SOC SERVICE - MANAGED SIEM MONITORING (24/7)

Der SOC Service stellt unseren Kunden ein vollständig betriebenes Security Operations Center (SOC) zur Verfügung - mit dem Fokus auf kontinuierliches Monitoring sicherheitsrelevanter Ereignisse über ein zentrales SIEM-System. Basierend auf unserem MDR-Service und verknüpft mit bewährten Detection Use Cases, übernehmen wir den Betrieb, die Analyse, die Priorisierung und - je nach Vereinbarung - die Eskalation von Vorfällen.

Funktionsumfang

Funktion / Bereich	Beschreibung
SIEM-Betrieb & Logsammlung	Anbindung relevanter Quellen (AD, Firewalls, EDR, Server, M365 etc.)
24/7 Ereignisanalyse	Kontinuierliche Überwachung durch Analysten-Team
Alert Triage & Priorisierung	Bewertung und Kategorisierung sicherheitsrelevante Events
Korrelation & Use Cases	Vordefinierte + kundenspezifische Detection-Regeln
Alarmweiterleitung / Eskalation	Je nach Vereinbarung (Mail, Ticketsystem, telefonisch)
Reporting	Monatsreport mit Vorfallhistorie, Übersicht und Handlungsempfehlung
Optional: Playbook-gestützte Reaktion	Basierend auf definierten Response-Aktionen
Dashboard-Zugriff (optional)	Co-View für Kunden (Read-only)

MH SERVICE
WORLD OF FORENSICS

SOC SERVICE - MANAGED SIEM MONITORING (24/7)

Abgrenzung / Nicht enthalten

Enthalten

24/7 SIEM-Monitoring & Alertbearbeitung
Detection & Bewertung verdächtiger Aktivitäten

Eskalation an definierte Ansprechpersonen
Reporting, Use Case Tuning

Nicht enthalten (optional zubuchbar)

Forensik / Tiefenanalyse / Incident Response

Systempflege der Kundensysteme

Vollständige Reediation / Incident Handling
Einführung Management externer Tools (SOAR etc.)

Technische Voraussetzung / Kundenanforderungen

- Bereitschaft zur zentralen Logbereitstellung / Log-Quellen-Anbindung
- Je nach Umfang: Agentenbereitstellung, API-Keys, Netzwerkzugriff
- Einführung i.d.R. durch SOC Readliness oder MDR Vorprojekt
- Verfügbarkeit technischer Ansprechpartner auf Kundenseite

Nutzen für den Kunden

- Permanente Überwachung sicherheitskritischer Infrastruktur
- Schnelle Erkennung realer Vorfälle, kein Rauschen
- Zeitersparnis & Entlastung der internen IT / Security
- Professioneller SOC-Service ohne Aufbau eigener Ressourcen
- Ideale Ergänzung zu Enpoint Security, Firewalls, MDR

SERVICE
WORLD OF FORENSICS