SOC READINESS - BERATUNG & BEGLEITUNG ZUM EIGENEN SECURITY OPERATIONS CENTER

Der SOC Readiness Service unterstützt Unternehmen dabei, ein eigenes Security Oerations Center (SOC) aufzubauen - fachlich, organisatorisch und technisch. Ziel ist es, Kunden auf dem Weg vom Projektstart bis zum stabilen SOC-Betrieb zu begleiten: praxisnah, anpassbar und auf Standards wie ISO 27001, BSI IT-Grundschutz oder NIST abgestimmt.

Der Service umfasst Prozessdesign, Rollenerklärung, Systemarchitektur, Tool-Setup, Detection Use Cases, Betriebskonzept - und auf Wunsch auch Begleitung in den ersten Betriebsmonaten.

Leistungsumfang (modular)

Modul / Thema	Beschreibung
Initialanalyse / Gap Assessment	Erhebung IST-Zustand, Zieldefinition, Identifikation von Lücken
SOC-Konzeptentwicklung	Aufbau- und Ablauforganisation, Rollenmodell, Schichtbetrieb (wenn erforderlich)
Prozessdefinition	Incident Handling, Use Case Mgmt, Escalation, Logmanagement, Change, Reporting
Toolauswahl / Architekturberatung	Unterstützung bei Auswahl SIEM, SOAR, EDR, Logsource-Anbindung
Detection Engineerin (optional)	Use-Case-Definition, Regelwerk, Korrelation, Tuning
Einführungsbegleitung / Pilotbetrieb	Begleitung der Umsetzung, Interimsrollen, Coaching
Betriebsübergabe / Controlling	Unterstützung beim Übergang in den Eigenbetribe inkl. Reporting-Templates

MH SERVICE
WORLD OF FORENSICS

SOC READINESS - BERATUNG & BEGLEITUNG ZUM EIGENEN SECURITY OPERATIONS CENTER

Abgrenzung / Nicht enthalten

Enthalten

Konzeption & Beratung
Prozessdefinition, Architektur, Tool- Bewertung
Unterstützung beim Aufbau des SOC
Begleitung der ersten Betriebsphasen (optional)

Nicht enthalten (optional zubuchbar)

Betrieb als Service (kein Outcourced SOC)
Tool-Lizenzen, Implementierung Dritter
Incident Response im Regelbetrieb
Schulungen für ganze Teams (seperates Awareness-Paket)

Technische Voraussetzung / Kundenanforderungen

- Bereitschaft zur Etablierung interner Security-Prozesse
- Beteiligung von IT-Security / IT-Leistung / Geschäftsführung
- Bereits vorhandenes oder geplantes SIEM-/Logkonzept vorteilhaft
- Projektlaufzeit typischerweise 6-12 Wochen (konzeptionell)
- Optional: längerfristige Begleitung (Pilot + 3-6 Monate Betrieb)

Nutzen für den Kunden

- **Eigener SOC-Betrieb ohne teure Fehlstarts**
- **Klare strukturierter Fahrplan mit Best-Practice-Prozesse**
- **Prozess- & Toolabgleich mit Compliance-Vorgaben**
- **Professionelle Betriebsübergabe inkl. Dokumentation**
- **Ideal für KRITIS, ISO 27001, interne Audits oder IT-Grundschutz**

SERVICE
WORLD OF FORENSICS