

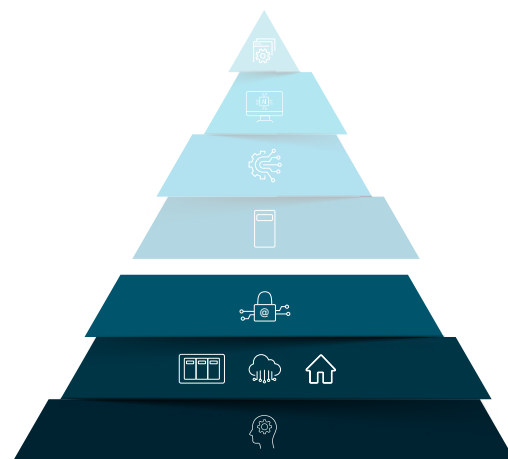
# TOPMDR SIEM DEDICATED

IHRE SKALIERBARE UND SICHERHEITSKONFORME SIEM-ARCHITEKTUR

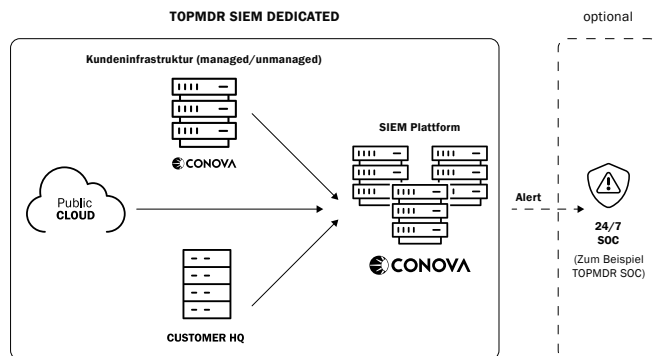
Mit TopMDR SIEM dedicated erhalten Sie eine gemanagte SIEM-Plattform (Security Information and Event Management) für Ihr Unternehmen, die in den conova Rechenzentren betrieben wird. Die Lösung kombiniert Endpoint-Überwachung in Echtzeit mit einer strukturierten Incident-Response-Plattform. Alle erkannten Abweichungen werden zentral zusammengefasst, dokumentiert und können an ein SOC (Security Operations Center wie TopMDR SOC) weitergegeben werden bzw. stehen als Reports für Audits und Zertifizierungen zur Verfügung.

## Highlights im Überblick

- Datenhoheit: Speicherung und Verarbeitung ausschließlich in Österreich
- Echtzeit-Überwachung von Endpunkten durch Log-Auswertung und CVE-Scans
- Identifikation von Schwachstellen in der Infrastruktur (CIS-Benchmark)
- Bereitstellung einer SIEM Lösung für die Nutzung durch TopMDR SOC oder ein unternehmenseigenes SOC
- Optional: Gemeinsame Clearingphase mit Einsatz von Best Practices für ein ideales Setup der SIEM-Lösung
- Optional: Betrieb On-Premises oder in einer Public Cloud möglich



TopMDR SIEM dedicated überwacht Endpoints wie Server, Clients sowie Netzwerk-Infrastruktur (z. B. Switches und Firewalls). Diese können On-Premises, in den conova Rechenzentren (unmanaged & managed Services) oder in Public Clouds (z. B. Microsoft Azure/M365, AWS, GCP) betrieben werden. Die erfassten Daten werden an die SIEM-Plattform übermittelt und dort analysiert. Unterstützt werden auf Client-Seite die Betriebssysteme Windows, Linux und macOS. Die von der Plattform generierten Alerts werden optional an ein SOC weitergeleitet.



TopMDR SIEM dedicated <sup>1)</sup>	S	M	L
Deployment	Single-Node	Dual-Node	Multi-Node+Cluster
Asset Monitoring (Empfehlung)	bis zu 100 Assets	bis zu 1.000 Assets	ab 1.000 Assets
Logspeicher inkludiert	100 GB	150 GB	1.500 GB
Preis pro Monat	auf Anfrage	auf Anfrage	auf Anfrage
Einrichtungskosten einmalig	auf Anfrage	auf Anfrage	auf Anfrage
<b>TopMDR SIEM – Erweiterungen (Auszug)</b>			
Erweiterung des Speicherkontingents pro 100 GB	auf Anfrage	auf Anfrage	auf Anfrage

<sup>1)</sup> SLA Economy inklusive, SLA Business und First Class (24x7) optional. Weitere Informationen entnehmen Sie bitte dem Datenblatt TopSLA. Dieses erhalten Sie auf Anfrage. Hinweise:

- Die Standard-Speicherung der Logdaten beträgt bis zu 3 Monate. Eine abweichende Dauer der Log-Speicherung kann in Abstimmung individuell vereinbart werden.
- Mindestvertragslaufzeit von 36 Monaten.
- Für Kunden, die aktuell noch keinen Managed Service von conova beziehen, ist für die Nutzung des Dashboards eine Verbindung über VPN oder statische IP-Freischaltung des Kunden erforderlich.
- Gemeinsames Onboarding, Alertclearing, Ticketsystemintegrationen oder Optimierungen des SOC-Betriebs können über das Stundenkonto dazu gebucht werden.

Weitere Optionen finden Sie in unserer aktuellen Preisliste.

