



Rhebo OT Security

Detección y monitorización eficaz de amenazas ICT para instalaciones de suministro eléctrico



VISIBILIDAD OT EN TIEMPO REAL

a través del descubrimiento de activos y a la monitorización de las comunicaciones ICS.



DETECCIÓN TEMPRANA DE INTRUSOS

a través de la detección de anomalías OT para la mitigación rápida de amenazas.



SERVICIOS DE SEGURIDAD OT

desde el análisis de riesgos en infraestructuras hasta la monitorización continua de OT y el análisis forense.



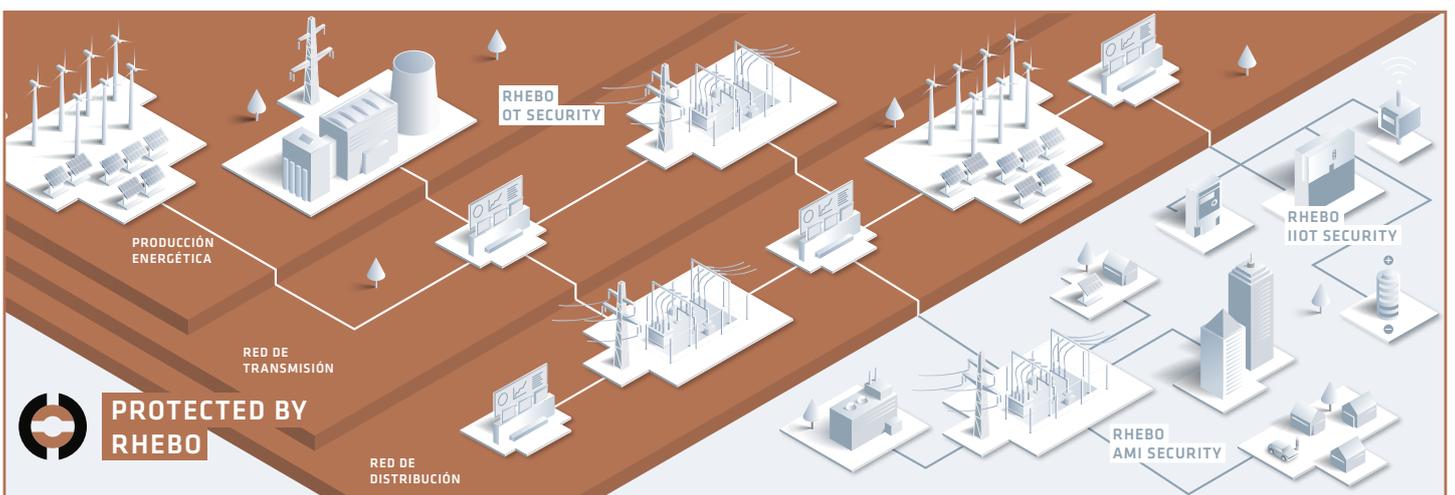
»Con Rhebo, podemos garantizar que nuestro Sistema de Control y Automatización Industrial (IACS) sea estable y seguro. Rhebo nos proporciona una mayor visibilidad en nuestro IACS para identificar y mitigar rápidamente los nuevos ataques y los errores de configuración que eran invisibles para nosotros en el pasado.«

Dipl.-Ing (TU) Sven Hanemann | Director de Seguridad de IT | e-netz Südhessen AG

Rhebo ofrece una solución de ciberseguridad y detección de intrusos sencilla y eficaz »Made in Germany« para la tecnología operativa (OT) y los activos industriales distribuidos para el sector energético las infraestructuras críticas y las empresas industriales. La solución monitoriza permanentemente las comunicaciones ICS y OT para

comprobar si hay amenazas y ataques. Cualquier anomalía en las comunicaciones se detecta, evalúa y notifica en tiempo real. Rhebo ofrece un ciclo completo de ciberseguridad a las empresas del sector energético, desde el análisis inicial de riesgos y vulnerabilidades hasta la monitorización continua de la OT.

Rhebo AMI Security sencillez y especialización



Nuevos desafíos en los sistemas complejos de suministro energético

La red eléctrica está cada vez más fragmentada, debido a la integración de los servicios municipales, las nuevas subestaciones y los recursos energéticos renovables. Las estaciones suelen estar alejadas de la sala de control central. Por lo tanto, cada vez es más común que el control se lleve a cabo de forma digital y mediante acceso remoto. Para proteger estos sistemas periféricos, los operadores de sistemas de distribución y transmisión suelen confiar únicamente en cortafuegos, que pueden detectar malwares de un modo fiable. Sin embargo, los cortafuegos no detectan los nuevos patrones de ataque ni los ataques profesionales que a menudo se prolongan durante meses o años. Con cientos de miles de nuevas variantes de malware¹ que se generan cada día, la seguridad informática se limita a identi-

ficar únicamente firmas conocidas y se vuelve muy poco fiable. Hay muy pocos mecanismos de protección para la tecnología operacional (OT) y los sistemas de control industrial (ICS). Normalmente, los trabajadores de las instalaciones no tienen ni la formación ni la autorización necesarias para gestionar los ICS. Los centros de operaciones de seguridad desconocen a menudo la comunicación dentro de las instalaciones. Las comunicaciones incorrectas o corruptas dentro de las subestaciones y de otros sistemas de energía controlados de forma remota solo se pueden detectar cuando ya han dañado el sistema energético. Esto ayuda a los ciberdelincuentes a penetrar en las redes e infraestructuras OT, generando daños e interrupciones.

¹ Federal Office For IT Security (BSI)



«La auditoría nos ha proporcionado una imagen más clara de todos los procesos de nuestro sistema de control industrial, lo que nos ha permitido analizar exhaustivamente todo el tráfico de comunicaciones y comprobar el ICS en busca de vulnerabilidades. Quedamos impresionados por la fluidez del proceso. El desarrollo directo de medidas eficaces nos preparó para futuros riesgos de ciberseguridad.»

Falk Fischer | Jefe de equipo de Sistemas y Aplicaciones de TI | Leipziger Wasserwerke (Aguas de Leipzig)

Ciberseguridad OT integral para infraestructuras esenciales

Rhebo protege a las empresas de energía y agua durante **el ciclo completo de ciberseguridad OT, es decir, desde su establecimiento hasta su mantenimiento**. Con Rhebo OT Security, las infraestructuras críticas pueden beneficiarse de la sólida experiencia de Rhebo, desde el análisis inicial de riesgos de OT hasta la integración de un sistema de detección de intrusiones y anomalías OT. Además, Rhebo puede gestionar el funcionamiento continuo del sistema de seguridad. **El sistema de detección de intrusiones OT de última generación de Rhebo combina la monitorización pasiva de OT con la detección no intrusiva de anomalías**. Se trata de una solución de ciberseguridad OT que abarca toda la infraestructura crítica, desde la sala de control y las centrales eléctricas, pasando por las subestaciones y recursos de energía renovable; esto permite ofrecer una **monitorización fiable en toda la infraestructura distribuida**. Todos los ciberataques, manipulaciones, rastros y errores técnicos que se producen en las instalaciones se detectan y se notifican en tiempo real según los correspondientes cambios en las comunicaciones.

Rhebo OT Security es compatible con las plataformas habituales y más conocidas, por lo tanto, permite la integración de forma sencilla, simple y rentable en cualquier red automatizada industrial con los siguientes métodos:

- Hardware industrial **específico** para configuraciones físicas.
- Dispositivos **virtuales** para el funcionamiento en VMware, Hyper-V y otros entornos virtuales.
- Sensores **de software** para las soluciones más comunes en los gateway de seguridad, dispositivos de borde y servidores de subestaciones; como los de Barracuda, Cisco, INSYS icom Smart Devices, RAD, Siemens RUGGEDCOM, Wago y Welotec.

Es importante destacar que la solución **es totalmente compatible con protocolos de subestación específicos**, como OPC, IEC 60870-5-104, IEC 61850-8-1, DNP3, etc. Con Rhebo OT Security, **se mejora la resistencia y la solidez del sistema**, ya que es posible mitigar las amenazas rápidamente y evitar que los ataques se propaguen a otros sitios o a los sistemas centrales.

Rhebo OT Security Made Simple



SÓLIDA TRAYECTORIA

en soluciones de seguridad industrial para el sector de la energía y el agua.



SOLUCIÓN ESPECIALIZADA

y sencilla para implantar de un modo rentable la ciberseguridad OT, AMI y IIoT.



SERVICIOS ADMINISTRADOS

para un apoyo total y así acelerar de manera eficaz la resiliencia industrial.



SEGURIDAD FRENTE A LAS VULNERABILIDADES

a través del análisis de riesgos cibernéticos OT y las evaluaciones de madurez.



SEGURIDAD CONTRA ATAQUES NUEVOS Y CONOCIDOS

a través de la monitorización OT permanente, el descubrimiento de activos y la detección de anomalías.



SEGURIDAD INTEGRAL

mediante la detección de anomalías para evitar la propagación de amenazas en la OT, IIoT y las infraestructuras de medición avanzada (AMI).



»Con Rhebo, podemos garantizar y centralizar nuestro suministro de energía, así como el servicio público municipal y a los más de 16.000 productores de energía para los que proveemos. La supervisión y el seguimiento continuo aumentan la calidad de nuestra red«.

Dipl.-Ing Daniel Beyer | Director de Ingeniería de Sistemas y de Seguridad de la Información | Thüringer Energienetze GmbH & Co. KG



SEGURIDAD OT SENCILLA

mediante el análisis detallado de OT y la visualización inteligente de eventos.



MEDIDAS DE PROTECCIÓN

a través del apoyo experto de Rhebo en el análisis de riesgos, las operaciones y el análisis forense.



SEGURIDAD DE LOS SISTEMAS

a través de una integración flexible y rentable de las soluciones Rhebo en los dispositivos IIoT y en los componentes de la red.



SEGURIDAD FRENTE AL IMPREVISTO TCO

a través de licencia simple y una instalación fácil y de bajo impacto.



CUMPLIMIENTO DE LA NORMATIVA Y LEYES DE SEGURIDAD NACIONALES E INTERNACIONALES

mediante soluciones de monitorización y IDS.



SEGURIDAD FIABLE MADE IN GERMANY

de acuerdo con la Organización Europea de Ciberseguridad (ECSO) y el RGPD.

Simple y eficaz

tres pasos para la seguridad OT

1



El primer paso para conseguir la seguridad OT

La ciberseguridad empieza por la visibilidad.

El análisis de riesgos cibernéticos y la evaluación de madurez de Rhebo OT proporcionan un conocimiento profundo de los activos ICS / OT y de la exposición al riesgo, así como asesoramiento sobre medidas eficaces para mejorar los sistemas.

Las ventajas para usted

- Identificación de todos los dispositivos y sistemas dentro de la OT, incluyendo propiedades, versiones de firmware, protocolos, conexiones (inventario y descubrimiento de activos);
- Análisis en profundidad de las vulnerabilidades CVE documentadas existentes;
- Identificación de la exposición a los riesgos, las brechas de seguridad y los errores técnicos;
- Obtención de un informe detallado y guía con recomendaciones prácticas.

2



Una transición fluida a la monitorización continua de la OT y la detección de amenazas

La ciberseguridad no termina en los límites de la red.

La monitorización de última generación de OT de Rhebo para la detección de intrusiones y amenazas de OT, ofrece una seguridad dedicada a la OT de nivel empresarial. Potencia la seguridad del cortafuegos perimetral existente, ya que integra una detección global de anomalías que no interfiere con los procesos industriales más críticos.

Las ventajas para usted

- Visibilidad en tiempo real de las comunicaciones de todos los activos ICS y OT (protocolos, conexiones, frecuencias).
- Notificación y localización en tiempo real de eventos (anomalías) que indiquen la existencia de ciberataques, manipulaciones o errores técnicos.
- Identificación y detección anticipada de ataques a través de puertas traseras, vulnerabilidades previamente desconocidas y adversarios internos que los cortafuegos no consiguen detectar (defensa en profundidad).

3



El secreto de la tranquilidad: nos encargamos de la monitorización

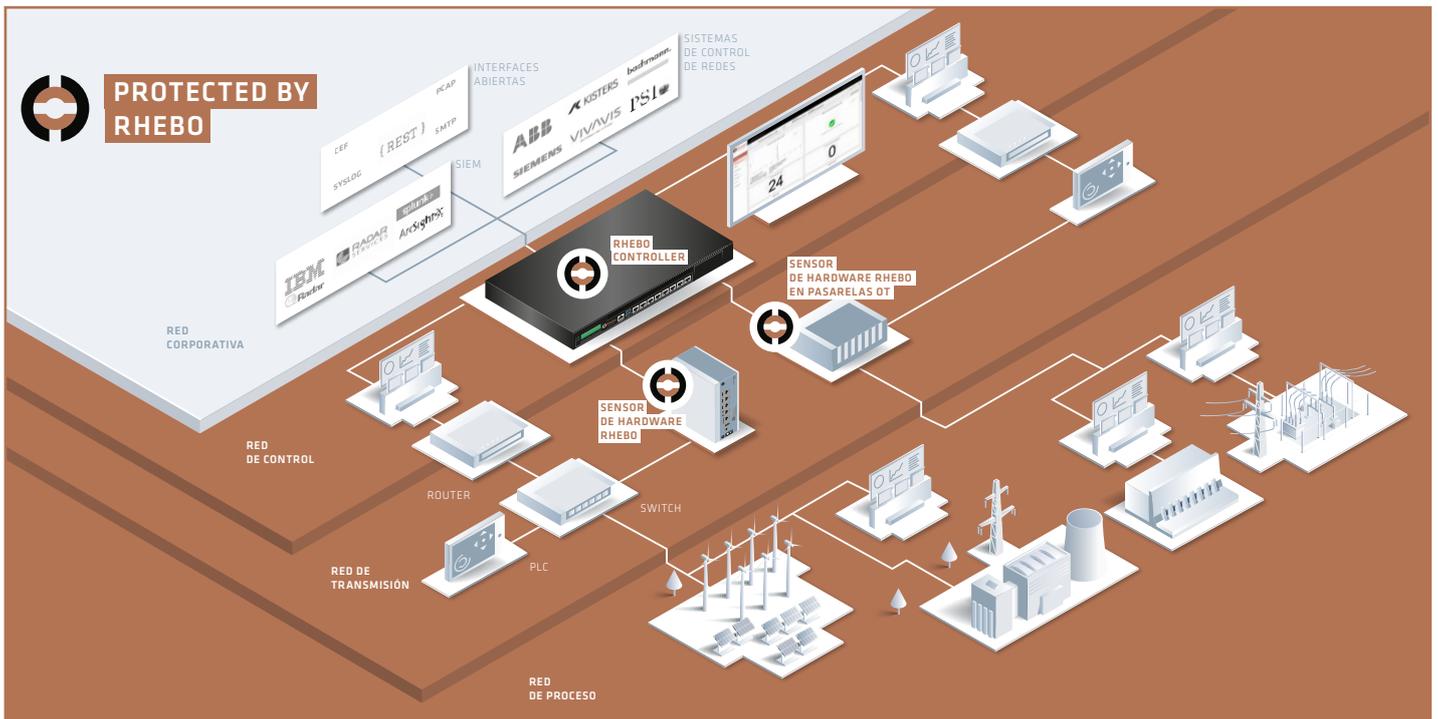
Para una ciberseguridad eficaz se requiere recursos y conocimientos técnicos.

Las ventajas para usted

- Apoyo experto para el funcionamiento del sistema de monitorización de la seguridad OT.
- Análisis forenses rápidos y evaluación de las anomalías en la OT.
- Actuación rápida en caso de incidentes.
- Análisis regulares de las ciberamenazas OT y evaluaciones de madurez para una mejora continua.

Rhebo OT Security

Sencillez y especialización



La formación significa conocimiento

Detección y análisis de protocolos con Rhebo AMI 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	Remote Shell	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	VERRP
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	QNX Qnet		
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					

Protocolos destacados:
protocolos para sectores
específicos.

*junio de 2022

** disponible en enero de 2023



Pida su evaluación personalizada de la seguridad para redes AMI o solicite una demostración

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

Explore más soluciones Rhebo

➤ [Rhebo AMI Security](#)

➤ [Rhebo IIoT Security](#)

Protegido por Rhebo



OT Security Made In Germany



Rhebo OT Security Made Simple

Rhebo ofrece soluciones de ciberseguridad simples y eficaces para la tecnología operativa y los activos industriales distribuidos para el sector energético, infraestructuras críticas y empresas industriales. Rhebo protege a las empresas con la seguridad OT desde el análisis inicial de riesgos y vulnerabilidades hasta la monitorización continua de OT contra la detección de intrusiones y anomalías. Desde 2021, Rhebo forma parte de Landis+Gyr, líder mundial de soluciones integradas de gestión de la energía para la in-

dustría energética, que actualmente cuenta con un total de 5.000 empleados en más de 30 países en todo el mundo. Rhebo también es miembro de la Alianza para la Ciberseguridad de la Oficina Federal de Seguridad de la Información (BSI) y de Teletrust -IT Asociación de Seguridad Informática de Alemania. Además, ha recibido los sellos »IT Security Made in Germany« y »Cybersecurity Made In Europe« por sus estrictas políticas de protección y seguridad de datos..

www.rhebo.com