Rhebo
a Landis+Gyr company

OT Security Made Simple

Rhebo OT Security

Effektive Angriffserkennung und Monitoring für die Netzleit- und Fernwirktechnik von Energieunternehmen

RISIKO VON OT-CYBER-VORFÄLLEN REDUZIEREN

durch Netzwerküberwachung,
Asset- und Schwachstellenerkennung

SCHNELL OT-SCHÄDEN ABWEHREN

durch frühzeitige Warnung
vor verdächtigen Netzwerkaktivitäten

FACHKRÄFTEMANGEL ÜBERBRÜCKEN

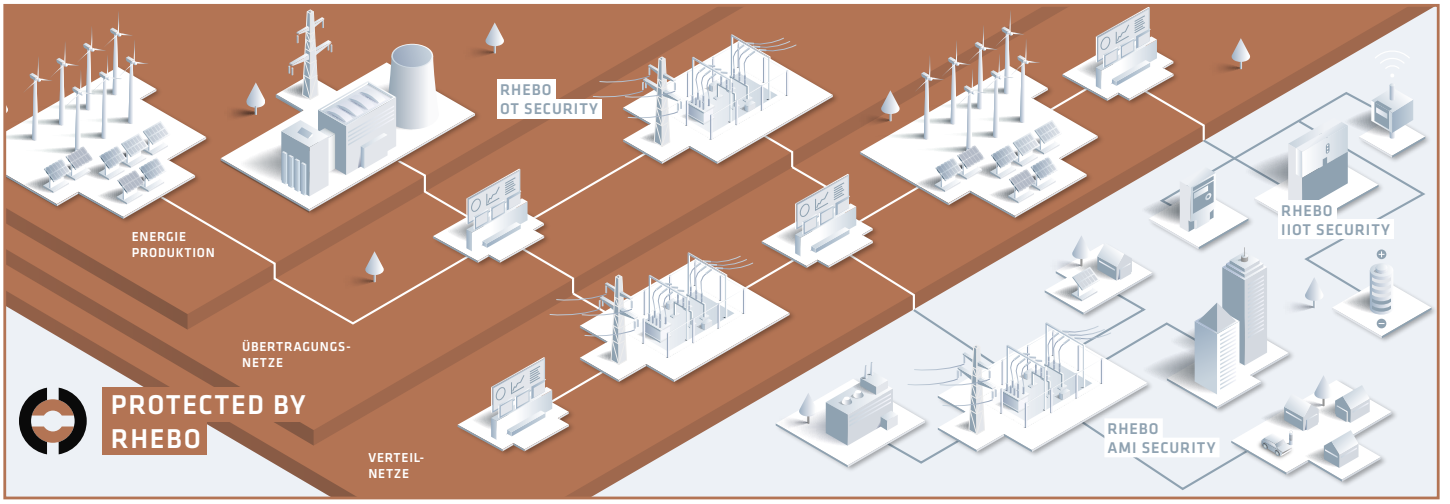
durch auf Sie zugeschnittene
OT-Sicherheits-Services

»Mit Rhebo können wir nicht nur fundiert prüfen und nachweisen, dass unsere Netzleittechnik sicher und stabil läuft. Rhebo schafft uns auch den detaillierten Einblick in unsere Fernwirktechnik und Prozessnetzsteuerung, um sonst schwer sichtbare neuartige Angriffe und Fehlkonfigurationen schnell zu erkennen, einzugrenzen und zu beheben«.

Dipl.-Ing (TU) Sven Hanemann | IT-Sicherheitsbeauftragter | e-netz Südhessen AG

Rhebo bietet einfache und effektive Cybersicherheitslösungen »Made in Germany« für die Netzleit- und Fernwirktechnik (Operational Technology, OT) von Energieunternehmen und Kritische Infrastrukturen. Rhebo OT Security überwacht kontinuierlich die Kommunikation innerhalb der OT. Jede Anomalie in der Netzleit- und Fernwirktechnik wird in Echtzeit erkannt, bewertet und gemeldet, so dass schnell und gezielt reagiert werden kann. Selbstverständlich werden Unternehmen aus dem Energiesektor von Rhebo entlang des gesamten OT-Sicherheitslebenszyklus unterstützt – von der ersten Risikoanalyse bis zur betreuten OT-Überwachung mit Anomalien- und Angriffserkennung.

Rhebo OT Security Gezielt & Einfach



Risiken
komplexer Infrastrukturen zur Energieversorgung

Durch das Einbinden von Stadtwerken, Erneuerbare-Energieanlagen und dem Aufbau neuer Umspannwerke **wird die Infrastruktur zur Energieversorgung immer komplexer.** Häufig liegen die einzelnen Stationen weit entfernt zur zentralen Leitwarte. Die Steuerung erfolgt deshalb zunehmend digital über Fernzugänge. Zur Absicherung dieser Peripherieanlagen setzen Verteilnetzbetreiber und Übertragungsnetzbetreiber häufig ausschließlich auf Firewalls. Diese erkennen in der Regel zuverlässig bekannte Schadsoftware. **Firewalls sind jedoch blind gegenüber neuartigen Angriffsmustern und professionellen Angriffen,** die häufig über Monate oder Jahre laufen. Das BSI spricht allein in Deutschland von 320.000 neuen Schadsoftware-Varianten pro Tag. **Die wenigen existierenden Sicherheitsmechanismen in der Netzleit- und Fernwirktechnik reichen nicht,** um gegen die wachsende Bedrohungslage gewappnet zu sein. Das Personal vor Ort ist selten für die Betreuung der Netzleittechnik ausgebildet oder befugt. Zudem ist die Kommunikation innerhalb der Anlagen für die zentrale Überwachung in der Leitwarte in der Regel eine Blackbox. Fehlerhafte oder schadhafte Kommunikation in Umspannwerken und anderen ferngesteuerten Energieanlagen wird erst erkannt, wenn sie bereits Auswirkungen auf die Systemstabilität hat. **Cyberkriminelle haben dadurch einfaches Spiel,** die Operational Technology auszukundschaften, sich in der Kritischen Infrastruktur auszubreiten sowie direkten Schaden anzurichten und die Behebung zu stören.

»Durch das Audit haben wir ein klareres Bild aller Vorgänge in unserer komplexen Netzleittechnik erhalten. So konnten wir den gesamten Kommunikationsverkehr ausgiebig analysieren und das Netz gezielt nach Sicherheitslücken überprüfen. Der reibungslose Ablauf hat uns begeistert und die direkte Erarbeitung sinnvoller Maßnahmen bestens auf kommende Cybersicherheitsrisiken vorbereitet.«

Falk Fischer | Team Leiter IT-Systeme und Anwendungen | Leipziger Wasserwerke

Durchgängige Angriffserkennung
in Kritischen Infrastrukturen aufbauen

Rhebo unterstützt Energieunternehmen auf dem gesamten Weg zu effektiver OT-Cybersicherheit – von der initialen Risikoanalyse bis zum Betrieb des Rhebo Angriffserkennungssystems. Mit Rhebo OT Security können sich Kritische Infrastrukturen auf die langjährige Expertise von Rhebo bei der Absicherung der Netzleit- und Fernwirktechnik verlassen. **Rhebos Next Generation OT Intrusion Detection System verbindet OT-Monitoring mit rückwirkungsfreier Anomalie- und Angriffserkennung,** wie es das IT-Sicherheitsgesetz bis 2023 von Kritischen Infrastrukturen verlangt. Das System wurde gezielt für industrielle Netzwerke entwickelt und überwacht die gesamte Kritische Infrastruktur von der zentralen Energieproduktion bis zu verteilten Energieversorgungssystemen wie Umspannwerken und Erneuerbare Energieanlagen. Mit Rhebo OT Security können Energieunternehmen gezielt ein **Ende-zu-Ende-Sicherheitsmonitoring für ihre komplexe Infrastruktur** aufbauen, das ihnen in Echtzeit jegliche Kommunikationsänderungen meldet, die auf Cyberangriffe, Manipulation, Scans oder technische Fehlerzustände hinweisen. Rhebo OT Security unterstützt alle gängigen Plattformen und lässt sich **kosteneffizient und einfach** in jedes industrielle Netzwerk integrieren als:

- dedizierte industrielle **Hardware** für physische Setups;
- **virtuelle** Appliance für den Betrieb in VMware, Hyper-V und anderen Virtualisierungsumgebungen;
- **softwarebasierte** Sensoren für gängige Sicherheitsgateways, Edge-Computing-Geräte und Substation Server von u.a. Barracuda, Bosch Rexroth, Cisco, INSYS icom Smart Devices, RAD, Siemens RUGGEDCOM und Welotec.

Rhebo OT Security **unterstützt alle spezifischen Protokolle,** die in Energieversorgungssystemen zur Anwendungen kommen, wie OPC, IEC 60870-5-104, IEC 61850-8-1 and DNP3 und viele mehr. Mit Rhebo OT Security steigern Energieunternehmen die **Cyberresilienz** ihrer OT-Systeme und können durch eine **Früherkennung von Risiken** die Ausbreitung von Angriffen auf andere Systembestandteile stoppen.

Einfach & Effektiv

3 Schritte zur sicheren Netzleit- und Fernwirktechnik

1

Der erste einfache Schritt
zu umfassender OT-Sicherheit:
Rhebo Industrial Security Assessment

Cybersicherheit beginnt mit Sichtbarkeit.

Die Rhebo OT-Risikoanalyse und Reifegradbeurteilung des **Rhebo Industrial Security Assessment** liefert ein detailliertes Verständnis der OT-Assets, der Netzwerk- und Kommunikationsstruktur sowie bestehender Sicherheitsrisiken. Unsere Kunden erhalten einen umfassende Übersicht und klare, effektive Handlungsempfehlungen, um die Systemhärtung zu steigern.

Sie profitieren von

- der Identifikation aller Geräte und Systeme in der OT inklusive ihrer Eigenschaften, Firmware-Versionen, Protokolle und Kommunikationsverbindungen (Asset Discovery & Inventory);
- der detaillierten Analyse bestehender Schwachstellen nach CVE;
- der Identifikation bestehender Gefährdungen, Sicherheitslücken und technischer Fehlerzustände;
- Handlungsempfehlungen mit Abschlussbericht und Workshop.

2

Der nahtlose Übergang zu
durchgängiger OT-Sicherheit:
Rhebo Industrial Protector

OT-Sicherheit endet nicht an den Netzwerkgrenzen.

Das OT-Monitoring mit integrierter Angriffserkennung **Rhebo Industrial Protector** schafft dedizierte OT-Sicherheit entsprechend des IT-SiG 2.0. Es erweitert die Absicherung durch Firewalls um eine ganzheitliche Anomalieerkennung innerhalb der OT, ohne kritische industrielle Prozesse zu stören.

Sie profitieren von

- der Echtzeit-Sichtbarkeit des Kommunikationsverhaltens aller OT- und ICS-Geräte (Protokolle, Verbindungen, Datenraten);
- der Echtzeitmeldung und -lokalisierung von Vorgängen (Anomalien), die auf Cyberattacken, Manipulation und technische Fehlerzustände hinweisen;
- der frühzeitige Identifikation von Angriffen über Backdoors, bislang unbekannte Schwachstellen und Innentätern, die von Firewalls übersehen werden (Defense-in-Depth)

3

Wir überwachen, damit Sie sich
um Ihr Kerngeschäft kümmern können:
Rhebo Managed Protection

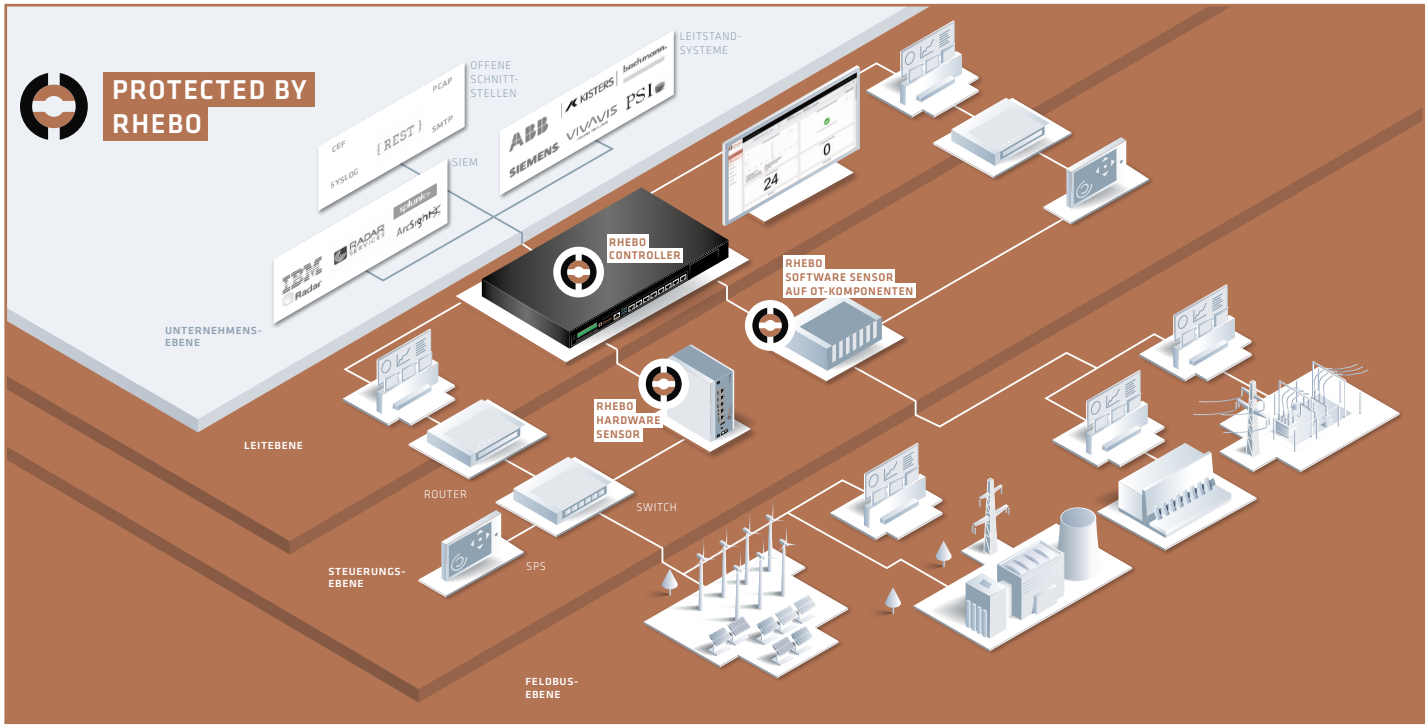
OT-Sicherheit braucht Ressourcen und Know-How.

Rhebo unterstützt Sie mit **Rhebo Managed Protection** beim Betrieb des OT-Sicherheitsmonitorings mit Anomalieerkennung, insbesondere bei der Auswertung und Reaktion auf Vorfälle sowie der kontinuierlichen Überprüfung und Verbesserung der Abwehrmechanismen.

Sie profitieren von

- der Unterstützung unserer Expert:innen beim Betrieb des OT-Sicherheitsmonitorings;
- der schnellen forensischen Analyse und Aufklärung von OT-Anomalien;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- regelmäßigen OT-Risikoanalysen für die kontinuierliche Verbesserung des Reifegrads Ihrer Cybersicherheit.

Beispiel-Deployment von Rhebo OT Security
in der Netzleit- und Fernwirktechnik



Rhebo Industrial Protector
Die schlanke und dedizierte OT-Angriffserkennung

Rhebo Industrial Protector bietet einsatzbereite **OT-Sicherheit für Unternehmen.** Das System zur Angriffserkennung erweitert die bestehende Perimeter-Firewall-Sicherheit durch die Integration von netzwerkbasierter OT-Überwachung mit Anomalieerkennung. Jede Kommunikation, die auf Cyberangriffe, Manipulationen, Spionage oder technische Fehler hinweist, wird in Echtzeit gemeldet. Dies ermöglicht auch die frühzeitige Erkennung von mehrstufigen Angriffsmustern, wie sie im MITRE ATT&CK for ICS Rahmenwerk beschrieben sind.

Was Sie erreichen
- Echtzeit-Erkennung von Cyberangriffen und technischen Fehlerzuständen innerhalb der OT und Leittechnik,
- vollständige Sichtbarkeit der OT-Komponenten für das Asset Inventory,
- Dokumentation von Asset-Eigenschaften einschließlich Protokollen, Verbindungen und Schwachstellen,
- Wissensaufbau zu OT-Sicherheit,
- Compliance mit den Anforderungen an ein System zur Angriffserkennung in der OT nach IT-SiG 2.0, NIS2UmsuCG und BSI.

Wie das funktioniert
- kontinuierliche netzbasierte Überwachung der Kommunikation in, zu und von der OT*,
- Verhaltensanalyse des Netzwerkverkehrs mit Deep Packet Inspection,
- Echtzeit-Meldung von Kommunikationsanomalien, einschließlich pcap-Dateien für forensische Analysen,
- passive, rückwirkungsfreie Überwachung und Erkennung,
- bedarfsorientierte Unterstützung durch Rhebo beim Betrieb der OT-Angriffserkennung.

Warum Rhebo
- bewährte OT-Cybersicherheit Made in Germany gegen mehrstufige, ausgefeilte Cyberangriffe und Zero-Day-Exploits,
- OT-Sicherheit leicht gemacht, auch für kleine Teams,
- einfache Skalierbarkeit auf mehrere Standorte mit einem zentralen Kontrollpunkt,
- umfassende Unterstützung von der ersten Risikoanalyse bis zum Betrieb der Angriffserkennung.

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

Rhebo OT Security Made Simple

LANGJÄHRIGE ERFAHRUNG
in industriellen Sicherheitslösungen für Energie- und Wasserunternehmen.

DEDIZIERTE UND EINFACHE LÖSUNG
für die kosteneffiziente Integration in die Operational Technology, Advanced Metering Infrastructure und IIoT.

UMFASSENDE UNTERSTÜTZUNG
bei der schnellen und gezielten Steigerung der industriellen Cyberresilienz.

SICHERHEIT VOR BESTEHENDEN SCHWACHSTELLEN
durch regelmäßige OT-Risikobewertungen, -Sicherheitsanalysen und -Reifegradbeurteilungen.

SICHERHEIT VOR BEKANNTEN UND NEUARTIGEN CYBERANGRIFFEN
durch OT-Angriffserkennungssystem (IDS) mit OT-Monitoring, Asset Discovery und Threat & Intrusion Detection.

ENDE-ZU-ENDE-SICHERHEIT
durch Anomalieerkennung zur Vermeidung der Risikoausbreitung über die OT, IIoT und Advanced Metering Infrastructure.

»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«.

Dipl.-Ing Daniel Beyer | ISB und Fachgebietsleiter Systemtechnik | Thüringer Energienetze GmbH & Co. KG

OT SECURITY MADE SIMPLE
durch OT-fokussierte Sicherheitsanalyse und intelligente Visualisierung.

SICHERSTELLUNG DER HANDLUNGSFÄHIGKEIT
durch Rhebo-Unterstützung bei Risikoanalyse, Betrieb und forensischer Analyse.

SYSTEMSICHERHEIT
durch flexible und kosteneffiziente Integration der Rhebo-Lösung auf IIoT-Geräten und Netzwerkkomponenten.

SICHERHEIT VOR INTRANSPARENTEN KOSTEN
durch einfache Lizenzpakete und unkomplizierte Lösungsintegration.

COMPLIANCE SICHERSTELLEN
durch System zur Angriffserkennung für die OT nach ITSiG 2.0 und einschlägigen Sicherheitsstandards.

VERTRAUENSVOLLE SICHERHEIT MADE IN GERMANY
nach den Anforderungen der European Cyber Security Organisation (ECSO) und DSGVO.

Machen Sie Ihre OT-Risikoanalyse oder buchen Sie eine Demo

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

Entdecken Sie industrielle End-to-End-Cybersicherheit von Rhebo

↗ Rhebo AMI Security

↗ Rhebo IIoT Security

Geschützt durch Rhebo

Stromnetz Hamburg · Leipziger Wasserwerke · Thüringer Energienetze · Landis+Gyr · BayWa r.e. · MITNETZ STROM

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 · Plattform Industrie 4.0

Rhebo OT Security Made Simple

Rhebo bietet einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen, Kritischen Infrastrukturen und Industrieunternehmen. Das deutsche Unternehmen unterstützt Kunden auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung. Rhebo ist seit 2021 Teil der Landis+Gyr AG, einem global führenden Anbieter integrierter Energiemanagement-Lösungen für die Energiewirtschaft mit weltweit rund 7.500 Mitarbeiter:innen in über 30 Ländern. 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 Spinnereistr. 7 | 04179 Leipzig | Germany
rhebo.com

SOLUTION BRIEF RHEBO OT SECURITY 02-2025