YELLO NETCOM

Rhebo

Industrial Network Continuity PORTFOLIO

Industrielle IT-Sicherheit von A bis Z Standortübergreifender Schutz für Kritische Infrastrukturen und Industrieunternehmen

OT-CYBERSECURITY UND ANGRIFFSERKENNUNG nach IT-SiG2.0 durch Next Generation OTIntrusion Detection.

ECHTZEIT-TRANSPARENZ vom ICSbis zum Industrial-IoT-Gerät durch OT-Monitoring.

GANZHEITLICHE BETREUUNG von der Risikoanalyse bis zur kontinuierlichen Überwachung und Abwehr.

Wir begleiten Sie bei jedem Schritt

Moderne industrielle Infrastrukturen benötigen ganzheitliche Cybersicherheit von der zentralen Leitwarte über die Netzleit-, Fernwirk- und Steuerungstechnik (Operational Technology, OT)bis zu den vernetzten IIoT Edge Devices.

Rhebo bietet standortübergreifende Sichtbarkeit und Intrusion Detection für industrielle Netzwerke und IIoT-Geräte.UnsereDienstleistungen und unser OT-Monitoring mit integrierter Anomalie- und Angriffserkennung unterstützen Energieunternehmen, Kritische Infrastrukturen und Industrie auf ihrem Weg zu durchgehender Cybersicherheit.

Rhebo begleitet Unternehmen Schritt für Schritt von der initialen Risiko- und Schwachstellenanalyse über den Aufbau eines kontinuierlichen OT-Monitorings bis zum Betrieb der Sicherheitslösung und forensischen Analyse auftretender Vorfälle.

So können sich unsere Kunden auf ihr Kerngeschäft konzentrieren sowie die Digitalisierung und Automatisierung ihrer industriellen Systeme und Anlagen sicher vorantreiben.

Mit Rhebo in 3 Schritten zu durchgängiger OT-Sicherheit

1

MODUL

Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit

Cybersicherheit beginnt mit Sichtbarkeit.

Bei der Rhebo OT-Risiko- und Schwachstellenanalyse identifizieren wir bestehende Gefährdungen in Ihren industriellen Netzwerken, bewerten das Sicherheitsrisiko und erarbeiten Handlungsempfehlungen.

Sie profitieren von

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

2

MODUL

Rhebo Industrial Protector

Cybersicherheit endet nicht an den Netzwerkgrenzen.

Das Rhebo OT-Monitoring mit integrierter Anomalieerkennung erweitert die Absicherung durch Firewalls um eine ganzheitliche Angriffserkennung entsprechend des IT-SiG2.0 und internationaler Standards.

Sie profitieren von

- der Echtzeit-Übersicht über das Kommunikationsverhalten aller OT-und IIoT-Assets (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

MODUL

Rhebo Managed Protection

Cybersicherheit braucht Ressourcen und Know-how.

Rhebo unterstützt Sie auch 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

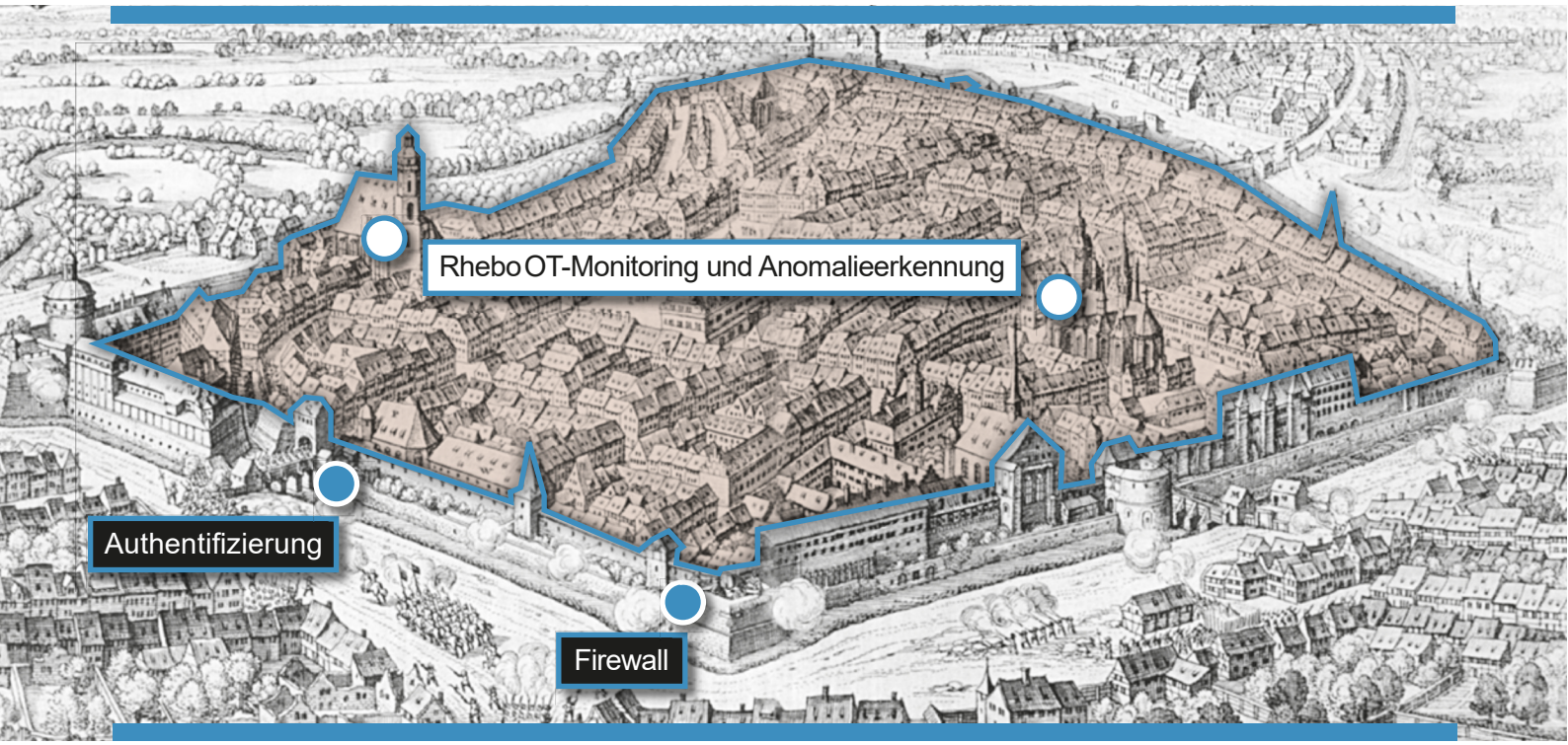
- Expert:innen-Unterstützung beim Betrieb des OT-Sicherheitsmonitorings;
- der schnellen forensischen Analyse und Aufklärung von Anomalien in der OT;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- regelmäßigen OT-Risiko- und Schwachstellenanalyse für kontinuierliche Verbesserung.

Rhebo schafft Sicherheit von der Leitwarte bis zum IIoT-Gerät

- SICHERHEIT VOR SCHWACHSTELLEN durch regelmäßige Risikobewertungen und Sicherheitsanalysen der industriellen Netzwerke.
- SICHERHEIT VOR TECHNISCH BEDINGTEN ANLAGENAUSFÄLLEN durch integriertes Network Condition Monitoring.
- COMPLIANCE-SICHERHEIT durch System zur Angriffserkennung für die OT nach ITSiG2.0 und internationalen Sicherheitsstandards.
- SICHERHEIT VOR UNBEKANNTEN GERÄTEN UND VORGÄNGEN durch detaillierte Asset Discovery und Inventarisierung der OT-und IoT-Infrastruktur.
- SICHERHEIT VOR ANGRIFFEN AUF VERTEILTE ANLAGEN durch standortübergreifendes Sicherheitsmonitoring von der Zentrale bis zu den IIoT-Geräten.
- SYSTEMSICHERHEIT durch flexible und kosteneffiziente Integration der Rhebo-Lösung auf IIoT-Geräten und Netzwerkkomponenten.
- SICHERHEIT VOR BEKANNTEN UND NEUARTIGEN CYBERANGRIFFEN durch Next Generation OT Intrusion Detection System mit OT-Monitoring und Anomalieerkennung.
- SICHERSTELLUNG DER HANDLUNGSFÄHIGKEIT durch Rhebo Expert:innen-Unterstützung bei Betrieb, forensischer Analyse und Risikobewertung.
- SICHERHEIT VOR BACKDOORS durch deutsche Produktentwicklung nach den Anforderungen der European Cyber Security Organisation (ECSO) und DSGVO.

Innere Sicherheit für Operational Technology

Automatisierte, vernetzte Industrieanlagen müssen wie ein moderner Stadtstaat gesichert werden. Firewalls, Datendioden und Authentifizierung bilden den Stadtwall und die Torwächter, die bekannte Gefährdungen von außen abwehren. Compliance-Richtlinien des ISMS liefern den Nutzer:innen im Unternehmen einen klaren Verhaltenskodex. Sie können jedoch nichts gegen den mittlerweile sehr wahrscheinlichen Fall ausrichten, dass Angreifende die klassischen Schutzmaßnahmen umgehen – ob durch Lücken in der Firewall, Brute-Force, unbekannte Schwachstellen (Zero Day Exploits), Innentäter:innen, Backdoors oder über gestohlene Zugangsdaten. Das Rhebo OT-Monitoring mit Anomalieerkennung bildet deshalb eine zweite Verteidigungslinie – die Polizei für Innere Sicherheit. Das System überwacht alle Bewegungen innerhalb der Netzleit-, Fernwirk- und Steuerungstechnik und meldet verdächtiges Verhalten, selbst wenn es über autorisierte Kanäle erfolgt. Eindringlinge werden in Echtzeit erkannt und so die Innere Sicherheit der industriellen Prozesse gewahrt.



Sichern Sie Ihre Operational Technology gegen Cyberangriffe und Störungen

1

OT-Risiko- und Schwachstellenanalyse

2

Kontinuierliche Überwachung und Angriffserkennung Ihrer OT

3

Managed Detection and Response

www.rhebo.com | sales@rhebo.com| +49 3413937900

Geschützt durch Rhebo

Stromnetz Hamburg · Leipziger Wasserwerke · Thüringer Energienetze · e·netz südhessen · BayWa r.e. · MITNETZ STROM

Über Rhebo

Rhebo entwickelt und vermarktet OT- und IIoT-Cybersecurity-Lösungen für Energieunternehmen, Kritische Infrastrukturen und Industrie. Das Unternehmen bietet standortübergreifende Cybersicherheit,Angriffserkennung und Sichtbarkeit in industriellen Netzwerken (ICS)durch OT-Monitoring und Threat & Intrusion Detection von der initialen Risikoanalyse bis zum Betrieb. Rhebo ist seit 2021Teil der Landis+Gyr AG,einem global führenden Anbieter integrierter Energiemanagement-Lösungenfür die Energiewirtschaft mit weltweit rund 5.000 Mitarbeiter:innen in über30 Ländern. Rhebo ist Partner der Allianz für Cyber-Sicherheitdes Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Teletrust – Bundesverband IT-Sicherheit e.V.. Als vertrauenswürdiges IT-Sicherheitsunternehmen ist Rhebo offizieller Träger der Gütesiegel »IT Security Made in Germany« sowie »Cybersecurity Made In Europe«.

www.rhebo.com

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