🗂️ Internes Produktdatenblatt

Produktname: SOC Readiness – Beratung & Begleitung zum eigenen Security Operations Center

„Vom Start zum SOC – ohne Umwege."

Status: aktiv / in Entwicklung
Version: 1.0
Erstellt am: 28.07.2025
Zielgruppe: Mittelstand, KRITIS-Unternehmen, IT-Abteilungen mit interner Security, Organisationen mit Compliance-Anforderungen
Verantwortlich: [Produktverantwortlicher eintragen]

---

1. 📌 Produktziel / Zweck

Der **SOC Readiness Service** unterstützt Unternehmen dabei, ein eigenes Security Operations 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, Rollenklärung, Systemarchitektur, Tool-Setup, Detection Use Cases, Betriebskonzept** – und auf Wunsch auch Begleitung in den ersten Betriebsmonaten.

---

2. ⚙️ 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 Engineering (optional)	Use-Case-Definition, Regelwerk, Korrelation, Tuning
Einführungsbegleitung / Pilotbetrieb	Begleitung der Umsetzung, Interimsrollen, Coaching
Betriebsübergabe / Controlling	Unterstützung beim Übergang in Eigenbetrieb inkl. Reporting-Templates

---

3. 🔒 Abgrenzung / Nicht enthalten

Enthalten	Nicht enthalten (optional zubuchbar)
Konzeption & Beratung	Betrieb als Service (kein Outsourced SOC)
Prozessdefinition, Architektur, Tool-Bewertung	Tool-Lizenzen, Implementierung Dritter
Unterstützung beim Aufbau des SOC	Incident Response im Regelbetrieb
Begleitung der ersten Betriebsphasen (optional)	Schulungen für ganze Teams (separates Awareness-Paket)

---

4. 🧩 Technische Voraussetzungen / Kundenanforderungen

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

---

5. 💶 Preisgestaltung (Richtwerte)

Modul	Beschreibung	Beispielpreis
SOC Readiness (Basis)	Konzeption + Prozesse + Architekturvorschlag	ab 4.900 € netto
Detection Engineering Paket	Use Cases, Regelsets, Korrelationen	ab 2.900 € netto
Pilotbegleitung (3 Monate)	Interimsbetrieb + Coaching	ab 3.500 € netto
Betriebsüberführung + Review	Abschlussbericht, Reporting-Vorlagen, Übergabe	ab 1.490 € netto

---

6. ✅ Nutzen für den Kunden

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

---

7. 🧩 Cross-Selling / Erweiterung

- MDR-Service für Hybridmodell (intern + extern)
- SIEM-/SOAR-Beschaffung & Einführung
- Awareness-Workshops: „SOC Rollen & Reaktion verstehen“
- Integration in Incident Response und Forensik-Prozesse