Rhebo
OT Security Made Simple

Solution Brief

Rhebo Industrial Protector

Netzbasierte Angriffserkennung für OT-Infrastruktur

OT SECURITY Made in Germany

ANGRIFFSERKENNUNG NACH NIS2 UND IEC 62443 UMSETZEN

CYBERRISIKO VON OT-STILLSTÄNDEN REDUZIEREN

CYBERSICHERHEIT EINFACH UND SCHNELL IN DER OT INTEGRIEREN

Rhebo Industrial Protector ist ein netzbasiertes Intrusion Detection System (NIDS), das die OT-Kommunikation kontinuierlich und passiv nach auffälligen, abweichenden Vorgängen untersucht. Die integrierte Anomalieerkennung informiert Sicherheitsverantwortliche in Kritischen Infrastrukturen und Industrieunternehmen in Echtzeit über aktuelle Cybergefahren in ihrer OT.

Selbst erfolgreiche Angriffe über Schwachstellen, Brute-Force, Backdoors, Innentäter oder gestohlene Credentials, aber auch technische Fehlerzustände werden so frühzeitig erkannt. Rhebo Industrial Protector ist damit der nahtlose Übergang von der OT-Risikoanalyse zur kontinuierlichen netzbasierten Angriffserkennung in der Netzleit-, Fernwirk- und Steuerungstechnik nach dem NIS2UmsuCG.

»Mit Rhebo können wir unsere landesweite Energieversorgung zentral und zuverlässig absichern – auch für die von uns betreuten Stadtwerke und über 16.000 dezentralen Erzeuger. Die neu gewonnene Transparenz und kontinuierliche Überwachung steigert sichtlich unsere Netzwerkqualität«.

Thüringer Energienetze GmbH & Co. KG

Gewinnen Sie mit Rhebo Industrial Protector

- **ECHTZEIT-SICHTBARKEIT IN DER OT** von Geräten, Verbindungen, Schwachstellen und Kommunikationstruktur durch passives Monitoring
- **DIE EINFACHE INTEGRATION VON OT-SICHERHEIT** durch On-Premise-Installation, hohe Usability und minimalen Aufwand
- **EINE EFFIZIENTE ANGRIFFSERKENNUNG** durch Echtzeitmeldung von Anomalien wie Kommunikationsveränderungen und Fehlerzuständen
- **RECHTSSICHERE DOKUMENTATION VON VORFÄLLEN** durch Packet Capture und genaue Lokalisierung der Anomalien
- **DIGITALE SOUVERÄNITÄT IN DER OT-SICHERHEIT** durch deutsche Entwicklung und Betreuung beim Betrieb des Angriffserkennungssystems
- **GESTÄRKE CYBERSICHERHEIT-COMPLIANCE** mit einem Angriffserkennungssystem nach NIS2 und IEC 62443

Erkennen Sie in Echtzeit OT-Anomalien und Schwachstellen

Rhebo Industrial Protector überwacht rund um die Uhr die gesamte Kommunikation innerhalb, zur und von der OT. Das Monitoring wird rückwirkungsfrei und passiv an Schlüsselpunkten des OT integriert. Jede Kommunikation, die auf Cyberangriffe, Manipulationen, Spionage oder technische Fehlerzustände hinweist, wird in Echtzeit gemeldet, ohne dass die empfindlichen industriellen Prozesse beeinträchtigt werden.

Betreiber und Sicherheitsbeauftragte können so schnell schnell auf Bedrohungen, bestehende Schwachstellen und professionelle Angriffsmuster reagieren, um die Sicherheit und Verfügbarkeit ihrer industriellen Prozesse zu gewährleisten.

Mit Hilfe praxisnaher Funktionen wie Risikobewertung, Netzwerkkarte, forensische Datenerfassung (pcap), Filter und Schnittstellenintegration in SIEM-Systeme unterstützt das OT-Monitoring mit Anomalieerkennung die Verantwortlichen gezielt bei der schnellen Detektion, Analyse und Beseitigung von Cybervorfällen wie:

- neue Hosts und Kommunikationstypen,
- neue Protokolle und Verbindungen zwischen Hosts,
- laterale Bewegungen,
- Netzwerk-Scans;
- Download oder Upload von Payloads,
- jegliche Änderungen in der legitimen OT-Kommunikation.

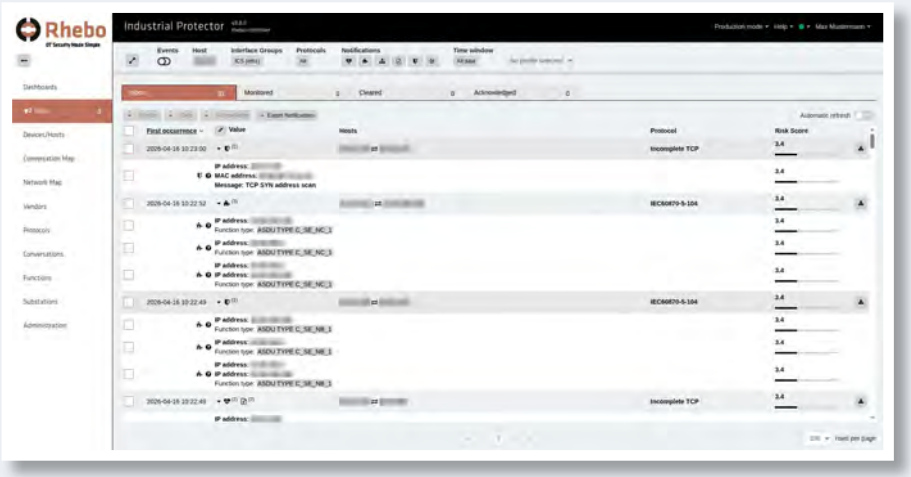
OT- & ASSET-SICHTBARKEIT

Das kontinuierliche OT-Monitoring stellt Echtzeit-OT-Sichtbarkeit über alle Geräte und Systeme her, die innerhalb, zum oder aus dem überwachten OT-Netzwerk kommunizieren. Diese Sichtbarkeit umfasst relevante Informationen über die Geräte und Systeme wie Firmware-Version, aktive Verbindungen, Protokolle und CVE-Schwachstellen. Die Funktion ermöglicht die Identifikation und Inventarisierung der Assets sowie eine eingehende Analyse von Kommunikationsmustern im Zeitverlauf.

Netzwerkkarte eines OT-Systems und seiner Verbindungen bei Rhebo Industrial Protector. Rechts werden Details einer ausgesuchten Verbindung angezeigt.

ANGRIFFS- & ANOMALIEERKENNUNG

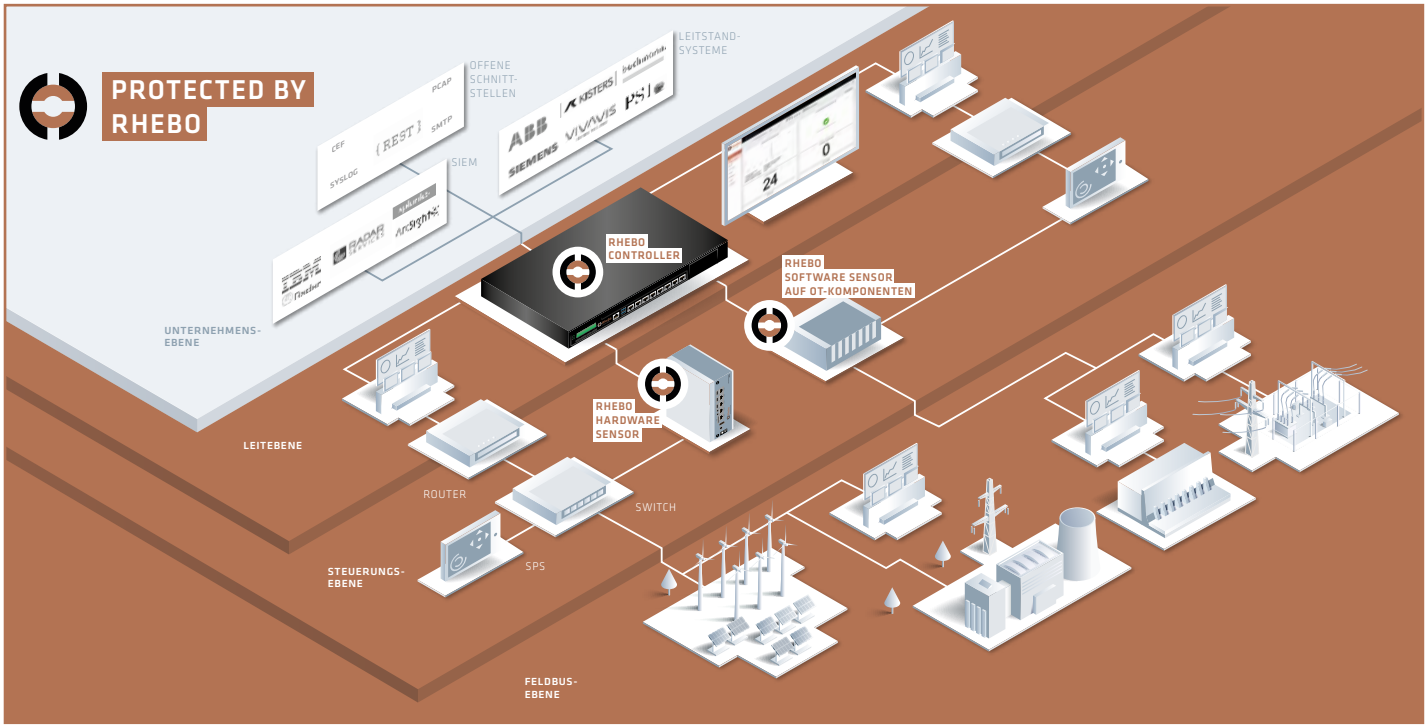
Die integrierte Anomalieerkennung identifiziert alle Abweichungen in den Verhaltensmustern der OT-Kommunikation. Dadurch können auch erfolgreiche Angriffe über Sicherheitslücken in der Firewall, Brute Force, Zero-Day-Exploits, Innentäter, Backdoors oder gestohlene Zugangsdaten sowie technische Fehlerzustände durch Fehlkonfigurationen oder Netzwerkprobleme frühzeitig erkannt werden.



Liste identifizierter Kommunikationsanomalien mit Anzeige der einzelnen Vorgänge (hier: ein Adress-Scan sowie die erstmalige Kommunikation zwischen zwei Hosts über das Protokoll IEC60870-5-104).

Integrieren Sie OT-Sicherheit

einfach, robust und ohne Störung Ihrer Prozesse



Rhebo Industrial Protector

Die schlanke und dedizierte OT-Angriffserkennung

Was Sie erreichen

- Echtzeitdetektion von Cyberangriffen und technischen Fehlerzuständen innerhalb der OT und Leittechnik,
- vollständige Sichtbarkeit der aktiven OT-Komponenten für das Asset Inventory,
- Dokumentation der Asset-Eigenschaften einschließlich der bestehenden Verbindungen und Schwachstellen sowie der verwendeten Protokolle,
- Wissensaufbau zu OT-Sicherheit,
- Compliance mit den Anforderungen an ein System zur Angriffserkennung in der OT nach dem NIS2-Umsetzungsgesetz und BSI-Empfehlungen.

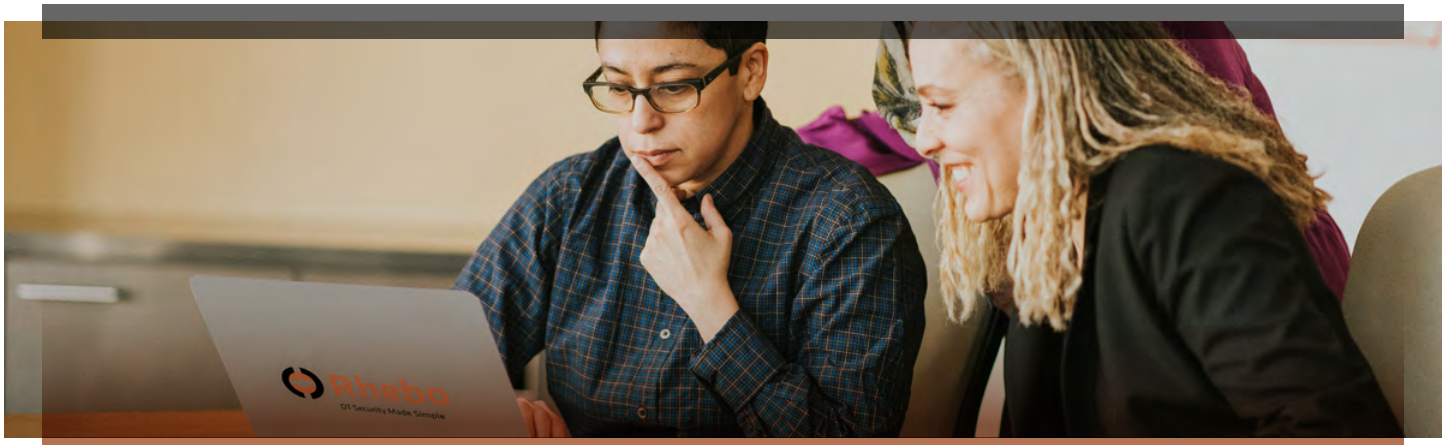
Wie das funktioniert

- kontinuierliche und netzbasierte Überwachung der Kommunikation in, zu und von der OT*,
- Verhaltensanalyse des laufenden Netzwerkverkehrs mit Deep Packet Inspection,
- passive und rückwirkungsfreie Überwachung und Detektion von Anomalien in der Kommunikation,
- Echtzeit-Meldung sicherheitsrelevanter Vorgänge und technischer Fehlerzustände,
- Bereitstellung der pcap-Dateien für die forensische Analyse,
- bedarfsorientierte Unterstützung durch Rhebo beim Aufbau der Baseline und dem Betrieb der OT-Angriffserkennung.

Warum Rhebo

- OT-Sicherheit Made in Germany für souveräne OT-Sicherheit,
- praxiserprobtes netzbasiertes Intrusion Detection System (NIDS) gegen mehrstufige und verdeckte Cyberangriffe,
- Installation isoliert und on-premise möglich,
- herstellerunabhängiges NIDS für jede OT-Umgebung,
- OT-Sicherheit leicht gemacht, auch für kleine Teams,
- einfache Skalierbarkeit auf mehrere Standorte mit einem zentralen Kontrollpunkt,
- aktives Support-Team mit jahrelanger Erfahrung in der OT-Sicherheit.

* Eine vollständige Liste der unterstützten Protokolle finden Sie im Spec Sheet für Rhebo Industrial Protector.



Schützen Sie Ihre OT vor Cyberangriffen

ww.rhebo.com | sales@rhebo.com | +49 341 3937900

1 OT-RISIKO- UND SCHWACHSTELLEN-BEWERTUNG

2 NETZBASIERTE ANOMALIE- UND ANGRIFFSERKENNUNG

3 FORENSIK & BETRIEBLICHER NIDS-SUPPORT

Geschützt durch Rhebo

Leipziger Wasserwerke | Thüringer Energienetze | envia TEL | MEGA | e·netz südhessen | STADTWERKE BOCHUM

OT Sicherheit Made In Germany

OT SECURITY Made in Germany | INFORMATION SECURITY MANAGEMENT SYSTEM DNV ISO/IEC 27001 | bitkom | CYBERSECURITY MADE IN EUROPE Initiated by ECSO. Issued by eurobits e.V. | Allianz für Cyber-Sicherheit

Rhebo OT Security Made Simple

Rhebo bietet einfache und effektive Lösungen zur Anomalie- und Angriffserkennung Made in Germany für die Netzleit-, Fernwirk- und Steuerungstechnik sowie IIoT Edge Devices in Kritischen Infrastrukturen, Versorgungs- und Industrieunternehmen. Wir unterstützen Unternehmen auf dem gesamten Weg der OT-Sicherheit von der initialen Risikobewertung über die forensische Analyse von Anomalien bis zum Betrieb des netzbasierten Angriffserkennungssystems. Als vertrauenswürdiges Cybersicherheitsunternehmen ist Rhebo nach ISO 27001 zertifiziert sowie Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«.

www.rhebo.com

Rhebo GmbH Spinnereistraße 7 | 04179 Leipzig | Deutschland
rhebo.com

SOLUTION BRIEF Rhebo Industrial Protector | 05-2026