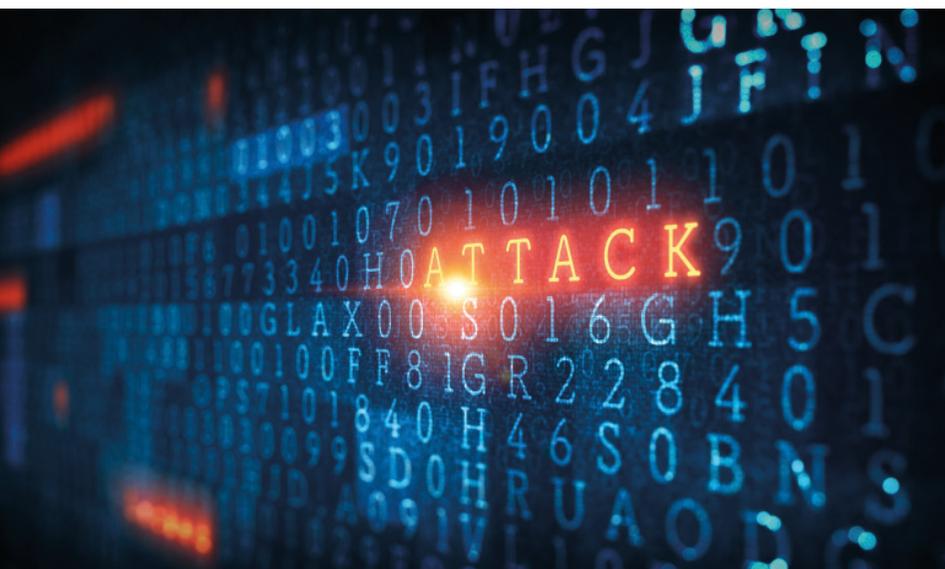


## Cyber Security Event Monitoring

Übergeordnete, kontinuierliche Überwachung und Alarmierung



Security  
Operations

ABB Ability™ Cyber Security Event Monitoring erkennt frühzeitig sicherheitsrelevante Verhaltensmuster im Automatisierungssystem und unterstützt bei der Bewertung möglicher Sicherheitsvorfälle.

### Security Information und Event Management (SIEM)

Ein SIEM-System bündelt sicherheitsrelevante Informationen und Meldungen des Automatisierungssystems. Ereignisse aus unterschiedlichen Datenquellen werden in Zusammenhang gebracht, auf verdächtige Verhaltensmuster überprüft und bewertet. Im Verdachtsfall löst das SIEM eine Alarmierung aus und leitet die Bearbeitung des Vorfalls anhand definierter Ablaufpläne oder einer detaillierten Analyse über das ABB Collaborative Operation Center (COC/SOC) ein.

### SIEM im Automatisierungssystem

Die kontinuierliche Überwachung definierter Systembereiche ist die Grundlage, Sicherheitsvorfälle umgehend zu identifizieren und bearbeiten zu können. Der ABB Event Collector stellt als zentrale Schnittstelle alle sicherheitsrelevanten Meldungen und Ereignisse aggregiert für das SIEM System bereit. In Verbindung mit den definierten Regelwerken können so potenzielle Angriffe zeitnah erkannt und analysiert werden.

### Funktionsweise

Die Überwachung umfasst eine Vielzahl von Komponenten im Automatisierungssystem. Meldungen von Hardwarekomponenten, Zugangsberechtigungen, Netzwerkkommunikation, Sicherheitsapplikationen und Betriebssystemmeldungen werden logisch miteinander verknüpft und können in Verbindung mit definierten Kontexten oder zeitlichen Abläufen, zum Beispiel dem Laden eines Controllers außerhalb der Arbeitszeit, gebracht werden.

### Unsere Leistungen

- Individuelle Beratung
- Mögliche Umsetzungsvarianten:
  - Aufbau eines SIEM vor Ort
  - Anbindung an Kunden SIEM möglich
  - Anbindung an ABB COC/SOC
  - 24/7 Überwachung durch ABB
- Implementierung definierter IT, OT und anlagen-spezifischer Regelwerke und Anwendungsfälle
- Unterstützung bei der Erfüllung geforderter Sicherheitsanforderungen
- Bereitstellung aussagekräftiger Reports
- Verbesserung und Beschleunigung der Bearbeitung möglicher Sicherheitsvorfälle
- Aktivierung des Incident Response Prozesses

---

**ABB AG**

Kallstadter Str. 1  
68309 Mannheim, Deutschland  
prozessautomatisierung  
@de.abb.com

**go.abb/prozessautomation**

---

Technische Änderungen der Produkte sowie Änderungen im Inhalt dieses Dokuments behalten wir uns jederzeit ohne Vorankündigung vor. Bei Bestellungen sind die jeweils vereinbarten Beschaffenheiten maßgebend. ABB übernimmt keinerlei Verantwortung für eventuelle Fehler oder Unvollständigkeiten in diesem Dokument.

Wir behalten uns alle Rechte an diesem Dokument und den darin enthaltenen Gegenständen und Abbildungen vor. Vervielfältigung, Bekanntgabe an Dritte oder Verwertung seines Inhaltes – auch von Teilen – ist ohne vorherige schriftliche Zustimmung durch ABB verboten.

Copyright© 2021 ABB. Alle Rechte vorbehalten.