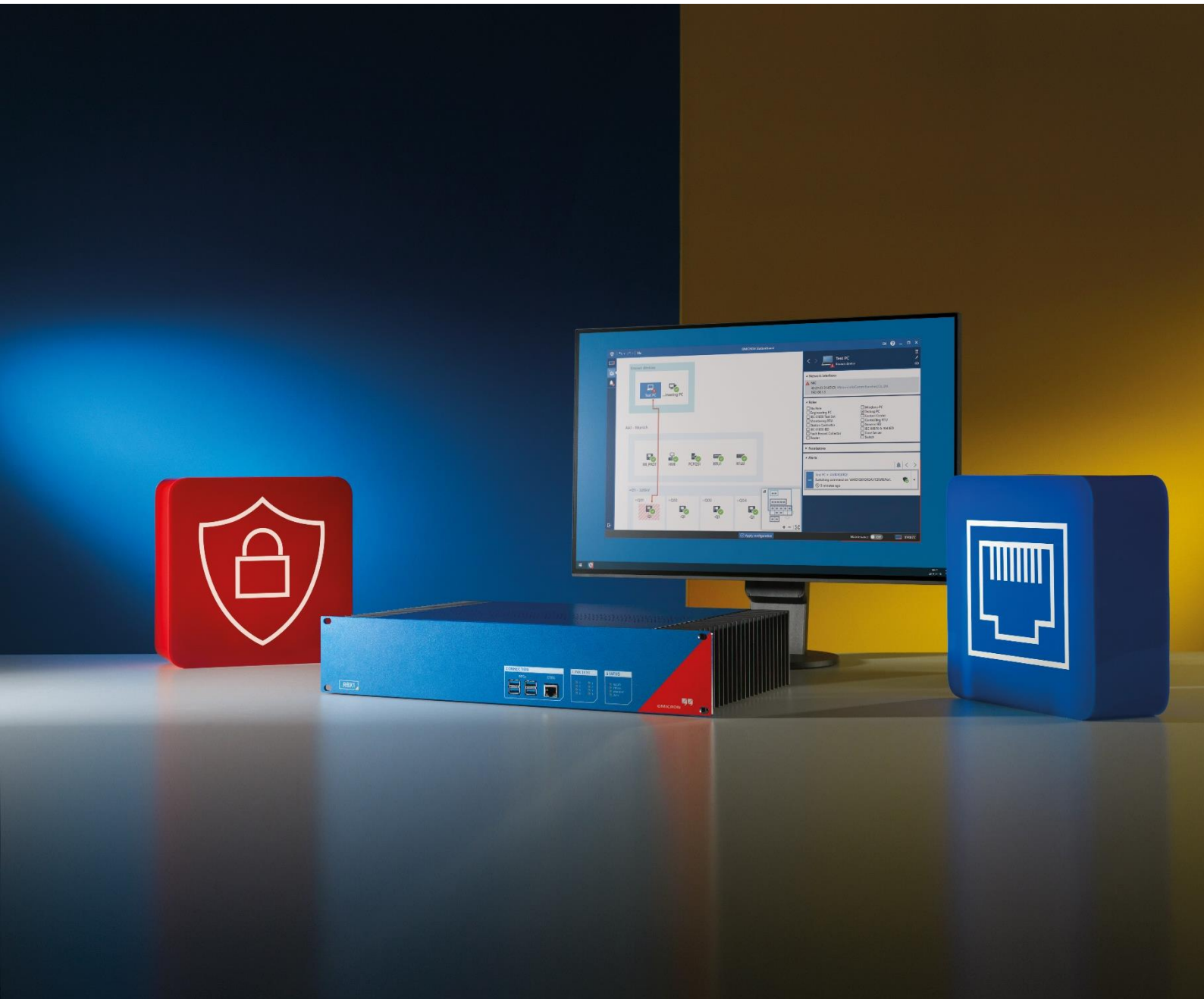
StationGuard und FortiSIEM

Integrationsanleitung



Inhalt

1 Allgemeine Informationen

1.1 Beschreibung

Dieses Dokument beschreibt den Konfigurationsprozess für den automatischen Import von OMICRON StationGuard Ereignissen in FortiSIEM über die **Inbound-Integration**. FortiSIEM empfängt alle syslogs über **TCP** und **UDP** (jeweils über die gleichen Ports).

1.2 Regeln

Der StationGuard stellt spezielle **Regeln** zur Verfügung. Regelmäßige Updates werden die Anzahl dieser Regeln erhöhen.
Zusätzlich können eigene bzw. allgemeine Regeln, welche sich auf **Ereignistypgruppen** beziehen, die auch von StationGuard Eventtypen verwendet werden, Reaktionen auslösen. Beispiele hierfür sind erfolgreiche oder nicht erfolgreiche Brute-Force Angriffe auf die Authentifizierung. Diese Regeln werden durch StationGuard-Ereignisse ebenfalls getriggert.

1.3 Reports

StationGuard gibt keine spezifischen automatischen **Reports** aus. Derlei Reports können jedoch Ergebnisse liefern, wenn sie mit den **Ereignistypgruppen** übereinstimmen, die mit StationGuard-Ereignissen verbunden sind.

2 Schritt-für-Schritt-Anleitung

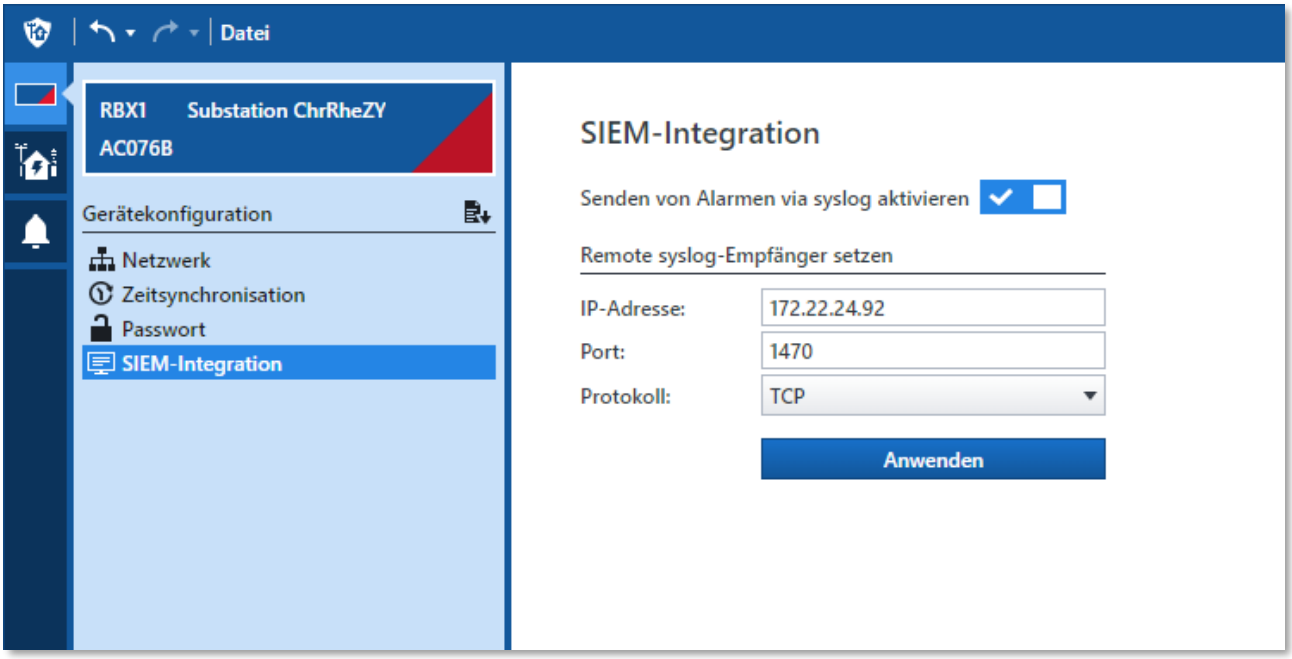
2.1 Konfiguration FortiSIEM

Ob eine Konfiguration in FortiSIEM notwendig ist, hängt von der installierten FortiSIEM-Version ab:

- Für Version 6.00 und höher benötigen Sie keine zusätzlichen Schritte (Fabric-Ready).
- Falls Sie Version 5.00 oder niedriger besitzen, emailen Sie uns bitte unter puc.support@omicronenergy.com. Von uns erhalten Sie alle relevanten Imports.

2.2 Integration StationGuard in FortiSIEM

1. Öffnen Sie Ihre *Gerätekonfiguration* in der oberen linken Ecke.
2. Klicken Sie auf den Reiter *SIEM-Integration*.
3. Schalten Sie den Schalter *Senden von Alarmen via syslog aktivieren* auf ein.
4. Geben Sie Ihre IP-Adresse und Portnummer sowie Ihren Protokolltyp ein.
   - **4a.** Wenn Sie TCP verwenden, setzen Sie die Portnummer auf 1470.
   - **4b** Wenn Sie UDP verwenden, setzen Sie die Portnummer auf 514.
5. Klicken Sie auf *Anwenden*.



OMICRON arbeitet mit Leidenschaft an wegweisenden Ideen, um Energiesysteme sicherer und zuverlässiger zu machen. Mit unseren neuartigen Lösungen stellen wir uns den aktuellen und zukünftigen Herausforderungen unserer Branche. Wir zeigen vollen Einsatz bei der Unterstützung unserer Kund:innen: Wir gehen auf ihre Bedürfnisse ein, bieten ihnen hervorragenden Vor-Ort-Support und teilen unsere Expertise und unsere Erfahrungen mit ihnen.

In der OMICRON-Gruppe entwickeln wir innovative Technologien für alle Bereiche elektrischer Energiesysteme. Im Fokus stehen elektrische Prüfungen an Mittel- und Hochspannungsbetriebsmitteln, Schutz-prüfungen, Prüfungen digitaler Schaltanlagen und Cyber Security. Kund*innen in aller Welt vertrauen auf unsere einfach zu bedienenden Lösungen und schätzen deren Genauigkeit, Schnelligkeit und Qualität.

Wir sind seit 1984 in der elektrischen Energietechnik tätig und verfügen über fundierte, langjährige Erfahrung in der Branche. Rund 900 Mitarbeiter*innen an 25 Standorten unterstützen unsere Kund:innen in mehr als 160 Ländern und unser technischer Support kümmert sich 24 Stunden am Tag, 7 Tage die Woche um sie.

For more information, additional literature, and detailed contact information of our worldwide offices please visit our website.

www.omicronenergy.com