Rhebo IIoT Security

Sistema di rilevamento e difesa dalle intrusioni per dispositivi e asset IIoT critici distribuiti

RIDURRE IL RISCHIO DI INCIDENTI INFORMATICI IIOT

attraverso il monitoraggio delle comunicazioni e il rilevamento delle vulnerabilità

CONSENTE UNA RAPIDA MITIGAZIONE DEGLI ATTACCHI IIOT

attraverso il rilevamento delle anomalie e l'automazione della sicurezza

COLMARE IL GAP DI COMPETENZE IN MATERIA DI SICUREZZA IIOT

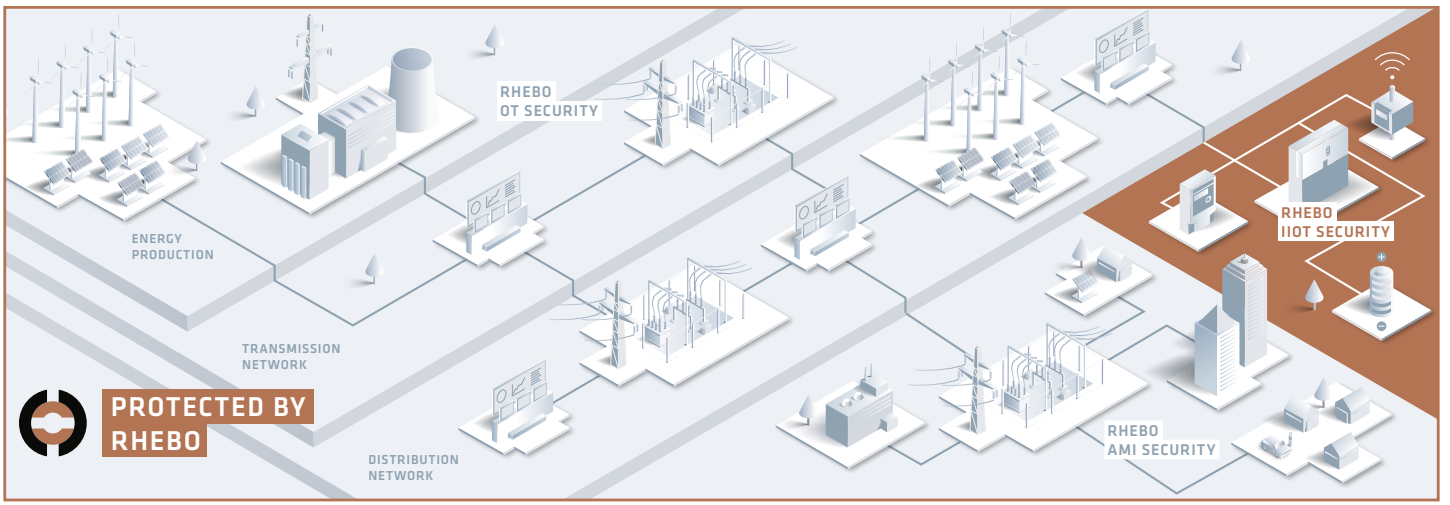
con servizi su misura per le vostre esigenze

»Nella scelta della soluzione, ritenevamo particolarmente importante che il monitoraggio e l'automazione della cybersicurezza fossero adattati in modo specifico ai nostri dispositivi e potessero essere ampliati in qualsiasi momento. Perché sia la nostra tecnologia che la situazione delle minacce sono in continua evoluzione«

Daniel Ackermann | Responsabile Software Development | Sonnen

Rhebo IIoT Security consente alle aziende di produzione e di gestione di proteggere i propri asset e reti IIoT di tipo critico, di rispettare le normative sulla cybersicurezza e di risparmiare costi legati ai tempi di inattività. La soluzione è progettata per fornire un'efficace cybersicurezza industriale ai sistemi di accumulo di energia, alle stazioni di ricarica elettrica e ad altri asset IIoT distribuiti di valore elevato. Offre tutte le funzionalità per bloccare le intrusioni fin dall'inizio e per rilevare le minacce prima che si verifichino le interruzioni. Rhebo offre soluzioni di cybersicurezza semplici ed efficaci »Made in Germany« per la tecnologia operativa (OT), per gli asset industriali distribuiti nelle reti industriali IoT (IIoT) e per l'Advanced Metering Infrastructure.

Rhebo IIoT Security una soluzione mirata e semplice



I dispositivi IIoT distribuiti sono intelligenti
uma altamente vulnerabili

Il numero di dispositivi intelligenti presenti negli ambienti industriali è in aumento. Ciò non si limita ai componenti dei classici ambienti industriali, che possono essere facilmente protetti con Rhebo OT Security. Un numero sempre maggiore di infrastrutture altamente distribuite, come i sistemi di accumulo di energia, le stazioni di ricarica elettrica e i sistemi intelligenti Demand-Site-Response, utilizzano tutti funzioni smart. Spesso comunicano con la piattaforma operativa centrale tramite Internet e servizi cloud pubblici. Inoltre, tali infrastrutture sono accessibili per interventi fisici e coinvolgono una varietà di utenti, tra cui aziende di manutenzione locali e utenti privati. Gli asset IIoT risultano quindi particolarmente esposti. Un singolo dispositivo compromesso può anche infettare l'intera flotta, se mancano i meccanismi di cybersicurezza adeguati. Ciò è particolarmente probabile nel caso di nuovi modelli di intrusione, di Advanced Persistent Threat e o vulnerabilità zero-day. Tale mancanza di chiarezza nell'esposizione al rischio rende le risorse critiche IIoT distribuite particolarmente vulnerabili ad attacchi su larga scala quali ransomware, attacchi DDoS, botnet o interruzioni orchestrate. Un attacco riuscito può implicare significative conseguenze negative per le operazioni e le relazioni con i clienti in tutto il mondo. Le aziende produttrici di dispositivi IIoT critici distribuiti hanno quindi bisogno di un sistema di rilevamento delle intrusioni e di anomalie intelligente, che rilevi anche i nuovi modelli di attacco e riduca al minimo il rischio della flotta, attraverso un'automazione intelligente e locale della cybersicurezza.

»La cybersicurezza dei nostri sistemi di stoccaggio dell'energia significa anche cybersicurezza per i nostri clienti in tutto il mondo.«

Daniel Ackermann | Responsabile Software Development | Sonnen

Endpoint Detection & Response
per la cybersicurezza della rete IIoT globale

Rhebo IIoT Security consente alle aziende di produzione e di gestione di dispositivi IIoT critici di garantire la disponibilità, l'integrità e la cybersicurezza della loro infrastruttura distribuita e di valore elevato. Rhebo IIoT Security si basa sul comprovato sistema di monitoraggio industriale dedicato di Rhebo con rilevamento delle anomalie e adatta la soluzione ai requisiti specifici dei dispositivi IIoT:

- utilizzo minimo della CPU,
- utilizzo minimo della larghezza di banda,
- automazione della cybersicurezza locale (ad esempio il blocklisting),
- semplice distribuzione globale,
- manutenzione remota.

Rhebo IIoT Security è integrato direttamente nel dispositivo IIoT come soluzione di Endpoint Detection and Response. Questa architettura di implementazione consente di rilevare e difendersi dagli attacchi a livello locale, impedendo il lateral movement, lo spillover e la propagazione progressiva delle minacce. Il rilevamento delle anomalie integrato apprende in poche ore la comunicazione autorizzata di tutti i dispositivi all'interno della rete IIoT. Durante il funzionamento, vengono monitorate tutte le comunicazioni tra i dispositivi IIoT e la piattaforma di gestione IIoT basata su cloud. Il rilevamento di specifici incidenti legati alla cybersicurezza su un dispositivo IIoT attiva l'automazione della cybersicurezza locale e blocca le comunicazioni dannose direttamente sul dispositivo interessato. Inoltre, qualsiasi deviazione dalla comunicazione autorizzata, ad esempio a causa di modifiche alla configurazione o alla comunicazione, nonché di condizioni di errore tecnico, viene segnalata come anomalia. In questo modo la gestione dell'azienda può localizzare i rischi di disponibilità e decidere misure correttive efficaci da applicare in modo immediato e mirato. Rhebo IIoT Security è disponibile sia come applicazione autonoma che come servizio gestito da Rhebo. Ciò permette alle aziende di produzione e di gestione degli asset IIoT distribuiti di concentrarsi sul proprio core business in tutta tranquillità.

Rhebo OT Security Made Simple

Rhebo aiuta le aziende industriali a **risparmiare milioni di euro** grazie alla conformità alla cybersicurezza e alla riduzione dei tempi di inattività.

Rhebo consente **l'immediata implementazione** di 10.000 – 100.000 dispositivi e oltre con una soluzione di cybersicurezza IIoT altamente scalabile.

Rhebo offre **un'installazione e un'amministrazione a basso costo,** senza team tecnici o di manutenzione locali.

PROTEZIONE DELLE VULNERABILITÀ ESISTENTI
attraverso la valutazione regolare dei rischi IIoT e la valutazione della maturità della cybersicurezza.

PROTEZIONE DA ATTACCHI NOTI E NUOVI
attraverso il sistema di rilevamento e difesa dalle intrusioni IIoT con funzioni quali monitoraggio, asset discovery, rilevamento di anomalie e automazione della cybersicurezza.

CYBERSICUREZZA END-TO END
attraverso il rilevamento delle anomalie per prevenire la propagazione delle minacce in OT, IIoT e nell'Advanced Metering Infrastructure.

»Rhebo ci consente di garantire a livello nazionale il nostro approvvigionamento energetico in modo centralizzato e affidabile, anche alle aziende che supervisioniamo personalmente e agli oltre 16.000 produttori decentralizzati. Grazie alla nuova trasparenza e al monitoraggio continuo, siamo riusciti ad aumentare visibilmente la qualità della nostra rete«.

Dipl.-Ing Daniel Beyer | Responsabile del settore ISB e dell'ingegneria dei sistemi | Thüringer Energienetze GmbH & Co. KG

(II)OT SECURITY MADE SIMPLE
attraverso l'analisi incentrata sull'IIoT, la visualizzazione degli incidenti e la difesa attiva contro vettori di attacco specifici.

GARANTIRE LA CAPACITÀ DI AGIRE
attraverso il supporto di Rhebo nella valutazione del rischio, nelle operazioni e nell'analisi forense.

SICUREZZA DEL SISTEMA
grazie all'integrazione e alla manutenzione flessibile ed economica della soluzione sotto forma di software containerizzato.

PROTEZIONE DAI COSTI NON TRASPARENTI
grazie a pacchetti di licenze semplici e all'integrazione immediata delle soluzioni.

GARANZIA DI CONFORMITÀ
attraverso un sistema di rilevamento delle intrusioni per l'IIoT conforme a ITSiG 2.0 e agli standard di cybersicurezza pertinenti.

CYBERSICUREZZA AFFIDABILE MADE IN GERMANY
secondo i requisiti della European Cyber Security Organisation (ECSO) e del GDPR.

Semplice ed efficace
3 passaggi per un IIoT sicuro

1

Il primo semplice passaggio per una cybersicurezza IIoT completa:
Rhebo Industrial Security Assessment

La sicurezza informatica inizia con la visibilità.

L'analisi dei rischi e la valutazione della maturità del **Rhebo Industrial Security Assessment** fornisce una visibilità dettagliata degli asset IIoT, della struttura di rete e di comunicazione e dei rischi di cybersicurezza esistenti. A seconda dei requisiti, la fase include una valutazione del rischio degli asset IIoT e della piattaforma operativa attraverso il monitoraggio delle comunicazioni e un pentest dei dispositivi IIoT selezionati.

Potrete beneficiare di

- analisi dei modelli di comunicazione tra i dispositivi IIoT e la piattaforma operativa, compresi i protocolli, le connessioni e il comportamento della comunicazione,
- analisi dettagliata delle vulnerabilità esistenti secondo CVE,
- identificazione dei rischi informatici e delle vulnerabilità della cybersicurezza,
- azioni consigliate con rapporto finale e workshop.

2

La transizione perfetta verso la cybersicurezza IIoT end-to-end:
Rhebo Industrial Protector

Una cybersicurezza personalizzata, che lavora a livello locale per proteggere a livello globale.

La soluzione Rhebo IIoT Security **Rhebo Industrial Protector** offre un monitoraggio della cybersicurezza industriale con rilevamento e difesa integrata di attacchi e anomalie. Funziona direttamente sugli asset IIoT e rileva qualsiasi deviazione di comunicazione. In base alle politiche di cybersicurezza individuali dell'azienda che opera, le anomalie vengono bloccate attivamente sul dispositivo interessato o segnalate al centro di controllo per un'ulteriore valutazione.

Potrete beneficiare di

- una soluzione di cybersicurezza IIoT su misura per le vostre esigenze di automazione della cybersicurezza,
- trasparenza in tempo reale del comportamento di comunicazione di tutti gli asset IIoT (protocolli, connessioni, frequenze),
- segnalazione in tempo reale di eventi di cybersicurezza e stati tecnici di errore,
- difesa dell'attacco a livello di dispositivo per impedire la propagazione nella rete,
- elevata scalabilità grazie al software containerizzato.

3

Il segreto per la tranquillità.
Siamo noi a occuparci del monitoraggio:
Rhebo Managed Protection

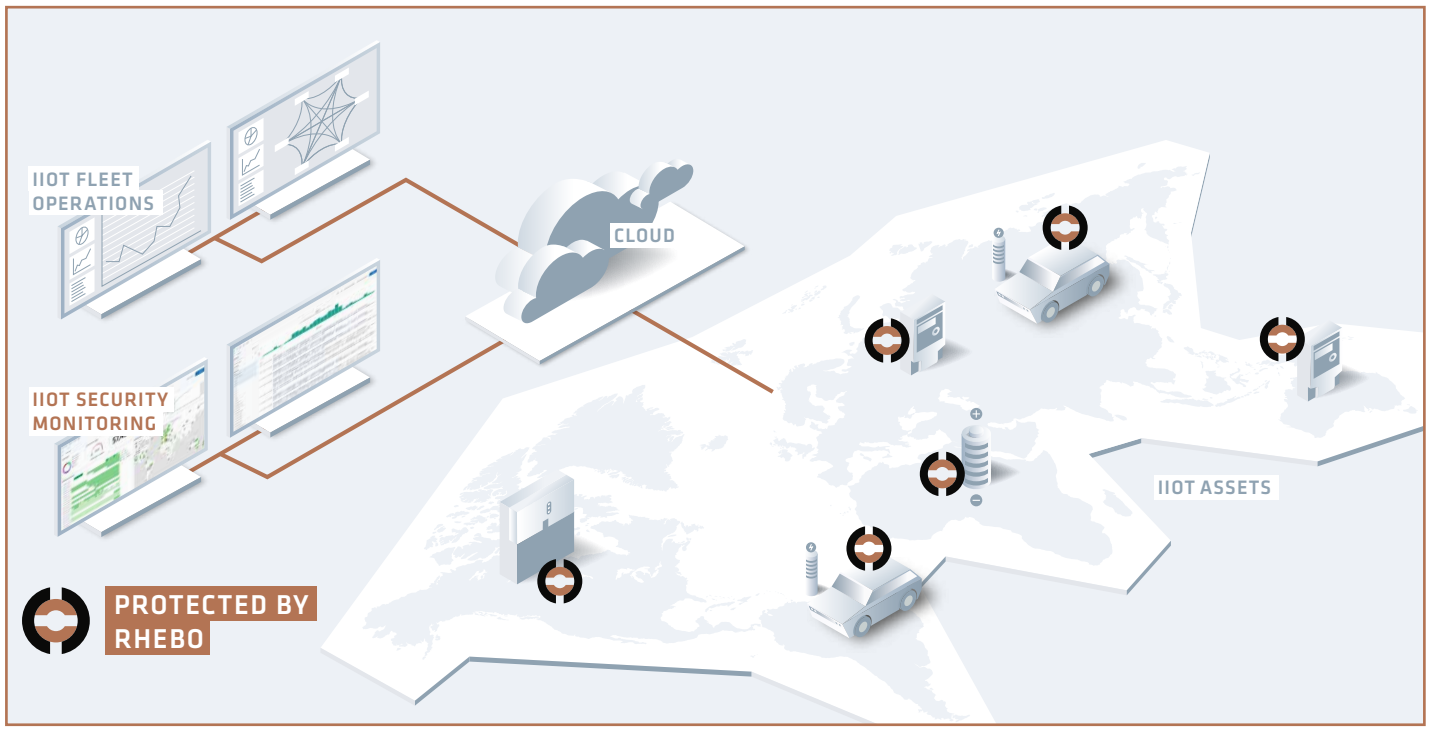
La sicurezza informatica necessita di risorse e know-how.

Vi supporta con **Rhebo Managed Protection** nelle operazioni di monitoraggio della cybersicurezza IIoT, in particolare nella valutazione e nella reazione agli incidenti, nonché nella revisione e nel miglioramento continuo dei meccanismi di difesa.

Potrete beneficiare di

- il supporto dei nostri esperti nelle operazioni di monitoraggio della cybersicurezza IIoT,
- analisi forense immediata e rilevamento delle anomalie IIoT,
- capacità di agire immediatamente in caso di incidenti,
- miglioramento continuo attraverso analisi regolari dei rischi IIoT e pentest.

Esempio di implementazione di Rhebo IIoT Security
nelle reti IIoT



Una cybersicurezza agile e personalizzata
per i vostri asset IIoT

Rhebo IIoT Security funziona come una soluzione di cybersicurezza IIoT completamente integrata e personalizzata. Si avvale del collaudato sistema di monitoraggio industriale e di rilevamento delle anomalie Rhebo Industrial Protector e lo integra con funzioni specifiche per l'IIoT, come la difesa attiva dagli attacchi e la containerizzazione del software. La soluzione viene implementata a livello di dispositivo tramite pacchetti software che possono essere installati e gestiti da remoto in modo completamente automatizzato.

Oggetto?

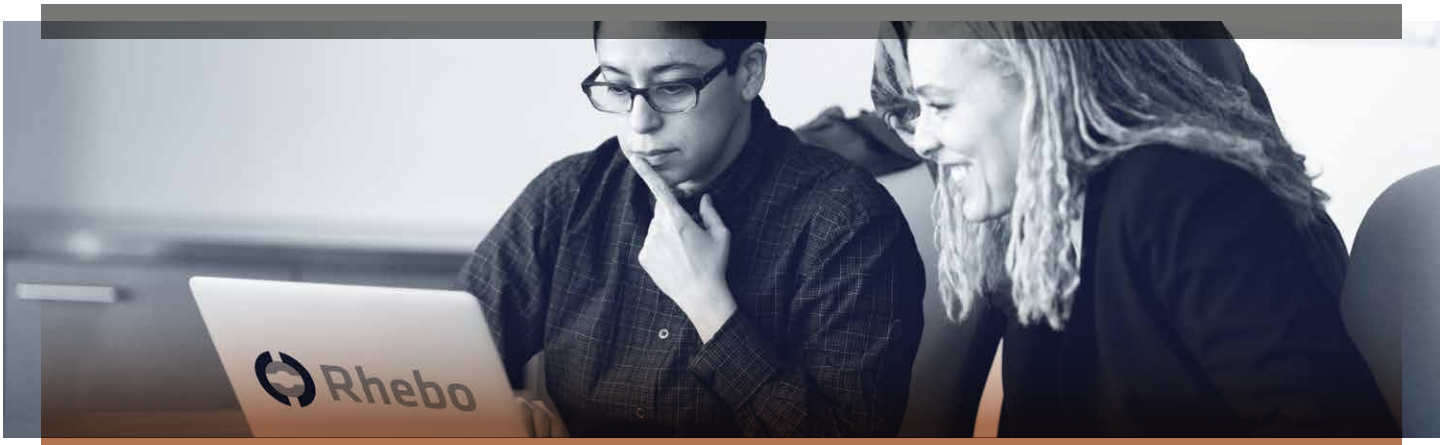
- rilevamento e difesa in tempo reale di attacchi informatici e incidenti informatici critici a livello di dispositivo,
- segnalazione in tempo reale di qualsiasi anomalia alla gestione dell'azienda,
- piena trasparenza dalla rete IIoT al dispositivo in termini di rischi, vulnerabilità e stati tecnici di errore,
- servizi opzionali gestiti dagli esperti Rhebo.

Soluzioni?

- monitoraggio locale di tutte le comunicazioni sui dispositivi IIoT,
- analisi continua del comportamento di ogni dispositivo e delle rispettive interfacce locali, come le interfacce web e i protocolli di sistema,
- Deep Packet Inspection fino al livello dei valori,
- automazione della cybersicurezza personalizzata per le linee guida di cybersicurezza del cliente.

Scopo?

- cybersicurezza completa contro gli attacchi informatici e le manipolazioni locali;
- nessun degrado delle prestazioni degli asset grazie a un design adattato alle limitazioni di CPU e memoria dei dispositivi IIoT;
- elevata scalabilità grazie alla distribuzione e alla manutenzione remote e automatizzate;
- supporto completo di Rhebo, dalla progettazione al funzionamento.



Rendete impenetrabili i vostri dispositivi e asset IIoT. Contattateci per una demo.

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

Convincetevi di persona. Chiedete ai nostri clienti!

↗ Scoprite come la rinomata Sonnen GmbH protegge i suoi oltre 60.000+ sistemi di accumulo di energia privati distribuiti a livello globale con la soluzione Rhebo IIoT Security.

Protetti da Rhebo

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

OT Security Made In Germany

OT SECURITY Made in Germany · TeleTrusT Pioneers in IT security. · 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 offre semplici ed efficaci soluzioni di cibersicurezza per la telegestione, per i sistemi di controllo, per gli impianti industriali, per fornitori di energia, per le infrastrutture critiche e per le aziende industriali. L´ impresa tedesca supporta i propri clienti durante tutto il processo della sicurezza OT a partire dall'analisi iniziale del rischio fino al monitoraggio con il rilevamento di anomalie e intrusioni. Dal 2021 Rhebo fa parte del gruppo multinazionale svizzero Landis+Gyr AG, leader di soluzioni integrate per la gestione energetica. Landis + Gyr conta circa 7.500 dipendenti in più di 30 paesi. Rhebo e' partner dell' Alleanza per Cybersicurezza dell'Ufficio Federale Tedesco per la Sicurezza Informatica (BSI) e della TeleTrust – Associazione Federale Tedesca della sicurezza IT. Come impresa affidabile IT, Rhebo e' portatore ufficiale del sigillo di qualità »Cybersecurity Made in Europe«.

www.rhebo.com

Rhebo GmbH Spinnereistr. 7 | 04179 Leipzig | Germany
rhebo.com

SOLUTION BRIEF RHEBO IIOT SECURITY 04-2023 IT