



## Sicurezza OT di Rhebo

### Monitoraggio efficace e rilevamento delle minacce ICS per le aziende di fornitura elettrica



#### VISIBILITÀ DELL'OT IN TEMPO REALE

attraverso il rilevamento degli asset e il monitoraggio delle comunicazioni ICS.



#### RILEVAMENTO TEMPESTIVO DELLE INTRUSIONI

attraverso il rilevamento delle anomalie nell'OT per una rapida mitigazione delle minacce.



#### SERVIZI DI SICUREZZA OT

dall'analisi dei rischi per l'infrastruttura al continuo monitoraggio dell'OT e l'analisi forense.



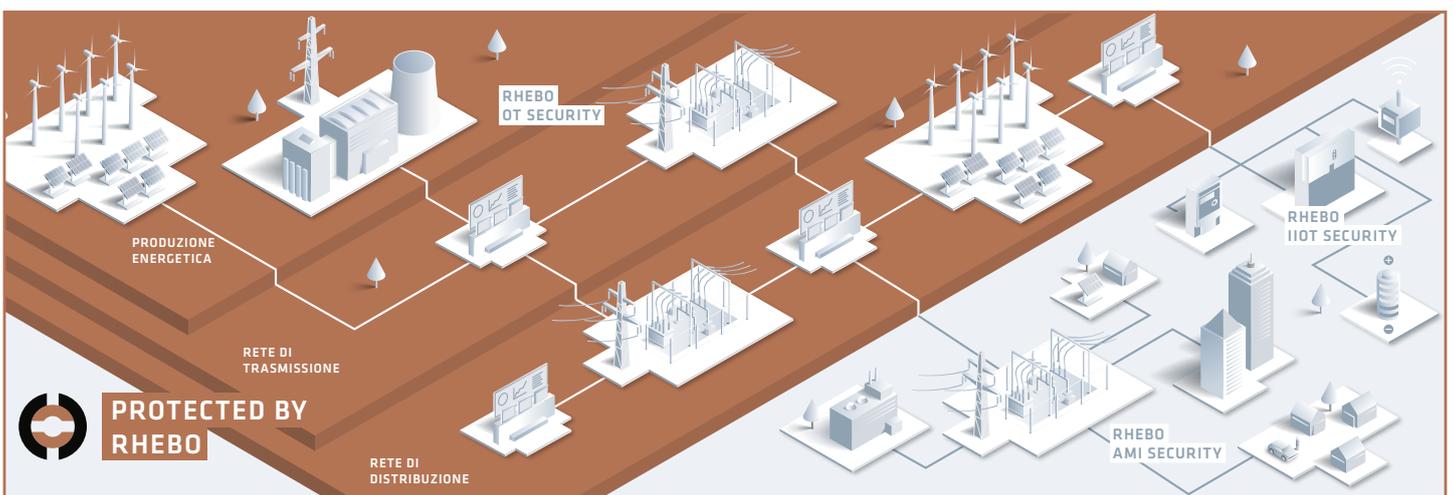
»Con Rhebo possiamo garantire attivamente che il nostro sistema di controllo e automazione industriale (Industrial Automation & Control System, IACS) sia stabile e sicuro. Rhebo fornisce maggiore visibilità nei nostri IACS al fine di identificare e mitigare rapidamente nuovi attacchi e configurazioni errate che non siamo riusciti a vedere in passato.«

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

Rhebo fornisce sicurezza informatica e rilevamento delle intrusioni »Made in Germany« semplici ed efficaci per l'Operational Technology (OT) e gli asset industriali distribuiti per il settore energetico, l'infrastruttura critica e la produzione. La soluzione monitora continuamente le comunicazioni ICS e OT per rilevare eventuali minacce e at-

tacchi. Eventuali anomalie nella comunicazione vengono rilevate, valutate e segnalate in tempo reale. Rhebo supporta completamente le aziende del settore energetico nel ciclo di vita della sicurezza informatica industriale, dall'analisi del rischio iniziale al monitoraggio gestito dell'OT con rilevamento di intrusioni e anomalie.

## Rhebo Sicurezza OT dedicata e semplice



## Nuove sfide per i sistemi di fornitura energetica complessi

La **rete elettrica sta diventando sempre più frammentata** a causa dell'integrazione di aziende dei servizi pubblici municipali, risorse di energia rinnovabile e la costruzione di nuove sottostazioni. Le singole stazioni sono spesso lontane dalla postazione di controllo centrale. Pertanto, il controllo viene eseguito sempre di più digitalmente attraverso l'accesso remoto. Per proteggere questi sistemi periferici, gli operatori dei sistemi di distribuzione e trasmissione spesso ricorrono esclusivamente ai firewall, che rilevano in modo affidabile il malware noto. Tuttavia, **i firewall non riconoscono i modelli di attacco nuovi e gli attacchi di professionisti** che spesso vengono eseguiti per mesi o anni. Con diverse centinaia di migliaia di nuove varianti di malware

ogni giorno, la sicurezza informatica si limita a identificare le firme note e diventa altamente inaffidabile. **Il procedimento di protezione in ambito di Operational Technology (OT) e dei sistemi di controllo industriale (ICS) è limitato.** Il personale in loco non è quasi mai formato e autorizzato a occuparsi di ICS. La comunicazione all'interno degli impianti spesso non è nota ai centri operativi della sicurezza. Comunicazioni errate o danneggiate nelle sottostazioni e in altri sistemi elettrici controllati da remoto non vengono rilevate finché non producano un impatto sulla fornitura elettrica. **Questo aiuta gli hacker** a penetrare nelle reti OT e nella infrastruttura, causando danni e interruzioni del servizio.

<sup>1</sup> Ufficio federale per la sicurezza IT (BSI)



«L'audit ci ha offerto un quadro più chiaro di tutti i processi nel nostro complesso sistema di controllo industriale. Questo ci ha permesso di analizzare approfonditamente tutto il traffico nell'ambito delle comunicazioni e controllare specificamente gli IACS per capirne le vulnerabilità. Siamo rimasti stupiti dalla fluidità del processo. Lo sviluppo diretto di misure efficaci ci ha preparato perfettamente ai rischi futuri di sicurezza informatica.»

Falk Fischer | Team Leader dei sistemi e delle applicazioni IT | Leipziger Wasserwerke

## Sicurezza informatica OT end-to-end per infrastrutture critiche

Rhebo supporta le aziende del settore energetico e idrico nell'**intero ciclo di vita della creazione e del mantenimento di un'effettiva e completa sicurezza informatica OT.** Con Rhebo OT Security, le infrastrutture critiche possono avvalersi della solida esperienza di Rhebo, dall'analisi del rischio OT iniziale all'integrazione di un sistema di rilevamento delle anomalie e delle intrusioni OT e (facoltativamente) la continua gestione del sistema di sicurezza. **Rhebo Next Generation OT Intrusion Detection System combina il monitoraggio OT passivo con il rilevamento delle anomalie non invasivo.** Si tratta di una soluzione di sicurezza informatica OT che copre tutta l'infrastruttura critica, dalle postazioni di controllo agli impianti elettrici centrali fino alle sottostazioni e alle risorse di energia rinnovabile, per consentire un **monitoraggio end-to-end dell'infrastruttura distribuita.** Gli attacchi informatici, le manipolazioni, le scansioni e gli errori tecnici che si verificano nelle strutture vengono rilevati e segnalati in tempo reale in base alle variazioni delle comunicazioni associate.

Rhebo OT Security supporta tutte le piattaforme comuni e **può essere integrata in modo conveniente** in qualsiasi rete automatizzata industriale tramite:

- **hardware industriale dedicato** per le configurazioni fisiche;
- **appliance virtuali** per la gestione in ambienti VMware, Hyper-V e altri ambienti virtuali;
- **sensori basati su software** per gateway di sicurezza comuni, dispositivi di edge computing e server delle sottostazioni come quelli di Barracuda, Cisco, INSYS icom Smart Devices, RAD, Siemens RUGGEDCOM, Wago e Welotec.

La soluzione **supporta completamente specifici protocolli di sottostazioni** come OPC, IEC 60870-5-104, IEC 61850-8-1, DNP3 e altri. Con Rhebo OT Security, **la resilienza e il rafforzamento dei sistemi sono migliorati** poiché le minacce possano essere mitigate velocemente ed è possibile impedire agli attacchi di diffondersi in altri siti o nei sistemi centrali.

# Rhebo OT Security Made Simple



## SOLIDA ESPERIENZA

nelle soluzioni di sicurezza industriali per il settore energetico e idrico



## SOLUZIONE DEDICATA E SEMPLICE

per un'implementazione efficiente in termini di costi della sicurezza informatica IIoT, AMI e OT.



## SERVIZI GESTITI

con supporto completo per aumentare la resilienza industriale effettiva



## SICUREZZA RISPETTO ALLE VULNERABILITÀ

attraverso l'analisi del rischio informatico dell'OT e la valutazione della maturità della sicurezza.



## SICUREZZA CONTRO ATTACCHI CONOSCIUTI E NUOVI

attraverso il continuo monitoraggio OT, il rilevamento degli asset e delle anomalie.



## SICUREZZA END-TO-END

attraverso il rilevamento delle anomalie per prevenire la propagazione delle minacce tra OT, IIoT e infrastruttura avanzata di misurazione (AMI).



»Con Rhebo, possiamo difendere e centralizzare la nostra fornitura di energia, le utenze municipali e più di 16.000 produttori di energia decentralizzata per i quali operiamo. La nuova trasparenza e il monitoraggio continuo aumentano visibilmente la qualità della nostra rete.«

Dipl.-Ing Daniel Beyer | Manager dell'ingegneria dei sistemi e responsabile della sicurezza delle informazioni | Thüringer Energienetze GmbH & Co. KG



## SICUREZZA DELL'OT SEMPLIFICATA

attraverso l'analisi dettagliata e visualizzazione intelligente degli eventi.



## SICUREZZA ATTIVA

con il supporto degli esperti Rhebo per l'analisi del rischio, delle operazioni e dell'analisi forense.



## SICUREZZA DEI SISTEMI

attraverso l'integrazione flessibile e conveniente delle soluzioni Rhebo su dispositivi IIoT e componenti di rete.



## SICUREZZA CONTRO UN TCO IMPREVEDIBILE

attraverso semplici schemi di licenze e facili installazioni a impatto ridotto.



## RISPETTO DELLA CONFORMITÀ

tutte le leggi nazionali e internazionali di sicurezza attraverso il monitoraggio e le soluzioni IDS.



## SICUREZZA AFFIDABILE MADE IN GERMANY

conforme alla European Cyber Security Organisation (ECSO) e al GDPR.

# Semplicità ed efficacia

## tre passaggi verso la sicurezza dell'OT

1



Il primo semplice passo verso la sicurezza dell'OT

### La sicurezza informatica inizia con la visibilità.

L'analisi del rischio informatico OT e la valutazione del livello di sicurezza fornite da Rhebo offrono una comprensione approfondita degli asset ICS/TO e dell'esposizione al rischio, nonché consigli sulle misure efficaci per rafforzare i sistemi.

#### Benefici

- identificazione di tutti i dispositivi e i sistemi all'interno dell'OT tra cui le proprietà, le versioni del firmware, i protocolli, le connessioni e il comportamento delle comunicazioni (rilevamento e inventario degli asset);
- analisi approfondita delle vulnerabilità esistenti documentate CVE;
- identificazione dell'esposizione al rischio, delle lacune nella sicurezza e degli errori tecnici;
- report di audit dettagliato e workshop con consigli utili.

2



La semplice transizione al monitoraggio continuo e al rilevamento delle minacce

### La sicurezza informatica non si ferma al perimetro della rete.

Il monitoraggio dell'OT Rhebo con rilevamento delle intrusioni e delle minacce OT di nuova generazione offre sicurezza dedicata per OT di livello enterprise. Aumenta la sicurezza del firewall perimetrale esistente integrando un rilevamento olistico delle anomalie che non interferisce con i processi industriali critici.

#### Benefici

- visibilità in tempo reale sul comportamento delle comunicazioni di tutti gli asset dell'ICS e dell'OT (protocolli, connessioni e frequenze);
- creazione di report in tempo reale e localizzazione di eventi (anomalie che indicano attacchi informatici, manipolazioni o errori tecnici);
- Rilevamento tempestivo di attacchi tramite Backdoors, e di punti vulnerabili e di minacce interne finora sconosciuti che sfuggono ai Firewalls (Defense-in-Depth).

3



Il segreto per la tranquillità: siamo noi a occuparci del monitoraggio

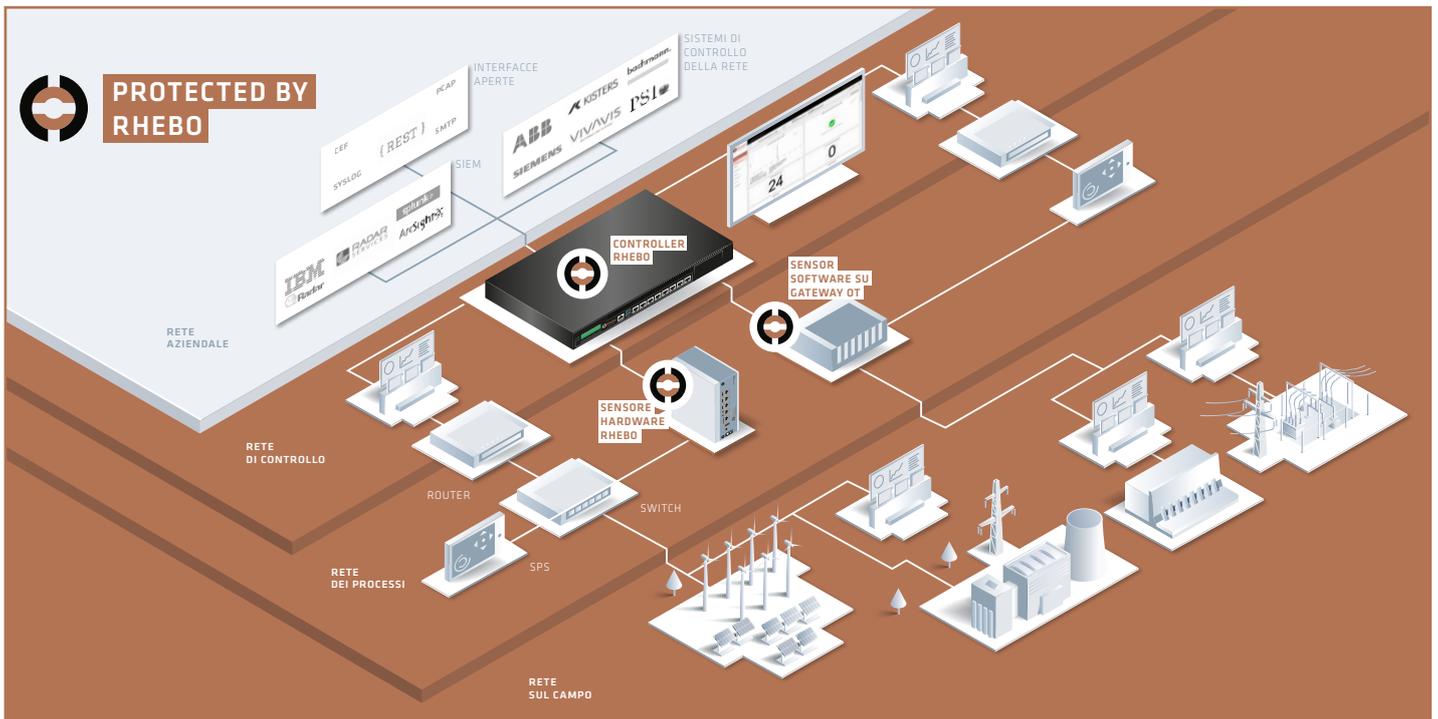
### La sicurezza informatica necessita di risorse e know-how.

Rhebo supporta la gestione del monitoraggio della sicurezza OT con il rilevamento delle anomalie, in particolare valutando e affrontando gli incidenti, nonché esaminando e migliorando continuamente i meccanismi di mitigazione.

#### Benefici

- supporto da parte di esperti per la gestione del sistema di monitoraggio della sicurezza OT;
- rapide analisi forensi e valutazione delle anomalie dell'OT;
- capacità di agire rapidamente in caso di incidenti;
- Regolare analisi OT dei rischi e delle vulnerabilità per garantire un miglioramento continuo

# Rhebo Sicurezza OT dedicata e semplice



## Formazione significa conoscenza Protocolli rilevati e analizzati con Rhebo OT Security\*

ABB Redundant Network Routing Protocol	ESET Remote Administrator	Internet Printing Protocol	MRP	Remote Desktop Protocol	Stream Control Transmission Protocol
Acronis Backup	EtherCAT	Internet Small Computer Systems Interface	Munin Data Exchange Protocol	Rhebo	Symantec Endpoint Protection Manager
Adobe Server	FTP Control	Inter-Switch Message Protocol	MySQL Client-Server Protocol	RK 512	Syslog
ARP	FTP Data	IPsec Authentication Header	Nagios	Routing Information Protocol	TCP Keep-Alive
AXIS Camera-Management	General Electric	IPsec Encapsulating Security Payload	NetBIOS	S7/S7+	TDS
BACnet	General Inter-ORB Protocol	IPv6	NFS	SentinelSRM	Telnet
Boot Service Discovery Protocol	GigE Vision Control Protocol	Java Remote Method Invocation	NTP	Sercos III	TFTP
Canon BJNP	GigE Vision Streaming Protocol	Kerberos	Omicron OMFind	Siemens Spectrum Power TG	Tivoli Storage Manager
CIP	Haag Damon	Landis+Gyr Outside Data Exchange Protocol	ONVIF Simple Object Access Protocol	Siemens SICAM PAS/PQS	TNS
Cisco	HART	Line Printer Daemon Protocol (LPD)	OPC-UA	Simple Object Access Protocol	Undo License Manager
Cisco CDP	HP	Link Aggregation Control Protocol	OpenProtocol	Sinec H1	Veritas Backup Exec Client
Cisco CGMP	HP DTC	Link Aggregation Marker Protocol	Operation, Administration, Maintenance	SKINNY	VMWare-Lab-Manager
Cisco DCE	HP Extended LLC	LDAP	OSPF	Slow Protocol	VMware Server Console
Cisco DTP	HP PROBE	LLC	PIM	SMA	VNC
Cisco EIGRP	HSR	LLDP	Powerlink	SMB	VRPP
Cisco WLCCP	HSRP	LLMNR	Proficy iFix	SMTP	Web-Based Enterprise Management
Codesys	HTTP/S	LonTalk	Profinet	SNMP	Web Services Discovery
COTP	iba Device Configuration Protocol	McAfee ePO	Profinet-IO CM	SqlNet2	WinCC
DCE/RPC	ICMP	mDNS	PSI	SQL Server Resolution Protocol	X11
DECnet	IEC60870-5-104	Modbus	PTP	STP	.NET TCP Binary Protocol
DHCP	IEC61850-GOOSE	MQTT	QXNet		
DLMS/Cosem **	IEC61850-GSSE		QUIC		
DNP3	IEC61850-MMS		Realtek Remote Control Protocol		
DNS	IEC61850-SMV		Real Time Streaming Protocol		
EAP over LA	IGMP				
ECTP	Intel Advanced-Network-Services				
EGP					
ELCOM-90					

Protocolli evidenziati:  
protocolli specifici del settore

\* aggiornato a giugno 2022  
\*\* disponibile a gennaio 2023



## Prenoti una valutazione personalizzata della sicurezza di rete OT o una demo

[www.rhebo.com](http://www.rhebo.com) | [sales@rhebo.com](mailto:sales@rhebo.com) | +49 341 3937900

### Scopra altre soluzioni Rhebo

➤ Rhebo AMI Security

➤ Rhebo IIoT Security

### Protette da By Rhebo

Stromnetz  
Hamburg

Leipziger  
Wasserwerke

Thüringer  
Energienetze

Landis  
+Gyr

BayWa re.

MITNETZ  
STROM

### Sicurezza OT Made In Germany

TeleTrust  
Pioneers in IT security.

CYBERSECURITY  
MADE IN EUROPE

Allianz für  
Cyber-Sicherheit

PLATTFORM  
INDUSTRIE4.0

SecurITy

Initiated by ECSO. Issued by eurobits e.V.

Trust Seal  
[www.teletrust.de/itsmig](http://www.teletrust.de/itsmig)

made  
in  
Germany

#### 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 di fornitori di energia, per le infrastrutture critiche e per le aziende industriali. L'impresa 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 5.000 dipendenti in più di 30 paesi. Rhebo è partner dell'Alleanza per Cibersicurezza dell'Ufficio Federale Tedesco per la Sicurezza Informatica (BSI) e della TeleTrust - Associazione Federale Tedesca della sicurezza IT. Come impresa affidabile IT, Rhebo è portatore ufficiale dei sigilli di qualità »IT Security Made in Germany« e »Cybersecurity Made in Europe«.

[www.rhebo.com](http://www.rhebo.com)