Security Operations Center

Ganzheitliche IT/OT-Überwachung für Industrie & KRITIS

• modular • rechtssicher • aus Deutschland

telent
service • commitment • value

HERAUSFORDERUNGEN & UNSER ANSATZ

Wenn Verfügbarkeit keine Option, sondern Voraussetzung ist

Die fortschreitende Vernetzung industrieller Anlagen (OT) mit der IT-Welt eröffnet enorme Effizienzpotenziale, verändert aber die Risikolandschaft grundlegend. Wo früher physikalische Trennung schützte, fordern heute komplexe Angriffsvektoren und gesetzliche Vorgaben wie NIS-2 und das IT-Sicherheitsgesetz 2.0 ein Umdenken in der Sicherheitsstrategie.

Herausforderungen einer vernetzten Infrastruktur:

- **Transparenz in der OT:** „Man kann nur schützen, was man sieht." Viele Betreiber suchen nach einem Echtzeit-Lagebild über ihre Assets und Kommunikationswege.
- **Security vs. Stabilität:** Klassische IT-Sicherheitsmaßnahmen dürfen sensible OT-Umgebungen nicht beeinträchtigen. Gefragt sind Lösungen, die Anomalien erkennen, ohne die Produktion zu gefährden.
- **Umgang mit Legacy-Systemen:** Veraltete Steuerungen lassen sich oft nicht einfach patchen. Hier werden kompensierende Schutzmechanismen benötigt.
- **Regulatorischer Hochdruck:** Professionelle Log-Erfassung und Analyse sind essenziell, um Compliance wirtschaftlich und rechtssicher abzubilden.
- **Alarm-Fatigue & Expertenmangel:** IT-Teams benötigen Unterstützung bei der Bewertung von Meldungen im industriellen Kontext.

Warum telent der richtige Partner ist:

- **50 Jahre Infrastruktur-DNA:** Seit Jahrzehnten planen, bauen und betreiben wir hochverfügbare Netze für Energie, Bahn, Autobahnen und Häfen. Wir kennen die Physik dieser Netze bis ins Detail.
- **20 Jahre OT-Security-Expertise:** Wir beherrschen die Protokolle der Automatisierungstechnik (z. B. Modbus, Profinet, IEC 60870-5-104 oder OPC UA) und richten unsere SOC-Prozesse strikt an der Verfügbarkeit Ihrer Anlagen aus.
- **Zentrales SOC – Bundesweiter Service:** Unsere Analysten überwachen die Lage zentral in Backnang und Saarbrücken, während unser flächendeckendes Netz aus Service Points schnelle Unterstützung vor Ort garantiert.
- **Einfach aus Deutschland:** Wir bieten tiefe Kenntnis der lokalen Regulatorik, deutsche Fach-Ansprechpartner und höchste Standards bei der Datenhaltung (On-Premises oder Private Cloud).
- **Herstellerunabhängige Integration:** Unser Stack basiert auf marktführenden Technologien wie Fortinet und Tenable, binden jedoch als Integrator auch Ihre vorhandenen Drittsysteme nahtlos in unsere Prozesse ein.

Maximale Resilienz für Ihre Prozesse

Wir lösen den Zielkonflikt zwischen Cybersicherheit und Betriebskontinuität auf. Das telent Managed SOC agiert als Ihr hochspezialisiertes Frühwarnsystem – exakt kalibriert auf die „No-Fail"-Anforderungen Ihrer produktions- und versorgungskritischen Umgebungen.

BETRIEBSMODELLE IM DETAIL

Flexibilität durch klare Rollenverteilung

Jede Infrastruktur erfordert eine individuelle Herangehensweise. Wir bieten zwei Modelle, die eine klare Trennung zwischen technischem Betrieb und sicherheitsfachlicher Bewertung sicherstellen.

Co-Managed: Gemeinsame Stärke & Stärkung Ihrer Experten

- **Operations:** Der technische Betrieb, die Wartung und die Administration der Systeme verbleiben bei Ihnen. telent unterstützt bei Konfigurationsanpassungen und Regelpflege.
- **Analyse:** telent übernimmt die Bewertung der Ereignisse, priorisiert Alarme und leitet konkrete Handlungsempfehlungen ab.
- **Ihr Mehrwert:** Wir stärken Ihre Experten durch kontinuierlichen Wissenstransfer und gemeinsame Analyse-Expertise.

Managed: Die Rundum-Sorglos-Lösung

Wir kümmern uns um Ihre Security, damit Sie sich voll auf Ihr Kerngeschäft konzentrieren können.

- **Operations:** telent übernimmt den vollständigen technischen Betrieb inklusive Einrichtung, Patch-Management, Signaturpflege und Systemüberwachung.
- **Analyse:** telent analysiert kontinuierlich alle Ereignisse, erstellt strukturierte Lagebewertungen und liefert technische Empfehlungen zur Risikobehandlung.
- I**hr Mehrwert:** Maximale Entlastung Ihrer internen Ressourcen bei höchster Detektionsqualität.

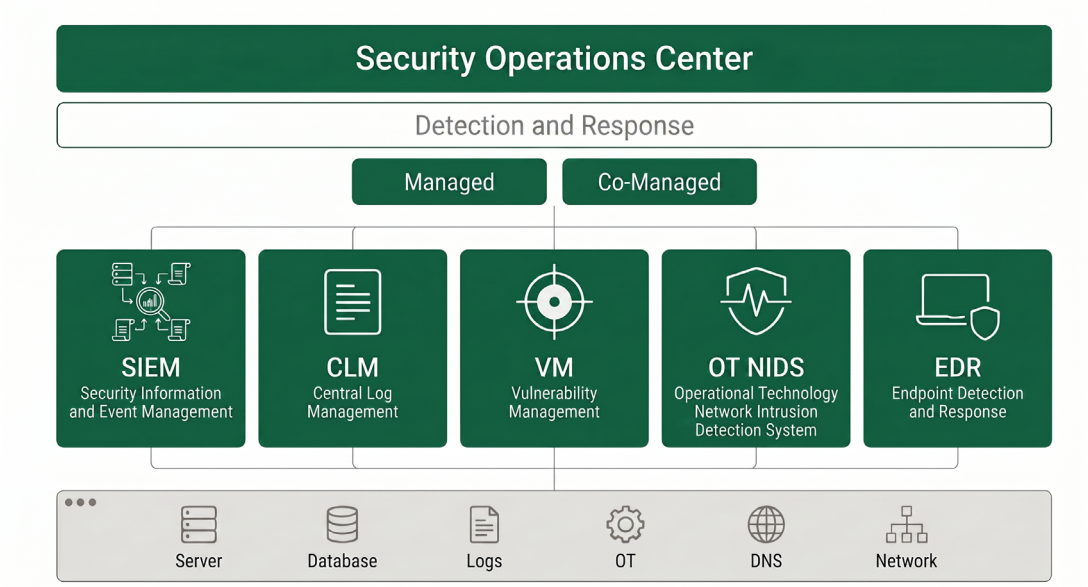
Wichtiger Grundsatz: Die operative Entscheidungsgewalt über Ihre produktiven Anlagen verbleibt stets bei Ihnen. Eingriffe erfolgen ausschließlich durch Sie oder in Ihrem expliziten Auftrag.

AUFBAU UNSERES SECURITY OPERATIONS CENTER

Technologische Tiefe für maximale Transparenz

Integrierter Schutz für komplexe Umgebungen.

Effektive Cybersicherheit in der OT lässt sich nicht mit Standardlösungen realisieren. Sie erfordert ein Zusammenspiel spezialisierter Technologien, die auf die Besonderheiten industrieller Prozesse kalibriert sind. Unser modularer Stack bildet das technologische Fundament unseres SOC-Services: Er vereint marktführende Intelligence mit tiefem Protokoll-Verständnis. Jedes Modul erfüllt dabei eine spezifische Schutzfunktion – von der passiven Netzüberwachung bis zur verhaltensorientierten Endpunkt-Analyse. Dabei greifen alle Komponenten nahtlos ineinander, um ein lückenloses Lagebild zu erstellen, ohne die Stabilität Ihrer Produktion zu gefährden.



1. SIEM – Security Information & Event Management

Zentrale Korrelation und intelligente Analyse - Erkennt komplexe Angriffe frühzeitig und schafft ein zentrales, verständliches Lagebild.

Das Herzstück Ihrer Sicherheitsüberwachung: Unser SIEM bildet das Gehirn Ihres Cyber-Abwehrzentrums. Es führt gigantische Datenmengen aus heterogenen Quellen in Echtzeit zusammen und wandelt isolierte Ereignisse durch intelligente Korrelation in ein glasklares Lagebild um. So machen wir selbst subtile, zeitversetzte Angriffsmuster über IT- und OT-Grenzen hinweg sichtbar, die in der Flut der Einzelmeldungen sonst unentdeckt blieben.

- **Operations:** Anbindung relevanter Datenquellen (SCADA, Firewalls, Netzwerk, Server). Kontinuierliche Wartung der Plattform sowie Anpassung von Erkennungsregeln und Use Cases.

  Analyse: Bewertung und Priorisierung von Alarmen. Korrelation von Ereignissen über mehrere Quellen hinweg unter Berücksichtigung des MITRE ATT&CK® for ICS Frameworks.

  Modell-Fokus: Im **Managed-Modell** stellt telent die gesamte Infrastruktur bereit. Im **Co-Managed-Modell** optimieren wir Ihre bestehenden Regeln.

2. CM – Centralized Log Management

Sichert alle relevanten Daten revisionssicher und ermöglicht schnelle Analyse im Ernstfall.

Das digitale Gedächtnis Ihrer IT/OT-Landschaft: Ein modernes Log-Management ist weit mehr als eine reine Datensammlung. Es bildet das unverzichtbare Fundament für die Revisionssicherheit und forensische Belastbarkeit Ihrer Sicherheitsarchitektur. Durch die zentrale Aggregation und Normalisierung von Log-Daten aus heterogenen Quellen schaffen wir die notwendige Transparenz, um regulatorische Anforderungen mühelos zu erfüllen und im Ernstfall eine lückenlose Rekonstruktion von Ereignissen zu ermöglichen.

- **Operations:** Anbindung der Logquellen, Normalisierung der Daten und Bereitstellung zentraler Speicherstrukturen. Überwachung der Datenflüsse an nachgelagerte Systeme.
- **Analyse:** Sicherung der notwendigen Datenqualität für alle Sicherheitsanalysen, forensische Untersuchungen und regulatorische Nachweise.
- **Modell-Fokus:** Im **Managed-Modell** verantwortet telent den vollständigen Datenfluss. Im **Co-Managed-Modell** unterstützen wir bei der technischen Strukturierung.

3. VM – Vulnerability Management

Identifiziert Schwachstellen proaktiv und priorisiert Maßnahmen nach tatsächlichem Risiko für Ihre Produktion.

Vorsprung durch proaktive Risikominimierung: In der komplexen Welt der OT-Infrastrukturen ist Wissen über Schwachstellen der entscheidende Schutzfaktor. Unser Vulnerability Management identifiziert systematisch Einfallstore in Ihren Systemen, bevor Angreifer sie finden können. Dabei bewerten wir Risiken nicht nur nach technischer Kritikalität, sondern setzen sie in Bezug zu Ihren spezifischen Produktionsprozessen, um eine zielgerichtete Priorisierung in Ihren Wartungsfenstern zu ermöglichen.

- **Operations:** Pflege der Scan-Plattform, Konfiguration von Prüfroutinen und Plugins. Durchführung technischer Prüfungen in abgestimmten OT-Wartungsfenstern.
- **Analyse:** Bewertung der Funde nach CVSS, Priorisierung nach Kritikalität und Ableitung von Empfehlungen für Patch-Pläne oder Härtungsmaßnahmen.
- **Modell-Fokus:** Im **Managed-Modell** übernimmt telent die komplette Scan-Planung. Im **Co-Managed-Modell** liefert telent die Experten-Bewertung Ihrer Scans.

4. OT-NIDS – Network Intrusion Detection System

Macht versteckte Kommunikationsmuster sichtbar und erkennt Anomalien ohne Eingriff in den Betrieb.

Der wachsame Blick in die Tiefe Ihrer Produktion: Unser OT-NIDS fungiert als passiver Radar, der den Datenverkehr Ihrer Steuerungsnetze kontinuierlich scannt, ohne den laufenden Betrieb zu beeinträchtigen. Wir machen Assets und deren Kommunikationsbeziehungen sichtbar, die sonst im Verborgenen blieben, und erkennen Anomalien in Echtzeit – ein entscheidender Faktor für die Früherkennung von Manipulationen oder technischen Fehlkonfigurationen.

- **Operations:** Pflege der Scan-Plattform, Konfiguration von Prüfroutinen und Plugins. Durchführung technischer Prüfungen in abgestimmten OT-Wartungsfenstern.
- **Analyse:** Bewertung der Funde nach CVSS, Priorisierung nach Kritikalität und Ableitung von Empfehlungen für Patch-Pläne oder Härtungsmaßnahmen.
- **Modell-Fokus:** Im **Managed-Modell** übernimmt telent die komplette Scan-Planung. Im **Co-Managed-Modell** liefert telent die Experten-Bewertung Ihrer Scans.

5. EDR – Endpoint Detection & Response

Erkennt Angriffe direkt auf Systemebene (Server & Workstations) und schützt effektiv vor Ransomware und gezielten Angriffen

Präzisionsschutz direkt am Asset: Während Netzwerk-Monitoring den Überblick behält, schützt EDR dort, wo die eigentliche Datenverarbeitung stattfindet. Auf Servern und Arbeitsstationen detektieren wir verdächtige Verhaltensmuster, die auf fortgeschrittene Angriffe hindeuten. Besonders in OT-Umgebungen mit Legacy-Systemen bietet EDR durch moderne Verhaltensanalyse einen lebenswichtigen Schutzwall gegen Ransomware und gezielte Manipulation.

- **Operations:** Bereitstellung und Pflege der Endpoint-Agenten, Verwaltung von Richtlinien und Überwachung der Sensorverfügbarkeit.
- **Analyse:** Bewertung der Funde nach CVSS, Priorisierung nach Kritikalität und Ableitung von Empfehlungen für Patch-Pläne oder Härtungsmaßnahmen.
- **Modell-Fokus:** Im **Managed-Modell** übernimmt telent das komplette Agenten-Management. Im **Co-Managed-Modell** unterstützen wir bei der Ereignisbewertung.

Im SOC inkludiert: KRITIS Audit Readiness & SOC Beratung

Strategische Begleitung und Vorbereitung auf regulatorische Prüfungen

Ganzheitliche Vorbereitung als strategischer Prozess: Echte Resilienz entsteht an der Schnittstelle zwischen Technologie, Organisation und Regulatorik. Unsere Experten begleiten Sie bei der gezielten Vorbereitung auf regulatorische Prüfungen und stellen sicher, dass technische Maßnahmen mit den komplexen Anforderungen von NIS-2 und dem BSI in Einklang stehen. Von der ersten Reifegrad-Analyse bis zur Begleitung bei der Audit-Vorbereitung übersetzen wir gesetzliche Pflichten in eine nachhaltige Sicherheitsstrategie.

- **Operations:** Strukturierte Aufnahme der Systemlandschaft, Bewertung von Komponenten und Analyse technischer Betriebsprozesse zwischen IT und OT.
- **Analyse:** Bewertung des Sicherheitsreifegrades (z. B. Audit Readiness), Identifikation organisatorischer Lücken und Entwicklung von Roadmaps für den SOC-Ausbau.
- **Kerninhalte:** Unterstützung bei Sicherheitskonzepten, Use-Case-Definitionen und Vorbereitung regulatorischer Nachweise sowie Audit-Begleitung (etwa BSI, NIS-2 etc.).

Starten Sie jetzt: telent begleitet Sie von der ersten Analyse bis zum 24/7-Betrieb – damit Ihre Produktion sicher vernetzt bleibt.

KNOW-HOW & ZERTIFIKATE

Verbände & Technologiegremien

bitkom

Teilnehmer der Allianz für Cyber-Sicherheit

UP KRITIS

BREKO BUNDESVERBAND BREITBANDKOMMUNIKATION

DMR DIGITAL MOBILE RADIO ASSOCIATION

SecurITy made in Germany Trust Seal www.teletrust.de/itsmig

PMeV NETZWERK SICHERE KOMMUNIKATION

Zertifizierte Managementsysteme

SILVER | Top 15% ecovadis Sustainability Rating SEP 2024

Zertifiziert durch TÜV THÜRINGEN ISO 9001 / ID:15 100 2511820 www.tuev-thueringen.de

Zertifiziert durch TÜV THÜRINGEN ISO 14001 / ID:15 104 252229 www.tuev-thueringen.de

Zertifiziert durch TÜV THÜRINGEN ISO 27001 / ID:15 121 25285 www.tuev-thueringen.de

Zertifiziert durch TÜV THÜRINGEN ISO 45001 / ID:15 118 25702 www.tuev-thueringen.de

Sicher. Vernetzt. Innovativ. telent!

telent GmbH

Gerberstraße 34
71522 Backnang
Telefon: +49 7191 900-0
E-Mail: info.germany@telent.de

www.telent.de

telent
service • commitment • value