Rhebo
a Landis+Gyr company

SUCCESS STORY

Angriffserkennung auf Energiespeichersystemen von Sonnen

sonnen

ANGRIFFSERKENNUNGS-SYSTEM FÜR ÜBER 50.000 PRIVATE UND KOMMERZIELLE ENERGIESPEICHER

SICHERHEITS-AUTOMATISIERUNG FÜR VERNETZTE ENERGIEANLAGEN

KOSTENEFFIZIENTES SICHERHEITSMANAGEMENT FÜR WELTWEIT VERTEILTE ANLAGEN

»Uns war bei der Auswahl der Lösung besonders wichtig, dass Monitoring und Sicherheitsautomatisierung konkret auf unsere Geräte zugeschnitten werden und jederzeit erweitert werden können. Denn sowohl unsere Technologie als auch die Gefährdungslage entwickeln sich ständig weiter.«

Daniel Ackermann, Director Software Development Sonnen

Ausgangssituation und Herausforderung

Als einer der führenden Anbieter moderner Energiespeicher und erneuerbarer Energielösungen steht für die Sonnen GmbH die Cybersicherheit ihrer Produkte im Mittelpunkt. Die Herausforderung dabei ist, dass die privat und kommerziell genutzten Energiespeicher meist im lokalen Heimnetz der Endkunden eingebunden sind. Diese Netze sind für Angreifer leicht zugänglich und besitzen kein dediziertes Alarmsystem für Angriffe auf die industriellen Prozesse der Energiespeicher. Nicht nur können gezielte Angriffe auf den weltweit verteilten Speichern dazu führen, dass Einzelanlagen beschädigt werden. In einem System identischer vernetzter Geräte steigt auch das Risiko signifkant, dass die Flotte übernommen und z. B. als Botnet missbraucht oder orchestriert abgeschaltet wird. Die weltweit installierten Energiespeichersystemen von Sonnen sollten deshalb mit einem industriellen Angriffserkennungssystem ausgerüstet werden, das Cyberangriffe und Störungen bereits auf dem Edge Device erkennt und abwehrt. Ziel war es, Angriffe zu blockieren und zu isolieren, bevor sie auf die zentrale Plattform oder andere Speicher übergreifen können.

Detection & Response für weltweit verteilte Energiespeicher

Unbekannte und bekannte Angriffsmuster erkennen, dokumentieren und über automatisierte Sicherheits-Policies abwehren.

Durchgängige Flottenabsicherung

Anomalien in Echtzeit an Security Operation Center (SOC) melden für weltweite Maßnahmen-umsetzung.

Globale Threat Intelligence

Anomalien über alle Energieanlagen zentral analysieren für vorausschauende Risikoerkennung und Wartung..

Lösung

ENDPOINT DETECTION & RESPONSE

für die weltweit verteilten Energiespeicher

- überwacht kontinuierlich Verhalten der Energiespeicher;
- identifiziert, analysiert und meldet Cyberangriffe, Schadprogramme und Fehlerzustände in Echtzeit;
- erlaubt via Security Policies automatische Reaktion auf kritische Ereignisse zum Schutz der Geräteflotte.

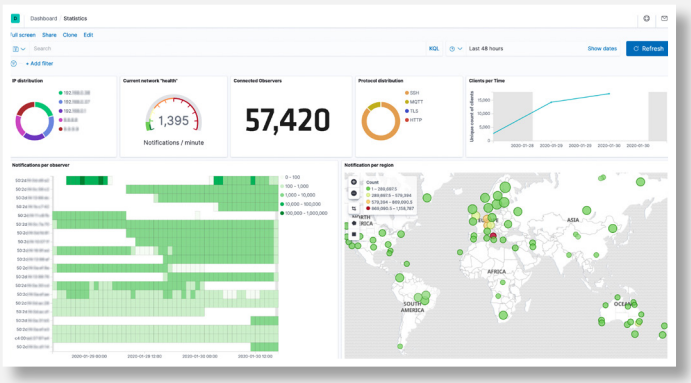
SOFTWAREBASIERTE SICHERHEITSLÖSUNGEN

für IIoT-Systeme und -Anlagen

- erlaubt schnelle Portierbarkeit auf Steuerungen der weltweit verteilten Energieanlagen;
- ermöglicht globales und kosteneffektives Sicherheits-Upgrade;
- bietet Standardschnittstellen zu gängigen Analysetools wie Elastic Stack, Splunk und QRadar.

Integration und Umsetzung

Sonnen integriert seit Anfang 2020 auf allen bestehenden und neu installierten Energiespeichern die weiterentwickelte Rhebo-Technologie zur aktiven Absicherung. Das Rollout erfolgt softwarebasiert auf den lokalen Steuerungen der verteilten Energiespeicher. Neben der Verhaltensanalyse des Energiespeichers werden auch lokale Schnittstellen wie Webinterfaces sowie die Systemprotokolle kontinuierlich überwacht. Für ein kosteneffizientes Upgrade der Bestandsanlagen sowie die Sicherstellung eines schnellen Return-on-Investment werden Standardschnittstellen (z.B. Syslog, MQTT) und Open-Source-Technologien verwendet. Diese erlauben auch die reibungslose Übermittlung von Anomaliedaten und Security Policies zwischen den verteilten Anlagen und dem zentralen SOC bei Sonnen. Rhebo betreut Sonnen zudem aktiv bei der Analyse und Bewertung auftretender Anomalien.



Übersichts-Dashboard des Rhebo IIoT-Sicherheitsmonitorings

Übersicht der weltweiten Anomaliemeldungen mit Detailansicht

Ergebnisse

ABWEHR BEKANNTER UND UNBEKANNTEN CYBERGEFAHREN durch gerätespezifische Verhaltensanalyse und Anomalieerkennung.

SCHNELLE BEHEBUNG VON SOFTWAREFEHLERN durch Früherkennung von Fehlerzuständen und einfache Ursachenanalyse.

COMPLIANCE UND STATE-OF-THE-ART-SICHERHEIT durch Einhaltung relevanter Standards wie IEC 62443 und BDEW-Whitepaper.

GLOBALER FLOTTENSCHUTZ durch automatisierte Security Policies auf den lokalen Energiespeichern.

ZENTRALES THREAT INTELLIGENCE UND RESPONSE MANAGEMENT durch globale Übersicht aller Anomalien.

KOSTENEFFIZIENTES SICHERHEITSDESIGN durch Standardschnittstellen und geringen CPU-Bedarf.

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 | Deutschland
Rhebo.com

SUCCESS STORY SONNEN GMBH V03-02-2025 © Rhebo GmbH
Alle Angaben ohne Gewähr. Änderungen vorbehalten. Fotos: Rhebo, Sonnen