🗂️ Internes Produktdatenblatt

Produktname: SOC Service – Managed SIEM Monitoring (24/7)

Status: aktiv / in Einführung
Version: 1.0
Erstellt am: 28.07.2025
Verantwortlich: Jonas Plitt
Zielgruppen: Mittelstand, KRITIS, Behörden, Kunden mit MDR-Vorstufe oder SOC Readiness

---

1. 📌 Produktziel / Zweck

Der **SOC Service** stellt unseren Kunden ein vollständig betriebenes **Security Operations Center (SOC)** zur Verfügung – mit 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.

Das Ziel: **Transparenz, Reaktionsfähigkeit und nachhaltige Bedrohungserkennung – rund um die Uhr.**

---

2. 🧩 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 sicherheitsrelevanter Events
Korrelation & Use Cases	Vordefinierte + kundenspezifische Detection-Regeln
Alarmweiterleitung / Eskalation	Je nach Vereinbarung (Mail, Ticketsystem, telefonisch)
Reporting	Monatsreport mit Vorfallhistorie, Übersicht und Handlungsempfehlungen
Optional: Playbook-gestützte Reaktion	Basierend auf definierten Response-Aktionen
Dashboard-Zugriff (optional)	Co-View für Kunden (Read-only)

---

3. 🔒 Abgrenzung

Enthalten	Nicht enthalten (optional zubuchbar)
24/7 SIEM-Monitoring & Alertbearbeitung	Forensik / Tiefenanalyse / Incident Response
Detection & Bewertung verdächtiger Aktivitäten	Systempflege der Kundensysteme
Eskalation an definierte Ansprechpersonen	Vollständige Remediation / Incident Handling
Reporting, Use Case Tuning	Einführung/Management externer Tools (SOAR etc.)

---

4. ⚙️ Technische Voraussetzungen

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

---

5. 💶 Preisgestaltung (Richtwerte)

Paketumfang	Beschreibung	Preisansatz
Basispaket bis 10 Quellen	inkl. 24/7 Monitoring & Reporting	ab 2.490 € / Monat netto
Erweiterung pro Quelle / Ereignislast	z. B. zusätzliche Systeme, Cloud-Logs	auf Anfrage
Einrichtungs-/ Onboardingpauschale	Use-Case-Setup, Quellintegration, Dashboards	ab 3.900 € einmalig

Preismodelle für einen SOC Service (exkl. SIEM-Lizenz)

Modell	Typischer Preisbereich	Einschätzung
Pro Endpoint	10 – 20 USD pro Monat pro Gerät	Skalierbare Preisgestaltung
Flat-Rate Paket	1.000 – 10.000 USD pro Monat	Mittelständisches Niveau oft 10k+
Managed SIEM Add-On	5.000 – 10.000 USD pro Monat	Zusätzlicher Log-Service

---

6. ✅ 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 Endpoint Security, Firewalls, MDR

---

7. 🧩 Cross-Selling / Erweiterung

- Integration mit **Incident Response** (Managed Response)
- Verknüpfung mit **Forensik / Beweissicherung** bei Eskalation
- Awareness & SOC-Reporting für Führungskräfte
- Automatisierte Reaktion (SOAR) – optional

Ihr digitales Frühwarnsystem – 24/7, mit echten Analysten.“