

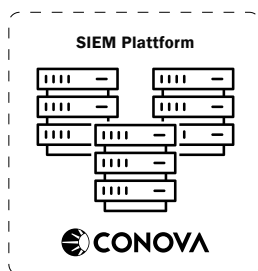
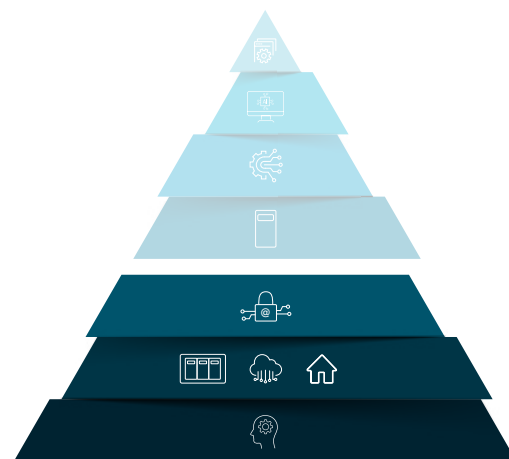
TOPMDR SOC

IHRE GANZHEITLICHE 24X7 SECURITY ÜBERWACHUNG AUS EINER HAND

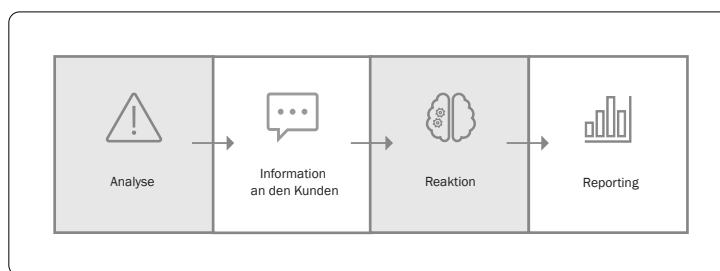
TopMDR SOC ist eine ganzheitliche SOC-as-a-Service-Lösung (Security Operations Center), die 24x7 sicherheitsrelevante Ereignisdaten aus IT-, Netzwerk-, und Cloud-Umgebungen zentral analysiert. Mithilfe moderner SIEM-Technologien (**TopMDR SIEM**) werden Anomalien und Bedrohungen in Echtzeit erkannt und als Alerts an das SOC übergeben. Ein Expertenteam bewertet und bearbeitet diese Vorfälle und dokumentiert alle Maßnahmen lückenlos – über On-Premises-, Hosted- und Public-Cloud-Umgebungen hinweg. Das sorgt für maximale Transparenz sowie eine sichere Grundlage für Audits und Zertifizierungen.

Highlights im Überblick

- DSGVO-konforme Datenverarbeitung &-speicherung innerhalb der EU
- Kein eigenes SOC notwendig: Entlastung interner IT-Teams
- Frühzeitige Angriffserkennung sowie automatisierte Identifikation und Bewertung von Bedrohungen in Echtzeit
- Unterstützt bei der Einhaltung regulatorischer Anforderungen (z.B. NIS2, DORA)
- Kommunikation und Unterstützung durch deutschsprachige Experten
- Optional Forensik & Incident Management on demand (AIR)
- Optimal mit TopMDR SIEM kombinierbar



Alert →



24x7 TOPMDR SOC

| TopMDR SOC ¹⁾ | Einrichtungskosten einmalig | Preis pro Monat |
|---|-----------------------------|-----------------|
| TopMDR SOC Basis | auf Anfrage | auf Anfrage |
| Asset Full Node; Preis pro Asset ²⁾ | -- | auf Anfrage |
| Asset Light Node, Preis pro Asset ²⁾ | -- | auf Anfrage |
| Incident Handling durch conova Experten ³⁾ | -- | Stundenkonto |

TopMDR SOC – Erweiterungen (Auszug)

| | | |
|---|--------------|-------------|
| Servicemeeting monatlich/quartalsweise | Stundenkonto | -- |
| Advanced Incident Response (AIR) Onboarding | auf Anfrage | -- |
| Advanced Incident Response pro Node | -- | auf Anfrage |
| TopMDR SOC Expert pro Tag | auf Anfrage | -- |
| TopMDR SOC Incident Responder pro Tag | auf Anfrage | -- |
| TopMDR SOC AIR Vor-Ort-Einsatz | auf Anfrage | auf Anfrage |

¹⁾ SLA First Class (24x7) inklusive. Weitere Informationen entnehmen Sie bitte dem Datenblatt TopSLA. Dieses erhalten Sie auf Anfrage.

²⁾ Full Node: Aktive Überwachung, Analyse & Alarmierung | Light Node: Keine Use Cases, keine Alarmierung, reaktive Nutzung der Daten bei der Analyse.

³⁾ Leistungen im Bereich Incident Handling werden ausschließlich für Managed Services von conova erbracht.

Hinweise:

- Mindestvertragslaufzeit von 36 Monaten.

