# Security Operations Center (SOC) und SIEM Integration

**StationGuard** bietet Plug-ins für Ticketing-Systeme wie ServiceNow, mit denen automatisch Arbeitstickets zur Bearbeitung von IDS-Alarmen erstellt werden können. Durch Importieren des Betriebsmittelverzeichnisses aus StationGuard werden die Tickets automatisch den Techniker:innen zugewiesen, die für das betreffende Betriebsmittel oder den Standort zuständig sind.

## Zugriffskontrolle zum Schutz von Daten und Netzwerken

Die Integration in LDAP/Active Directory kann über das zentrale Verwaltungssystem konfiguriert werden. Für die Kontrolle des Zugriffs auf die verschiedenen Funktionen zur Anzeige und Konfiguration Ihrer StationGuard-Instanzen können unterschiedliche Nutzer:innenrollen definiert werden. So lässt sich zum Beispiel festlegen, dass Änderungen der Konfiguration oder das Aktivieren des Wartungsmodus nur entsprechend befugten Nutzer:innen vorbehalten sind. Bei einem Ausfall aller Netzwerke kann über die lokale Bedienoberfläche des StationGuard-Clients auch einzeln auf die StationGuard-Sensoren zugegriffen werden.

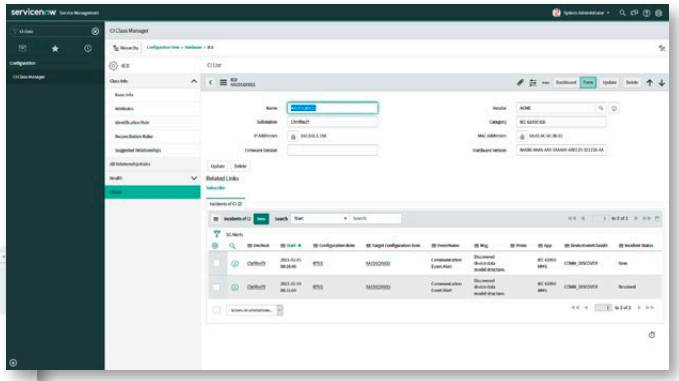
Bedrohungen von innen können mit rollenbasierter Zugriffskontrolle (Role-Base Access Control, RBAC) reduziert und sogar eliminiert werden.

Das sorgt für eine höhere Sicherheit des Systems und der Netzwerke und gleichzeitig auch für mehr Effizienz, denn Passwörter müssen weniger häufig geändert werden und es kann nicht mehr so oft zu Irrtümern bei der Zuweisung von Berechtigungen kommen.

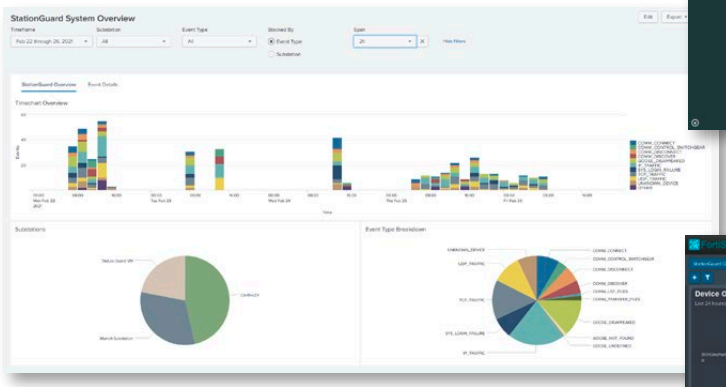
## Einfache Integration ins Netzwerk

Für das einfache Integrieren von StationGuard in ältere Systeme können die Binärausgänge der Plattform RBX1 verwendet werden. Das Vorhandensein eines unbestätigten Alarms wird an den Binärausgängen signalisiert, die mit einer RTU (Remote Terminal Unit, Fernbedienungsterminal) verdrahtet und in die Leittechnik-Signalliste integriert werden können.

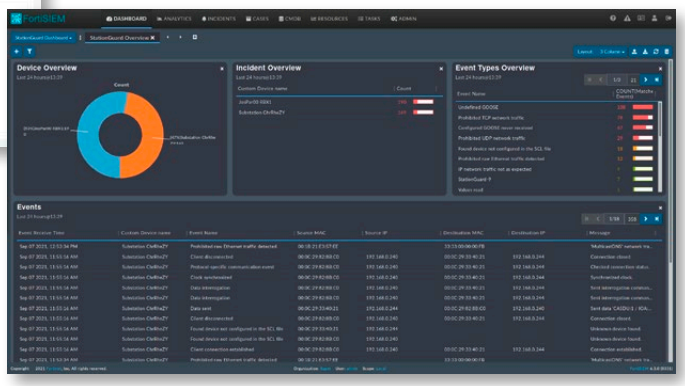
Alternativ dazu können unsere leicht verständlichen Alarmmeldungen auch über das Syslog-Protokoll weitergeleitet werden. Für die Integration von StationGuard-Sensoren in SIEM(Security Information and Event Management)- und Ticketing-Systeme verschiedener Hersteller:innen stehen mehrere Plug-ins zur Verfügung.



ServiceNow-Integration




„StationGuard for Splunk"-App




FortiSIEM-Integration