Protokollierung bei Veränderungen			regelmäßige Kontrolle der Ereignismeldungen auf Auffälligkeiten	Qualifizierung der SRE in nicht eindeutig zuordenbaren Fällen (Anomalien) durch festgelegte Verantwortliche im Unternehmen	keine Beeinträchtigung der kritischen Dienstleistung durch automatisiert ergriffene Maßnahmen
				regelmäßige Aktualisierung der Signaturen der Detektionssysteme	Nachjustierung der Detektionsmechanismen basierend auf qualifizierter SRE	Unterstützung auch einer nicht-automatisierten Qualifizierung und Behandlung von Ereignissen
				Berücksichtigung externer Quellen zu neuen Erkenntnissen über SRE	Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Detektion	
				Prozesse zur internen: • Verteilung neuer Erkenntnisse an relevante Stellen • Bewertung und Eskalierung sicherheitsrelevanter Erkenntnisse und Informationen aus externen Quellen		
				Personal zur Auswertung der Protokolldaten: • sind beauftragt (intern oder extern) • ausschließlich für diese Aufgabe zuständig		

LEGENDE

erfüllt Rhebo*
unterstützt Rhebo*
Interner Kundenprozess (kann durch Rhebo-Partner unterstützt werden)
Muss Anforderung
Sollte- / Kann-Anforderung
SzA System zur Angriffserkennung
SRE sicherheitsrelevante Ereignisse

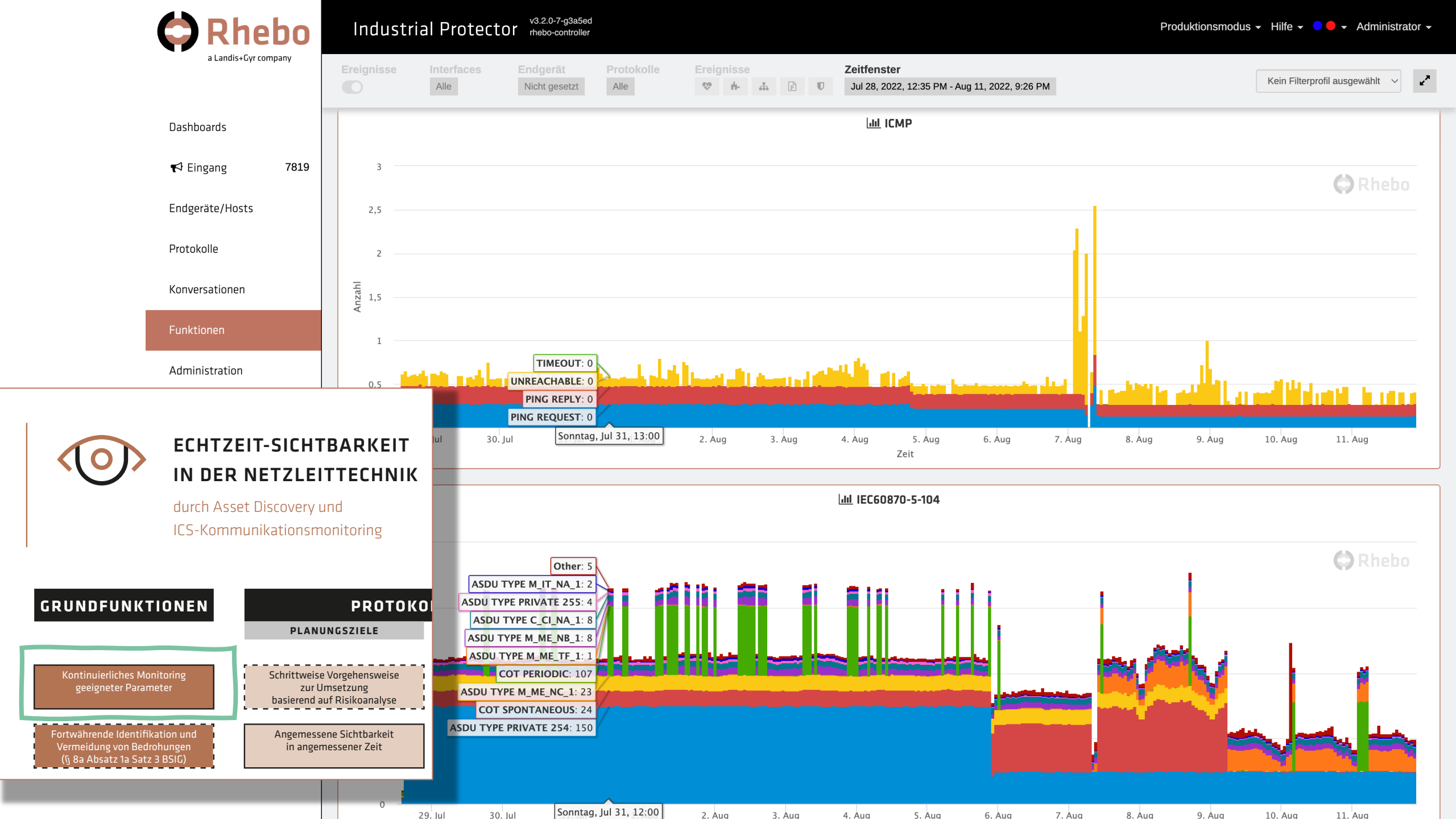
* Die Kategorien »erfüllt Rhebo« und »unterstützt Rhebo« beziehen sich ausschließlich auf die Anforderungen für ein System zur Angriffserkennung in der Operational Technology (OT, Netzleittechnik, Fernwirktechnik)
** in der Orientierungshilfe unter dem Kapitel »Detektion« gelistet

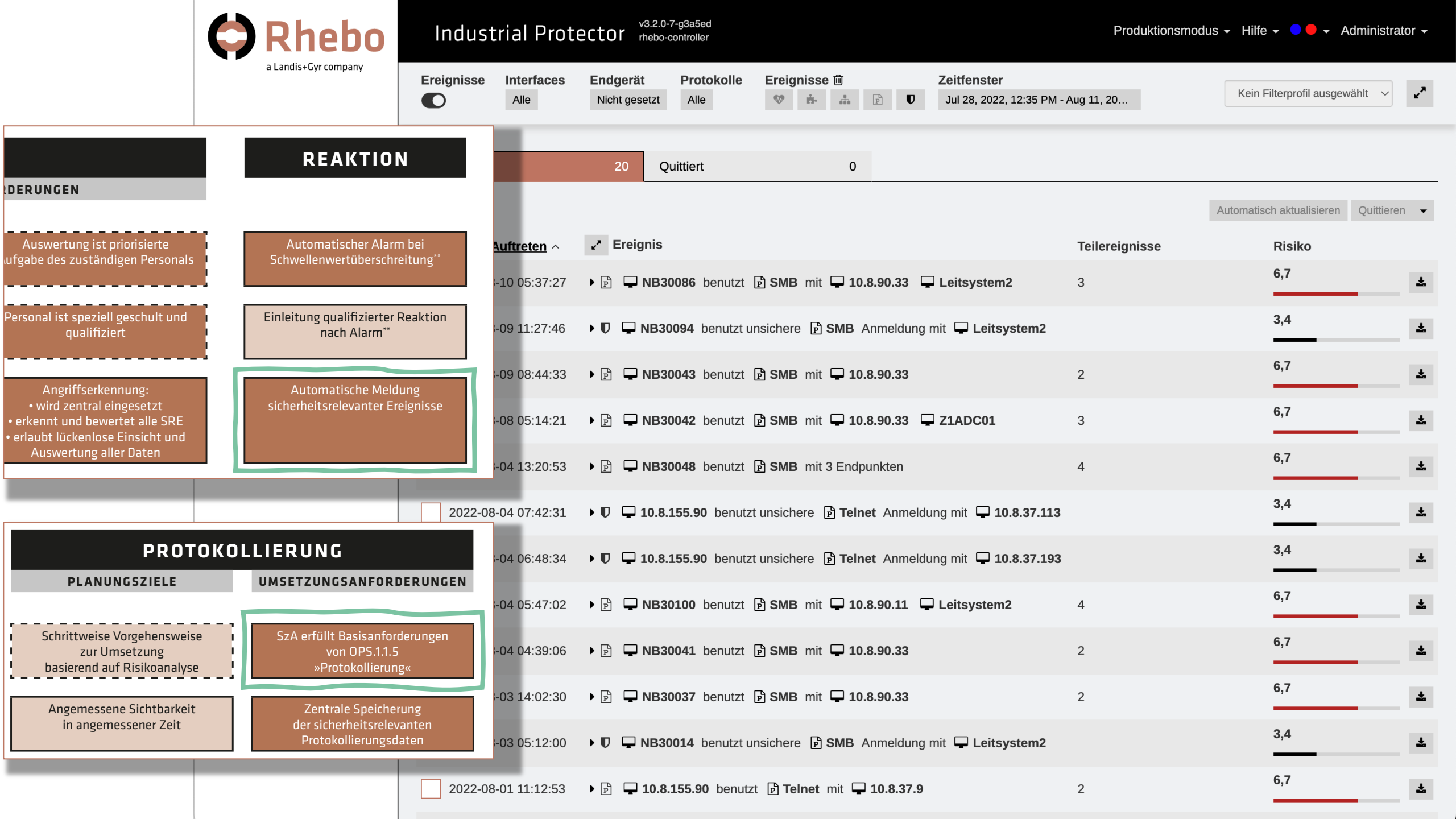
MATRIX ZUR BSI-ORIENTIERUNGSHILFE SZA 10-2022 V2

Spinnereistr. 7 | 04179 Leipzig | Germany
rhebo.com

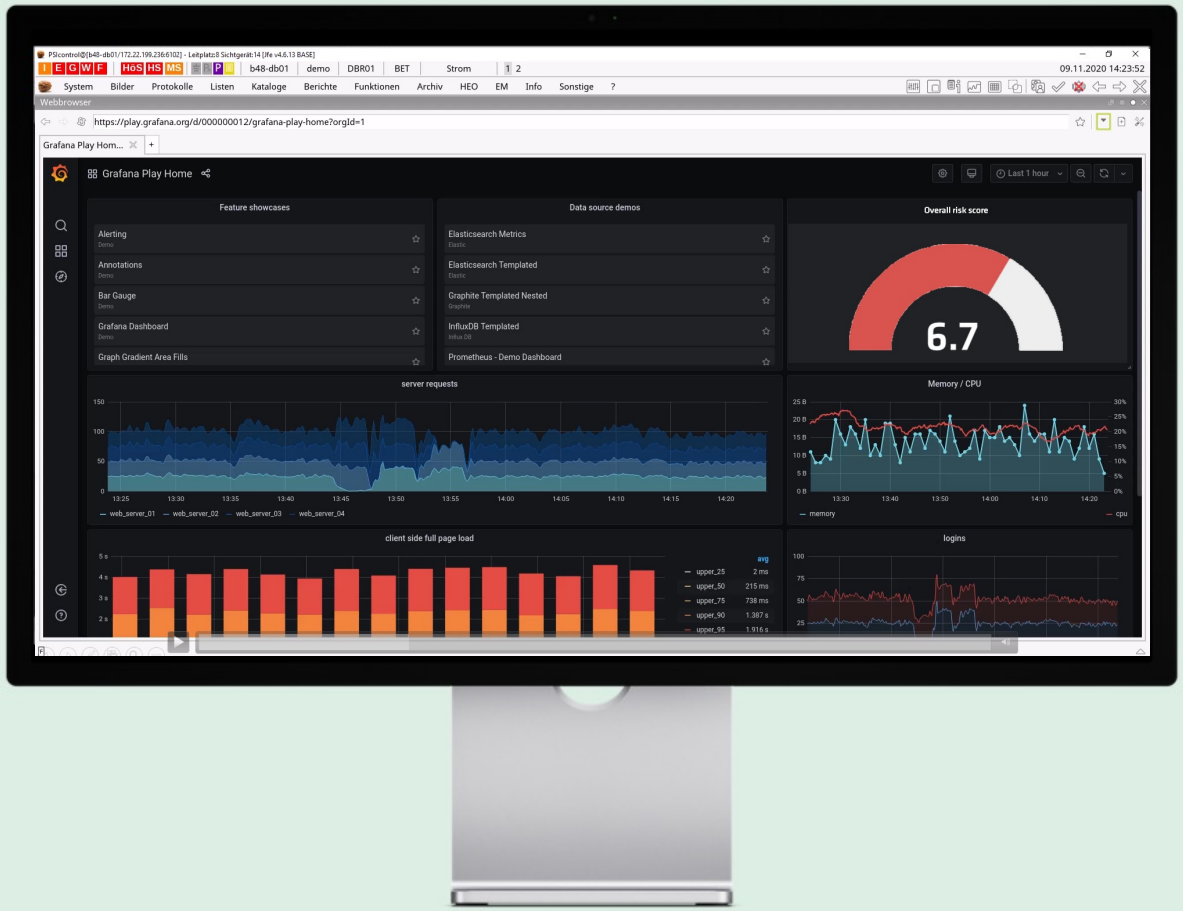
Matrix BSI-Anforderungen & Umsetzung Rhebo

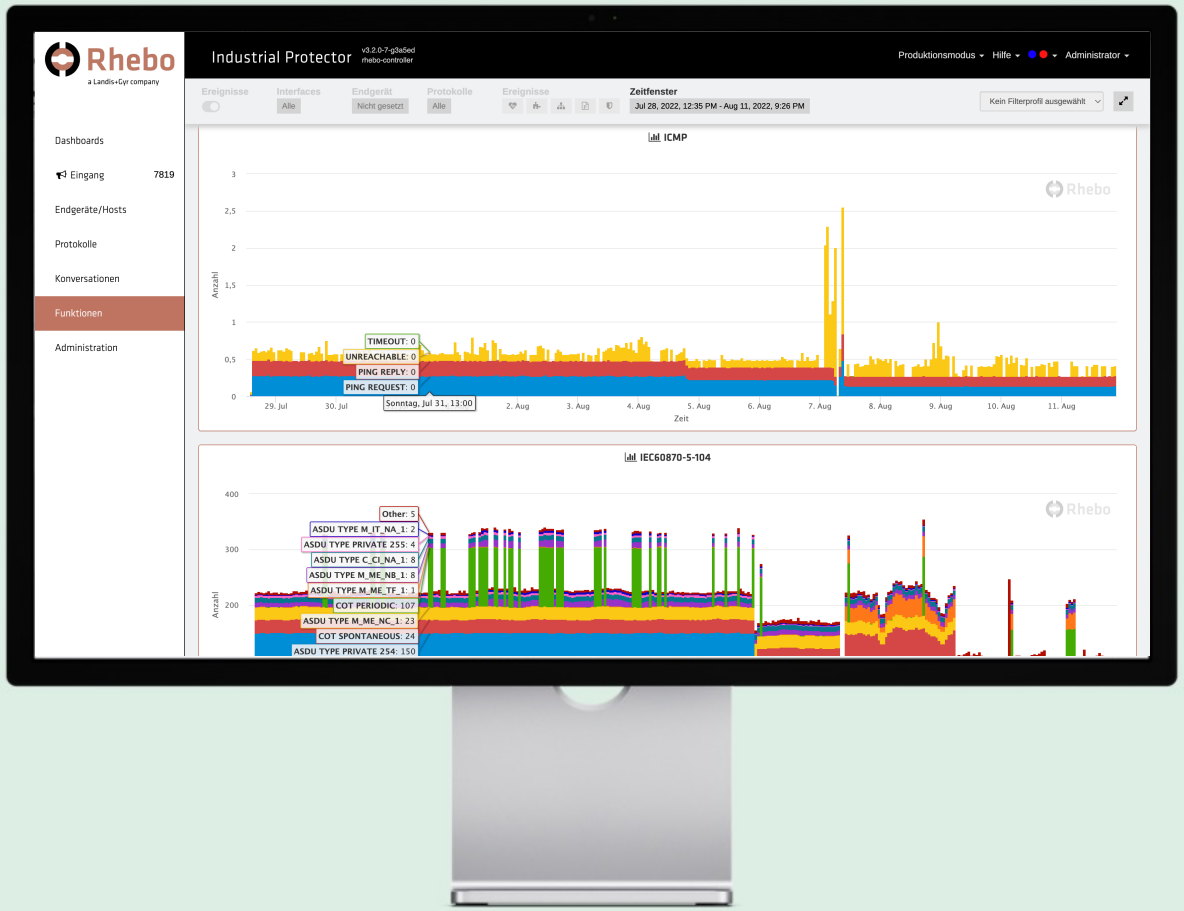
- Direkte Anforderungen an SzA (Systeme zur Angriffserkennung) werden direkt erfüllt
- Indirekte Anforderungen (z.B. in der Planung) werden unterstützt
- Anforderungen an den internen Kundenprozess (z.B. in der operativen Anwendung) können direkt oder durch Partner geleistet werden


Rhebo
a Landis+Gyr company
Industrial Protector
v3.2.0-7-g3a5ed
rhebo-controller
Produktionsmodus
Hilfe
Administrator
Ereignisse
Interfaces
Alle
Endgerät
Nicht gesetzt
Protokolle
Alle
Ereignisse
Zeitfenster
Jul 28, 2022, 12:35 PM - Aug 11, 2022, 9:26 PM
Kein Filterprofil ausgewählt
Dashboards
Eingang 7819
Endgeräte/Hosts
Protokolle
Konversationen
Funktionen
Administration
ICMP
Anzahl
Zeit
TIMEOUT: 0
UNREACHABLE: 0
PING REPLY: 0
PING REQUEST: 0
Sonntag, Jul 31, 13:00
IEC60870-5-104
Other: 5
ASDU TYPE M_IT_NA_1: 2
ASDU TYPE PRIVATE 255: 4
ASDU TYPE C_CI_NA_1: 8
ASDU TYPE M_ME_NB_1: 8
ASDU TYPE M_ME_TF_1: 1
COT PERIODIC: 107
ASDU TYPE M_ME_NC_1: 23
COT SPONTANEOUS: 24
ASDU TYPE PRIVATE 254: 150
Sonntag, Jul 31, 12:00
ECHTZEIT-SICHTBARKEIT
IN DER NETZLEITTECHNIK
durch Asset Discovery und
ICS-Kommunikationsmonitoring
GRUNDFUNKTIONEN
PROTOKO
PLANUNGSZIELE
Kontinuierliches Monitoring geeigneter Parameter
Schrittweise Vorgehensweise zur Umsetzung basierend auf Risikoanalyse
Fortwährende Identifikation und Vermeidung von Bedrohungen (§ 8a Absatz 1a Satz 3 BSIG)
Angemessene Sichtbarkeit in angemessener Zeit


Rhebo
a Landis+Gyr company
Industrial Protector
v3.2.0-7-g3a5ed
rhebo-controller
Produktionsmodus
Hilfe
Administrator
Ereignisse
Interfaces
Alle
Endgerät
Nicht gesetzt
Protokolle
Alle
Ereignisse
Zeitfenster
Jul 28, 2022, 12:35 PM - Aug 11, 20…
Kein Filterprofil ausgewählt
20
Quittiert
0
Automatisch aktualisieren
Quittieren
Auftreten
Ereignis
Teilereignisse
Risiko
-10 05:37:27 NB30086 benutzt SMB mit 10.8.90.33 Leitsystem2 3 6,7
-09 11:27:46 NB30094 benutzt unsichere SMB Anmeldung mit Leitsystem2 3,4
-09 08:44:33 NB30043 benutzt SMB mit 10.8.90.33 2 6,7
-08 05:14:21 NB30042 benutzt SMB mit 10.8.90.33 Z1ADC01 3 6,7
-04 13:20:53 NB30048 benutzt SMB mit 3 Endpunkten 4 6,7
2022-08-04 07:42:31 10.8.155.90 benutzt unsichere Telnet Anmeldung mit 10.8.37.113 3,4
-04 06:48:34 10.8.155.90 benutzt unsichere Telnet Anmeldung mit 10.8.37.193 3,4
-04 05:47:02 NB30100 benutzt SMB mit 10.8.90.11 Leitsystem2 4 6,7
-04 04:39:06 NB30041 benutzt SMB mit 10.8.90.33 2 6,7
-03 14:02:30 NB30037 benutzt SMB mit 10.8.90.33 2 6,7
-03 05:12:00 NB30014 benutzt unsichere SMB Anmeldung mit Leitsystem2 3,4
2022-08-01 11:12:53 10.8.155.90 benutzt Telnet mit 10.8.37.9 2 6,7
REAKTION
DERUNGEN
Auswertung ist priorisierte
ufgabe des zuständigen Personals
Automatischer Alarm bei
Schwellenwertüberschreitung**
Personal ist speziell geschult und
qualifiziert
Einleitung qualifizierter Reaktion
nach Alarm**
Angriffserkennung:
• wird zentral eingesetzt
• erkennt und bewertet alle SRE
• erlaubt lückenlose Einsicht und
Auswertung aller Daten
Automatische Meldung
sicherheitsrelevanter Ereignisse
PROTOKOLLIERUNG
PLANUNGSZIELE
UMSETZUNGSANFORDERUNGEN
Schrittweise Vorgehensweise
zur Umsetzung
basierend auf Risikoanalyse
SzA erfüllt Basisanforderungen
von OPS.1.1.5
»Protokollierung«
Angemessene Sichtbarkeit
in angemessener Zeit
Zentrale Speicherung
der sicherheitsrelevanten
Protokollierungsdaten

Integration von sicherheitsrelevanten Ereignissen direkt ins Leitsystem





Umsetzungsgrade

Erreichung von Mindest-Umsetzungsgrad 3 zeitgerecht bis 01. Mai 2023 ohne weiteres möglich

In einem KVP können höhere Umsetzungsgrade in nächsten Zyklen erreicht werden (mindestens gefordert ist später Grad 4)

0. Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.
1. Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
2. In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen[9] erfüllt worden.
3. Alle MUSS-Anforderungen[9] wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.
4. Alle MUSS- Anforderungen[9] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
5. Alle MUSS-Anforderungen[9] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

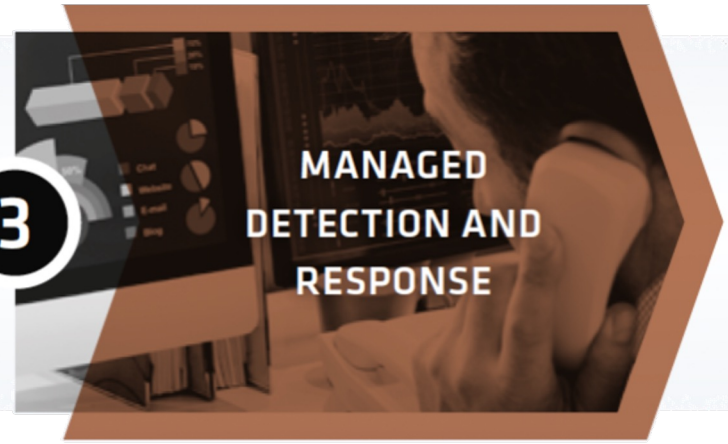
Mit Rhebo in 3 Schritten zu durchgängiger OT-Sicherheit

RHEBO INDUSTRIE 4.0 STABILITÄTS- & SICHERHEITSAUDIT

- Identifikation aller OT-Geräte & Systeme
- Identifikation von Schwachstellen, Sicherheitslücken & technischen Fehlerzuständen
- Handlungsempfehlungen mit Abschlussbericht & Workshop
- **in nur 60 Tagen**

RHEBO INDUSTRIAL PROTECTOR

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



RHEBO MANAGED PROTECTION

- Expert:innen-Unterstützung beim Betrieb des OT-Sicherheitsmonitorings
- schnelle forensischen Analyse und Aufklärung von Anomalien in der OT
- regelmäßige OT-Risiko- und Schwachstellenanalyse

VIELEN DANK FÜR IHRE TEILNAHME AN UNSERER WEBINARREIHE

EINE AUFZEICHNUNG ERHALTEN SIE IN DEN NÄCHSTEN TAGEN.

Rhebo
a Landis+Gyr company

OT SECURITY
Made in Germany

OT Security Made Simple