



Systeme zur Angriffserkennung (SzA)

Angriffe erkennen. Ereignisse bewerten.
Maßnahmen ableiten. Betrieb unterstützen.

• Sicher • Vernetzt • Innovativ

telent
service • commitment • value





Praxisnaher Schutz für OT- und KRITIS-Umgebungen



Betreiber kritischer Infrastrukturen müssen sicherheitsrelevante Ereignisse frühzeitig erkennen, bewerten und nachvollziehbar dokumentieren.

Die reine Installation isolierter Systeme genügt den gesetzlichen und betrieblichen Anforderungen meist nicht.

Wirksam wird die verknüpfte Verteidigung durch die koordinierte Abstimmung von Datenquellen, Erkennungslogik, Alarmbewertung und klar definierten Betriebsprozessen.

telent unterstützt Sie beim Aufbau und Betrieb von Systemen zur Angriffserkennung. Unser Service reicht von der strukturierten Anforderungsaufnahme über die technische Integration bis zur fachlichen Bewertung durch das telent Security Operations Center (SOC).

Der telent Ansatz: Modular und prozessorientiert

Ein funktionierendes SzA bindet vorhandene IT- und OT-Infrastrukturen nahtlos ein. Es führt relevante Ereignisse zusammen, identifiziert Anomalien und übergibt qualifizierte Ergebnisse direkt in Ihre Betriebsprozesse.

Unser Vorgehen gliedert sich in vier aufeinander aufbauende Phasen:

1. Anforderungen und Scope klären
2. Angriffserkennung technisch aufbauen
3. Ereignisse fachlich bewerten
4. Betrieb und Wirksamkeit sicherstellen



Warum telent? Systemintegration trifft OT-DNA

- **Infrastruktur-DNA:** Seit Jahrzehnten planen, bauen und betreiben wir hochverfügbare Netze für Energie, Bahn, Autobahnen, Häfen und Industrie. Wir kennen die physikalischen Details dieser kritischen Umgebungen.
- **OT-Protokollkompetenz:** Wir beherrschen die Automatisierungstechnik und ihre spezifischen Protokolle wie Modbus, Profinet, IEC 60870-5-104 oder OPC UA.
- **Sicherheit aus Deutschland:** Unser zentrales SOC arbeitet an den Standorten Backnang und Saarbrücken. Wir bieten tiefe Kenntnis der Regulatorik (wie NIS-2 oder BSI-Vorgaben) und höchste Standards bei der Datenhaltung.
- **Herstellerunabhängige Integration:** Unser Technologie-Stack nutzt marktführende Lösungen wie Fortinet und Tenable. Als Integrator binden wir Ihre vorhandenen Drittsysteme nahtlos in die Prozesse ein.
- **Qualifizierte Führung:** Sie erhalten verständliche Lageberichte und konkrete Handlungsempfehlungen statt ungefilterte technische Alarmer.





PHASE 1: ANFORDERUNGEN UND SCOPE KLÄREN

Wir holen Sie dort ab, wo Sie stehen

Die strukturierte Aufnahme aller Rahmenbedingungen bildet das Fundament einer wirksamen Erkennungsstrategie. Gemeinsam legen wir fest, welche Systeme, Netzwerke und Prozesse für Ihre Konformität und Betriebssicherheit relevant sind. Neben den technischen Faktoren definieren wir von Beginn an Zuständigkeiten, Eskalationsstufen und Nachweispflichten.

Anforderungsaufnahme

- **telent Leistung:** Erfassung der regulatorischen, technischen und organisatorischen Vorgaben für Ihr Unternehmen.
- **Ihr Nutzen - Klarer Fokus.** Ein exakt definierter Betrachtungsbereich verhindert Lücken beim Audit.

Architekturreview

- **telent Leistung:** Bewertung von Netzsegmenten, IT/OT-Übergängen, Kommunikationswegen und kritischen Assets.
- **Ihr Nutzen - Ressourceneffizienz.** Vermeidung unnötiger Datenmengen und Reduzierung potenzieller Alarmfluten.

Datenquellenanalyse

- **telent Leistung:** Prüfung vorhandener Systeme (wie Firewalls, Server oder OT-Sensorik) auf verwertbare Sicherheitsereignisse.
- **Ihr Nutzen - Sichere Basis.** Eine strukturierte Grundlage für die anschließende technische Umsetzung.

Use-Case-Planung

- **telent Leistung:** Definition spezifischer Erkennungsszenarien wie unbefugte Fernzugriffe, ungewöhnliche Protokollmuster oder abweichendes Kommunikationsverhalten.
- **Ihr Nutzen - Relevante Alarme.** Zielgerichtete Use Cases reduzieren unnötige Meldungen und schaffen eine klare Grundlage für die Bewertung sicherheitsrelevanter Auffälligkeiten.

Betriebsmodell-Abstimmung

- **telent Leistung:** Festlegung der Schnittstellen zum telent SOC und Definition der verbleibenden Aufgaben im eigenen Haus.
- **Ihr Nutzen - Audit Readiness.** Transparente Nachvollziehbarkeit für das Management, die interne Revision und externe Prüfer.





PHASE 2: ANGRIFFSERKENNUNG TECHNISCH AUFBAUEN

Individuell, auf Ihre Bedürfnisse angepasst



Nach der strategischen Planung folgt die physische und logische Integration in Ihre Infrastruktur. telent implementiert die notwendigen Komponenten direkt in Ihre bestehende Umgebung. Der Fokus liegt auf einer stabilen, sicheren Implementierung, die Ihre Produktionsprozesse zu keinem Zeitpunkt beeinträchtigt. Hierbei verknüpfen wir die technische Anbindung mit klar dokumentierten Betriebsprozessen.

Zentrale Ereignisanalyse

- **telent Leistung:** Zentrale Sammlung und Korrelation von Sicherheitsereignissen aus IT-, OT- und Netzwerksystemen.
- **Ihr Nutzen - Ganzheitliches Lagebild.** Sie erhalten eine plattformübergreifende Sichtbarkeit aller relevanten Sicherheitsereignisse an einer zentralen Stelle.

Netzwerk-Anomalieerkennung & OT-Sensorik

- **telent Leistung:** Integration passiver Sensorik (OT-NIDS) zur kontinuierlichen Überwachung industrieller Kommunikationsprotokolle.
- **Ihr Nutzen - Schutz ohne Risiko.** Volle Transparenz über Assets und Kommunikationswege, ohne den laufenden Betrieb oder sensible Steuerungssysteme zu gefährden.

Datenquellen-Onboarding

- **telent Leistung:** Technische Anbindung inklusive Parsing, Normalisierung und Qualitätsprüfung aller relevanten Logdaten.
- **Ihr Nutzen - Verlässliche Datenbasis.** Saubere, strukturierte Datenströme garantieren eine präzise Erkennungsqualität und verhindern fehlerhafte Analysen.

Erkennungsregeln & Detektion

- **telent Leistung:** Implementierung spezifischer Erkennungsszenarien auf Basis von Bedrohungsmustern und bekannten Angriffsvektoren.
- **Ihr Nutzen - Früherkennung.** Gezielte Identifikation von Anomalien und echten Angriffsversuchen statt einer unkontrollierten Alarmflut.

Prozessintegration & Dokumentation

- **telent Leistung:** Einrichtung definierter Melde- und Eskalationswege zum telent SOC sowie vollständige Dokumentation der Systemarchitektur.
- **Ihr Nutzen - Betriebsbereitschaft.** Ein reibungsloser Übergang in den Echtzeit-Betrieb und eine transparente, auditfähige Dokumentation für Prüfungen.



PHASE 3: EREIGNISSE FACHLICH BEWERTEN

Relevante Alarmierung, die Ihnen Mehrwert bietet

Die reine Erzeugung von Alarmen reicht für den sicheren Betrieb kritischer Infrastrukturen nicht aus. Sicherheitsereignisse müssen präzise analysiert, priorisiert und in klare Handlungsschritte übersetzt werden. Das telent Security Operations Center (SOC) übernimmt diese kontinuierliche Filterung und Bewertung. Sie erhalten qualifizierte Lageberichte zur Relevanz und den potenziellen Auswirkungen auf Ihre Produktion statt ungefilterter technischer Meldungen.

Alarmbewertung und Triage

- **telent Leistung:** Analyse und Priorisierung eingehender Ereignisse nach Risiko, Dringlichkeit und betroffenen Systemen im industriellen Kontext.
- **Ihr Nutzen - Entlastung der Teams.** Relevante Vorfälle werden sofort identifiziert, während Fehlalarme und technisches Rauschen effektiv minimiert werden.



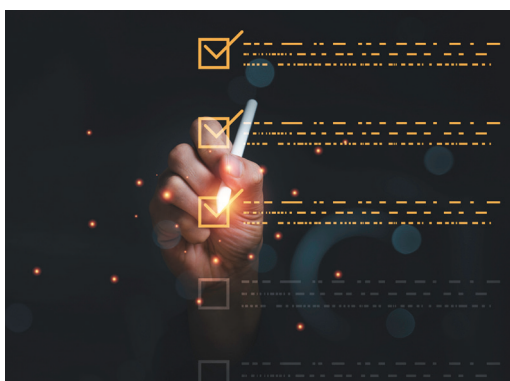
Konkrete Handlungsempfehlungen

- **telent Leistung:** Ausarbeitung klarer Empfehlungen zur Eindämmung und Behebung verifizierter Anomalien.
- **Ihr Nutzen - Schnelle Reaktionsfähigkeit.** Ihre internen Teams wissen im Ernstfall sofort, welche spezifischen Schutzmaßnahmen an den Anlagen einzuleiten sind.

Gezielte Kommunikation

- **telent Leistung:** Direkte Übergabe der bewerteten Vorfälle über vorab definierte Meldewege an Ihre zuständigen Ansprechpartner.
- **Ihr Nutzen - Verlässliche Prozesse.** Informationsverluste werden ausgeschlossen und interne Eskalationsketten greifen ohne Zeitverzug.

Regelmäßige Reviews und Optimierung



- **telent Leistung:** Gemeinsame Analyse der Alarmqualität, Feinabstimmung von Schwellenwerten und kontinuierliche Anpassung der Erkennungsregeln.
- **Ihr Nutzen - Fortlaufende Qualitätssteigerung.** Die Erkennungsgenauigkeit passt sich dynamisch an Veränderungen in Ihrer Infrastruktur sowie an neue Bedrohungslagen an.



PHASE 4: BETRIEB UND WIRKSAMKEIT SICHERSTELLEN

Stetige Verbesserung im laufenden Betrieb

Ein System zur Angriffserkennung ist kein einmaliges Projekt. Neue Systeme, veränderte Kommunikationswege, neue Bedrohungen oder angepasste Betriebsprozesse erfordern eine regelmäßige Überprüfung.

telent unterstützt Sie dabei, Ihre Angriffserkennung dauerhaft aktuell, wirksam und betriebsbereit zu halten.



Managed Security Monitoring & Operations

- **telent Leistung:** Laufende Unterstützung bei der Überwachung sowie der technischen Pflege, Updates und Optimierung des Systems.
- **Ihr Nutzen - Dauerhafte Betriebsbereitschaft.** Ihre Angriffserkennung bleibt technisch auf dem neuesten Stand und passt sich flexibel an Veränderungen Ihrer Infrastruktur an.

Datenquellen- und Use-Case-Review

- **telent Leistung:** Regelmäßige Prüfung der angebundenen Systeme sowie die Anpassung der Erkennungsszenarien an die aktuelle Bedrohungslage.
- **Ihr Nutzen - Präzise Detektion.** Die Daten- und Alarmqualität wird fortlaufend hoch gehalten, um Lücken in der Überwachung frühzeitig zu schließen.

Reporting und Nachweisunterstützung

- **telent Leistung:** Bereitstellung strukturierter Auswertungen, Berichte und Dokumentationen für interne und externe Reviews.
- **Ihr Nutzen - Auditfähigkeit.** Sie erhalten belastbare Dokumente zur Unterstützung Ihrer Nachweisfähigkeit gegenüber Auditoren und dem Management.

Kontinuierliche Verbesserung

- **telent Leistung:** Fortlaufende Optimierung von Erkennungsregeln, Meldewege und betrieblichen Prozessen.
- **Ihr Nutzen - Steigendes Sicherheitsniveau.** Ihr Schutzkonzept entwickelt sich dynamisch weiter und stärkt die Resilienz Ihrer produktionskritischen Umgebungen nachhaltig.



SCOPE UND ABGRENZUNG

Eindeutige Zuständigkeiten für einen reibungslosen Ablauf

Für den sicheren Betrieb kritischer Infrastrukturen ist eine klare Aufgabenverteilung essenziell. Während telent den technischen Aufbau und die analytische Bewertung übernimmt, verbleibt die operative Entscheidungsgewalt über die produktiven Anlagen stets bei Ihnen als Betreiber.

Die Aufgaben von telent

- Planung und technische Integration der Angriffserkennung
- Anbindung relevanter Datenquellen und logischer Sensoren
- Einrichtung und Optimierung spezifischer Erkennungsszenarien
- Analytische Bewertung von Ereignissen und Bereitstellung von Handlungsempfehlungen durch das SOC
- gemeinsame Reviews zu Schwachstellen in der Systemlandschaft
- Regelmäßige gemeinsame Reviews und Unterstützung bei regulatorischen Nachweisen



Die Aufgaben auf Kundenseite

- Bereitstellung von Zugängen, Ansprechpartnern und notwendigen Systeminformationen
- Freigabe von Systemänderungen in der Angriffserkennung und von vorgeschlagenen Optimierungen der Sicherheitsmaßnahmen
- Direkte Umsetzung betrieblicher oder technischer Maßnahmen in der eigenen Umgebung
- Pflege der internen Melde- und Eskalationswege
- Letztliche Entscheidung über organisatorische, technische oder regulatorische Schritte

KNOW-HOW, ZERTIFIKATE & AUSZEICHNUNGEN

Verbände & Technologiegremien

bitkom



BREKO
BUNDESVERBAND
BREITBANDKOMMUNIKATION



PMeV
NETZWERK SICHERE
KOMMUNIKATION

Zertifizierte Managementsysteme



Auszeichnungen



Ihr Systemintegrator und Security-Operations-Partner für wirksame Angriffserkennung in KRITIS- und OT-Umgebungen.

telent GmbH

Gerberstraße 34

71522 Backnang

Telefon: +49 7191 900-0

E-Mail: info.germany@telent.de

www.telent.de



© telent GmbH. Alle Rechte vorbehalten