Security Operations Center

Managed Service

IT- und OT-Security aus Deutschland

telent

service • commitment • value

Das telent SOC im Überblick

Ihre Vorteile

- Kontinuierlicher Schutz Ihrer OT und IT
- Erfahrungen mit proprietären Protokollen
- Schnelle Erkennung „abnormaler“ Kommunikation
- Identifizierung von potenziellen und realen Bedrohungen
- Schutz vor aktuellen Bedrohungen
- Schnelle und wirksame Reaktionen
- Kommunikation und Zusammenarbeit zwischen dem SOC und Ihren Security-Verantwortlichen
- Erhöhte Sicherheitsexpertise
- Voller Überblick über das Geschehen im Netzwerk
- Senkung der Kosten im laufenden Betrieb
- Konformität: Nachweis der Einhaltung von gesetzlichen Regeln und Compliance-Vorgaben
- Return on Security Invest

Unsere Prozesse

- Konvergierte Darstellung Ihrer IT- und OT-Sicherheitslage über unsere Benutzeroberfläche
- Ihre Daten verbleiben in Ihrem Unternehmen. Wir erfüllen höchste Datenschutzstandards

Unser Personal

- Unsere Mitarbeiter können auf einen jahrelangen Erfahrungsschatz in Cybersecurity, Automatisierungs-, Prozess- und Netzleittechnik in Industrie und KRITIS zurückgreifen. Diese Expertise, gepaart mit dem neuesten Stand der Technik, kommt Ihnen zugute

SOC as a Service

Ein SOC setzt auf die Kombination aus Prozessen, Technik und Experten, um Security-Risiken zu verhindern, aufzudecken, zu bewerten und unter Kontrolle zu bringen sowie die forensische Analyse einzuleiten.

telent etabliert sich als Security Operations Center (SOC) in Ihrem Unternehmen und übernimmt den laufenden Betrieb. In kürzester Zeit ist das SOC einsatzbereit, operiert nach bewährten Prinzipien und basiert auf modernster Technologie unseres Partners RADAR Cyber Security. Persönliche Ansprechpartner:innen, klare Regelungen und dokumentierte Prozesse ermöglichen strukturierte Abläufe und eine einfache und zielführende Kommunikation zwischen Ihrem Unternehmen und unserem SOC.

Empfohlene Kernmodule

LDA NBA VMC

Empfohlene Zusatzmodule

ATD EDR

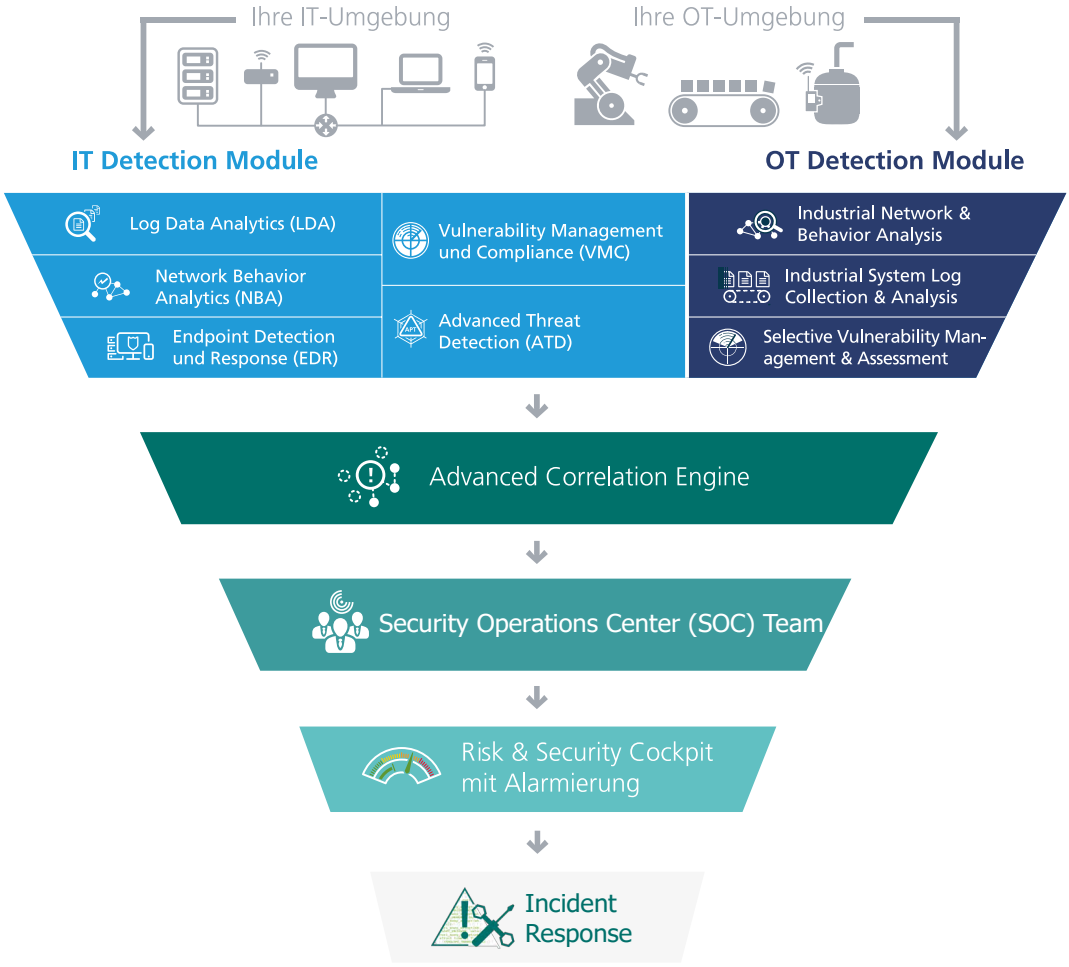
Die Kompetenzen unseres Security Operations Center

- Team mit Fokus auf Angriffs- und Risikoerkennung
- Branchenübergreifender Einsatz von Use Cases
- Erkenntnisse aus der fortlaufenden Analyse werden zur Modifikation der geltenden Richtlinien und Regeln der automatisierten Risikoerkennung genutzt
- Jede Vorfallsbeschreibung wird durch unsere Experten mit einer Empfehlung zur Risikoerkennung ergänzt

IT- und OT-Detection: Alles im Blick

telent erfasst und analysiert die Risiken in der IT- und OT-Infrastruktur unter Einbeziehung der Wichtigkeit von Komponenten, stellt das interne Kontrollsystem (IKS) dar und bildet Compliance sowie Gesetzesanforderungen ab. Klare Informationen zu Geschäftsprozessen und Risikomanagement der IT-/OT-Services sind abrufbar.

Konsolidierte IT- und OT-Security



Module für Ihre Cybersecurity

Das telent SOC wird von einer starken Kombination aus menschlicher Expertise und Erfahrung angetrieben. Wir vereinen Cyber Security Expert:innen und die europäische Technologie unseres Partners RADAR Cyber Security, um Ihnen passgenaue Lösungen für die Herausforderungen von heute und morgen anzubieten.

Log Data Analytics

Logdatenanalyse mit Machine Learning und Use-Case-Forschung

Die Sammlung, Analyse und Korrelation von Logdaten aus verschiedensten Quellen ist die Kerndisziplin der IT-Sicherheit. Diese Art der Erkennungsleistung wird oftmals über ein SIEM verwirklicht. Das Resultat: Sicherheitsrelevante Informationen und Indicators of Comprise in Echtzeit, die schnellstmögliche Maßnahmen bei einem Sicherheitsvorfall erlauben.

- Unterstützung gängiger Log-Formate
- Aggregation von Events und Informationen aus allen Bereichen
- Identifizierung potentieller Risiken durch die Correlation Engine mit kontinuierlich erweiterten und maßgeschneiderten Regeln und Policies

Network Behavior Analytics (NBA)

Erkennung von gefährlicher Malware, Anomalien und anderen Risiken im Netzwerkverkehr auf Basis von signatur- und verhaltensbasierten Detection Engines.

- Mehr als 19.000 kontinuierlich erweiterte, mit IP-Reputationsdaten verglichene, Signaturen und Regeln
- Verhaltensbasierte Analysen für Zero-Day-Exploits und andere noch nicht bekannte Angriffsarten, Erkennung von Protokollen und Ports
- Identifizierung verschiedener Dateitypen anhand der MD5-Prüfsummen und weitergehender Dateiextraktion, um Dokumente gegebenenfalls nicht in oder aus dem Netzwerk transferieren zu lassen

Vulnerability Management & Compliance (VMC)

Kontinuierliche, interne und externe Schwachstellen-Scans mit Erkennung, Compliance Checks und Tests für eine komplette Abdeckung zu allen Schwachstellen.

- Kontinuierliche interne und externe Schwachstellen-Scans für einen 360-Grad-Überblick
- Authentifizierte oder nicht-authentifizierte Schwachstellen-Scans
- Erkennung von offenen Ports und der Nutzung von potentiell unsicheren oder überflüssigen Services auf diesen Ports
- Compliance- und Passwort-Checks zur Erkennung von Konfigurationsproblemen in Bezug auf Anwendungen und Passwörter- sowie Benutzerrichtlinien
- Feststellung von Standard- oder fehlenden Passwörtern
- Empfehlungen zur Schwachstellen-Kategorisierung in hohes, mittleres und geringes Risiko und die Möglichkeit ihrer Ausnutzung

Advanced Threat Detection (E-Mail & Web / ATD)

Sandbox-Technologien der nächsten Generation werden für die Erkennung von „Advanced Malware“ in E-Mails und Downloads eingesetzt.

- Modernste Erkennungsmethoden für hochentwickelte und getarnte Malware
- Sandbox-Technologien der nächsten Generation mit vollständiger Systememulation und tiefgreifendem Verständnis von Malware-Verhalten
- Feststellung von Standard- oder fehlenden Passwörtern
- Produktiver E-Mail-Verkehr – verdächtige Nachrichten erkennen und blockieren
- Kontinuierliche Updates des Feeds für Advanced Threats

Endpoint Detection & Response (EDR)

Die Analyse, Überwachung und Erkennung von Anomalien bei Hosts führen zu aktiven Reaktionen und sofortiger Alarmierung.

- Sammlung, Analyse und Korrelation von Logs eines Servers oder Clients
- Alarmierung bei der Erkennung von Angriffen, Missbrauch oder Fehlern
- Überprüfung der Dateiintegrität des lokalen Systems
- Rootkit-Erkennung identifiziert z.B. versteckte Angriffe, Trojaner oder Viren anhand von Systemveränderungen

Schutz Ihrer OT-Infrastruktur

Operational Technology (OT) und industrielle Kontrollsysteme sind oft mit der IT-Infrastruktur vernetzt. Ein ganzheitlicher Überblick und eine konvergente Sicht auf IT- und OT-Systeme gewährleisten einen optimalen Schutz vor Cyberbedrohungen.
Alle gesammelten Daten werden synchron analysiert und weiterverarbeitet.

Industrielle Netzwerkverhaltensanalyse

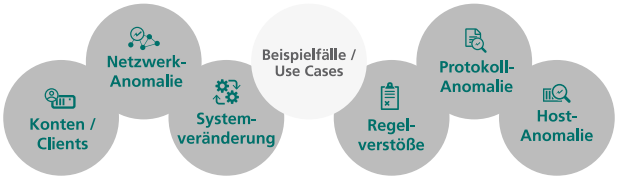
- Erkennung aus Protokoll- und Flow-Daten
- Metadaten-Extraktion aus industriellen Protokollen
- Automatische Analyse durch Machine Learching

Industrielle System-Protokollsammlung und Analyse

- Erkennung von sicherheitskritischen Vorgängen und Anomalien auf der Grundlage von definierten Use Cases
- Sammlung, Normalisierung und Korrelation von OT-Logs
- Erweiterte Korrelation mit integrierter IT- und OT-Protokolldatenanalyse

Gezieltes OT-Schwachstellenmanagement und Bewertung

- OT-Schwachstellenscans
- Bewertung von Schwachstellen basierend auf Asset-Daten
- OT Threat Intelligence und Wissensaufbau zu Bedrohungsarten



Analyse, Schlussfolgerung & Visualisierung

Advanced Correlation Engine

Die Korrelation innerhalb eines Moduls und die Cross-Korrelation von Informationen aus verschiedenen Modulen führen zu einer hochqualitativen Erkennung von Risiken und Sicherheitsproblemen. Dies ermöglicht einen umfassenden Blick auf die sicherheitsrelevanten Vorkommnisse innerhalb eines Unternehmens.

- Gesamtüberblick über sicherheitsrelevante Daten
- Miteinbeziehung von Logs, Schwachstellen, Anomalien, Asset-Informationen und vielem mehr
- Korrelation und Cross-Korrelation basieren auf Regeln, Policies und selbstlernenden Algorithmen
- Unterscheidung zwischen normalem und abnormalem Verhalten in der IT- und OT-Infrastruktur
- Laufende Erweiterung der Regelwerke und statistischen Modelle
- Alarmierung in kritischen Situationen

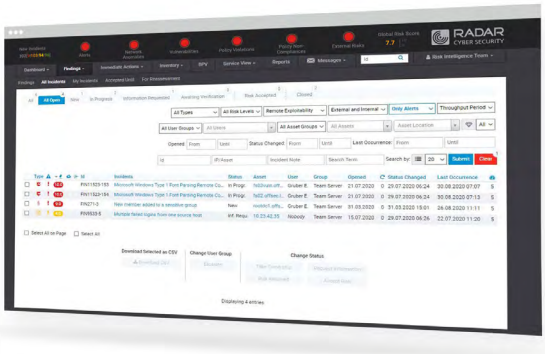
Dashboards: Analyse und Entscheidung leicht gemacht

Unsere Technologie-Ausstattung umfasst Benutzeroberflächen, die schnell und unkompliziert einen Überblick zu wesentlichen Sicherheitsfragen aus konsolidierten IT- und OT-Daten geben.

RADAR Analytics Interface (RAIN)

Das RADAR Analytics Interface ist ein ideales Cybersecurity-Analysewerkzeug. Komplexe Daten werden vereinfacht und können so leichter interpretiert werden. SOC-Analysten, Threat-Hunter sowie Incident Response Verantwortliche können Alarmmeldungen analysieren, mittels Drill Downs die dahinterliegenden Daten aus verschiedenen Perspektiven beleuchten und damit weitere Analyseergebnisse liefern, die wiederum im Risk & Security Cockpit ausgeworfen werden. Für spätere Analysen können Abläufe in Regeln überführt und damit automatisiert werden, um dazu laufend weitere Alarmierungen zu erhalten. Aufgrund der breiten Datenbasis aus der gesamten IT- und OT-Infrastruktur können die Bedrohungen anschaulich auf Dashboards visualisiert und Beziehungen zwischen Sicherheitsereignissen veranschaulicht werden.

- Big Data Analytics verringern mithilfe der Kombination aus historischen und aktuellen Risikodaten den administrativen Aufwand
- Ansicht von Daten im relevanten Kontext
- Nahtlose Konvergenz und effiziente Orchestrierung



Risk & Security Cockpit

Im Risk & Security Cockpit werden Ergebnisse aus der Sicherheitsanalyse und -bewertung dargestellt. Diese dienen als Grundlage für die Festlegung von Gegenmaßnahmen im Fall von gemeldeten Cyberangriffen. Analysierte Risiko- und Sicherheitsbenachrichtigungen werden zentral im Risk & Security Cockpit präsentiert. Maßgeschneiderte und leicht verständliche Risikoberichte und Statistiken sind auf Knopfdruck verfügbar.

- Risikolevel-Bewertung in 4 Stufen
- Berichte und Statistiken in der gewünschten Detailtiefe
- Alarmierung in kritischen Fällen
- Durchgehender und nachvollziehbarer Risikobehebungs-Workflow
- Nachrichten- und Feedback-System für die Kommunikation mit dem SOC-Team
- Integrierter Business Process View zeigt die durch die Sicherheitsprobleme gefährdeten Geschäftsprozesse auf

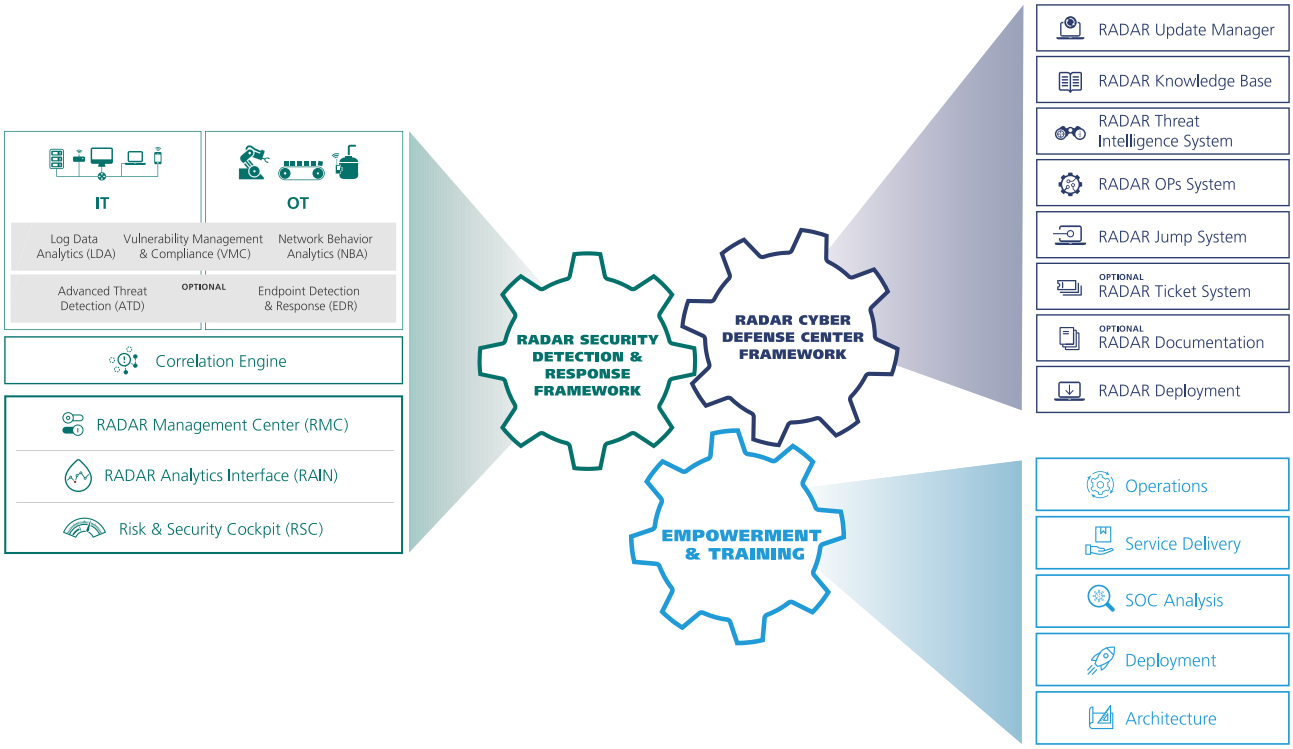
Incident Response

Die telent GmbH bietet einen Incident Response Service an, der Teil unseres umfassenden Security Operations Center (SOC) ist. Dieser Service ist darauf ausgerichtet, Kunden bei der Bewältigung von Sicherheitsvorfällen zu unterstützen.
Ein engagiertes Team erfahrener Sicherheitsexperten und moderne Technologien gewährleisten schnelle Reaktionen auf Bedrohungen und Schutz rund um die Uhr.

Der Incident Response Service dient zur Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen. Dies umfasst die schnelle Reaktion auf Bedrohungen, um Schäden und Datenverlust zu minimieren.

Technik des telent SOC im Detail

Das telent SOC nutzt die Technologie und Prozesse seines Partners RADAR Cyber Security. RADAR ist der einzige europäische Anbieter von Managed Detection & Response, der seit über 10 Jahren auf Basis einer eigenentwickelten Kerntechnologie arbeitet.
Auf Grundlage dieser bewährten Technologie erarbeiten wir für unsere Kunden eine passende Ausprägung und lassen die individuellen Anforderungen einfließen.



Cyber Defense Center Framework

Das Cyber Defense Framework umfasst alle verwendeten Technologien von RADAR Solutions, die wir zum Betrieb des telent SOC nutzen, um IT- und OT-Sicherheitsinformationen aufbereiten und analysieren zu können.

RADAR Update Manager

Komponente zur Integration der neuesten Updates für den gesamten Software-Stack, Threat Intelligence-Daten, Detection Use Cases, Signaturen und Knowledge Base.

RADAR Jump System

Komponente zur Gewährleistung einer sicheren Verbindung zum SOC mit RADAR-Technologie am Standort des RADAR Solutions Anwenders mithilfe von Thin Clients, Bildschirmaufzeichnungen und sicheren Anmeldeprozessen.

RADAR Knowledge Base

Komponente zur Speicherung aller Use Cases sowie Warnmeldungen und Vorfallsbeschreibungen mit klarer Zusammenfassung, Beschreibung und Handlungsempfehlungen.

RADAR Ticket System

Zentrales Tool für SOC-Supportfälle, Koordination von CDC-Serviceaufgaben und interne Nachverfolgung mit Schnittstelle zur zentralen Alarmierung.

RADAR Threat Intel-System

Komponente zur Analyse, Verwaltung sowie Integration von Indicators of Compromise, Data Enrichment (Closed/Open Source) und Erkennungsregeln.

RADAR-Dokumentationssystem

Komponenten für den Wissensaustausch innerhalb Ihres CDC-Teams sowie für die Ablage von Playbooks, Runbooks, etc.

RADAR-Betriebssystem

Alle notwendigen Komponenten für den Betrieb der Plattform (z.B. Monitoring, Backup, Wiederherstellung).

RADAR Deployment System

Deployment zu Installationen beim Kunden.

Security Detection & Response Framework

Dieses Framework umfasst alle Komponenten, welche für die Erkennung und Analyse und in Folge zur strukturierten Aufarbeitung der angezeigten Sicherheitsvorfälle notwendig sind. Die Daten aus den Erkennungsmodulen werden gesammelt und in übersichtlichen Dashboards aufbereitet.
Sicherheitsvorfälle in der überwachten IT-/OT-Umgebung können erfasst werden.

- RADAR Analytics Interface für Security Operations Center-Analysten
- Risk & Security Cockpit für Entscheidungsträger
- Darüber hinaus sind Workflow-Cockpits für die Verwaltung aller administrativen Aufgaben innerhalb eines SOC in das RADAR Management Center integriert

Empowerment & Training

RADAR Cyber Security bietet SOC-Verantwortlichen Schulungsprogramme für die unterschiedlichen Aufgaben bei der Anwendung von RADAR Solutions. Natürlich haben unsere Analysten und SOC-Mitarbeiter diese durchlaufen.
Zusätzlich bringen Sie ihre eigene, in vielen Jahren erworbene Expertise in der Erkennung und Abwendung von Cyberbedrohungen in IT- und OT-Umgebungen mit ein.

Um Angriffe und Cybersecurity-Incidents zu verhindern, ist es notwendig, die Kommunikationsprotokolle zu überwachen und den Netzwerkverkehr mittels modernster Technik und der entsprechenden Fachkenntnis auszuwerten.
Um auf sicherheitsrelevante Ereignisse angemessen reagieren zu können, kommt ein moderner Technologiemix aus fortlaufender Überwachung und Auswertung der Kommunikation im IT/OT-Netzwerk sowie auf die Erkennung von Anomalien inklusive Alarmierung bei sicherheitsrelevanten Ereignissen zum Einsatz.

Haben Sie Fragen zum telent SOC oder anderen Managed Security Services?

Gemeinsam finden wir die für Sie ideale Lösung - Versprochen!

telent

service • commitment • value

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

POWERED BY RADAR CYBER SECURITY

www.telent.de