



# BODYGUARD SERVICE

## managed detection & response

Bodyguard ist ein Managed Service zur Erkennung, Abwehr und kontinuierlichen Überwachung von Cyberbedrohungen.

Der Bodyguard Service sorgt dafür, dass Angriffe früh erkannt und schnell entschärft werden – rund um die Uhr, herstellerunabhängig, mit technischer Unterstützung durch KI-gestützte Plattformen.

- ✓ On-Premises or Cloud
- ✓ Managed SIEM
- ✓ Managed EDR / XDR
- ✓ Managed Vulnerability



### Leistungen und Funktionen

Funktion	Beschreibung
Security Operations Center <b>SOC</b>	24/7 Monitoring durch Sicherheitsexperten, inklusive Überwachung aller sicherheitsrelevanten Ereignisse.
Incident Detection & Response	Identifizierung von Vorfällen, Analyse und Einleitung von Gegenmaßnahmen durch das Telonic CERT-Team - remote oder deutschlandweit vor Ort
Security Automation Plattform <b>SOAR</b>	Unsere eigene Plattform zur Automatisierung und Unterstützung: Aus Protokoll Daten (Logs) und anderen Quellen werden automatisiert leicht verständliche, nachvollziehbare Handlungsempfehlungen bzw. Maßnahmen abgeleitet oder durchgeführt.
Vulnerability Management	Erkennung und Bewertung von Schwachstellen in der Infrastruktur; proaktives Maßnahmenmanagement (Patching / Upgrades), sowie Risk-Scoring.
Performance- / Netzwerk-Monitoring	Überwachung von Netz- und Systemleistung, Auslastung und Nutzerverhalten, um Auffälligkeiten frühzeitig zu erkennen und zu stoppen.
Herstellerunabhängig	Unsere Lösungen und Tools sind nicht an einen Anbieter gebunden. Maßnahmen und Integration erfolgen individuell nach Kundenbedarf.

### Vorteile / Nutzen

- **Frühzeitige Erkennung & schnelle Reaktion:** versteckte Angriffe erkennen und sofort Gegenmaßnahmen einleiten
- **Rund-um-die-Uhr-Abdeckung:** Monitoring und Service 24/7
- **Risikominimierung:** Geringere Schäden durch datengestützte Schwachstellenanalyse und aktive Gegenmaßnahmen
- **Compliance:** Unterstützung bei der Einhaltung von Vorgaben wie NIS2 oder Cyber Resilience Act
- **Skalierbar & modular:** Kunden wählen passende Module nach Bedarf – z. B. nur Monitoring & Detection, oder inkl. Response, Vulnerability Management, Performance-Monitoring

### Operative Angaben

- **Standort**  
SOC in Köln, deutschlandweit im Einsatz, eigenes Team & Infrastruktur
- **Features**  
Log-Analyse, Event-Management, Vulnerability-Scanning/-Management, Response-Prozesse.
- **Implementierung**  
Schnelle Integration in Security-Systeme (Firewall, EDR/XDR, NDR, Virens Scanner) sowie in die Microsoft-Domäne. Inkl. großem Katalog vorgefertigter Run-/Playbooks
- **Automatisierung**  
SOAR ist mit an Bord, Schnelle Priorisierung und Handlungsempfehlungen aus unserer KI.

### Warum Telonic?

Der Telonic Bodyguard Service verbindet eine KI-Plattform mit menschlicher Expertise (SOC/CERT) zu einem vollständig betreuten Managed Service – mit klaren Prozessen, lokalen Ansprechpartnern und schneller, verlässlicher Reaktion statt einer anonymer Standard-Cloud-Lösung.

