

## Referenz - OT SOC Betrieb zur Angriffserkennung im KRITIS-Umfeld



### Kunde

Betreiber kritischer Infrastrukturen (KRITIS)

### Ausgangssituation

- Hohe Anzahl sicherheitsrelevanter Events aus IT- und OT-Systemen
- Keine durchgängige Bewertung und Priorisierung gemäß SzA-Anforderungen
- Begrenzte interne Ressourcen für kontinuierliche Analyse
- Anforderungen an Nachweisfähigkeit und Reporting

### Lösung

- Unterstützung bei Analyse und Bewertung des Sicherheitsvorfalls
- Auswertung von SIEM-, NIDS- und Systemdaten
- Identifikation von Ursache und betroffenen Systemen
- Ableitung und Abstimmung von Gegenmaßnahmen unter Berücksichtigung des Betriebs

### Projektziele

- Betrieb eines OT Security Operations Centers im 8x5 Modell
- Analyse von SIEM-, OT-NIDS- und Schwachstellendaten
- Priorisierung von Events gemäß Risikobewertung
- Regelmäßiges Reporting und Abstimmung mit dem Kunden

### Ergebnisse

- Reduktion der Event-Flut auf relevante Findings
- Strukturierte Dokumentation sicherheitsrelevanter Ereignisse
- Verbesserung der Detection-Qualität durch Use-Case-Optimierung
- Etablierte Reporting- und Abstimmungsprozesse

### Kundenvorteile

- Entlastung interner Ressourcen im KRITIS-Betrieb
- Auditierbare und nachvollziehbare Angriffserkennung
- Klare Handlungsempfehlungen statt Alarmflut
- Verbesserte Sicherheits- und Reaktionsfähigkeit

telent GmbH

Gerberstraße 34  
71522 Backnang

Telefon: +49 7191 900-0  
E-Mail: Sales@telent.de

[www.telent.de](http://www.telent.de)

**telent**  
service • commitment • value