

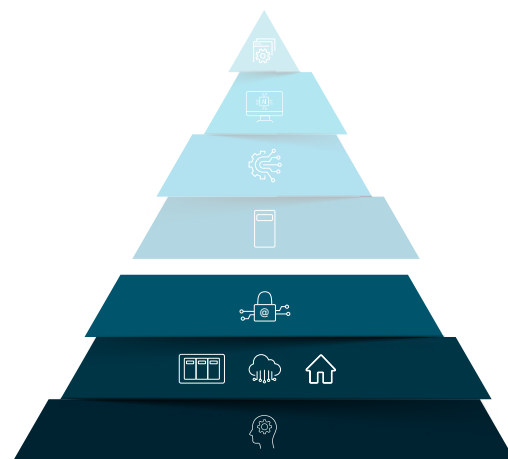
TOPMDR SIEM DEDICATED

YOUR SCALABLE AND SAFETY-COMPLIANT SIEM-ARCHITECTURE

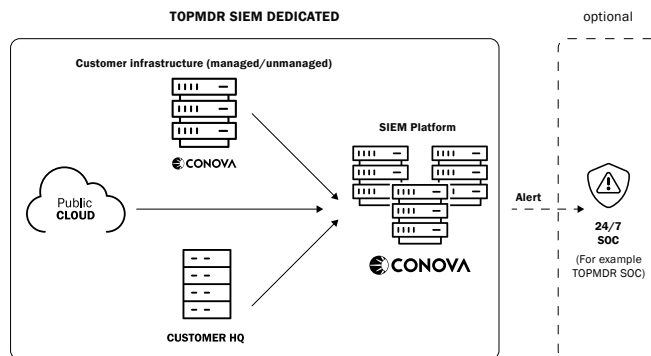
With TopMDR SIEM dedicated you receive a managed SIEM platform (Security Information and Event Management) for your company that is operated within conova's data centers. The solution combines real-time endpoint monitoring with a structured incident response platform. All detected anomalies are centrally consolidated, documented and can then be forwarded to a SOC (Security Operations Center, such as TopMDR SOC). In addition they are available in the form of reports for audits and certification purposes.

Highlights at a glance

- Data sovereignty: Storage and processing exclusively within Austria
- Real-time endpoint monitoring via log analysis and CVE scanning
- Identification of infrastructure vulnerabilities based on CIS Benchmarks
- Provision of a SIEM solution for use by TopMDR SOC or your company's own Security Operations Center (SOC)
- Optional: Joint tuning and optimization phase using best practices to achieve an optimal SIEM setup
- Optional: Deployment on-premises or within a public cloud environment



TopMDR SIEM dedicated monitors endpoints such as servers, clients and network infrastructure components (e.g., switches and firewalls). These systems may be operated on-premises, in conova data centers (unmanaged and managed services), or in public cloud environments (e.g., Microsoft Azure/M365, AWS or GCP). Collected data is transmitted to the SIEM platform, for analysis. On the client side, the platform supports Windows, Linux and macOS operating systems. Alerts that are generated by the platform can optionally be forwarded to a SOC.



TopMDR SIEM dedicated ¹⁾	S	M	L
Deployment	Single-Node	Dual-Node	Multi-Node+Cluster
Asset Monitoring (recommendation)	up to 100 Assets	up to 1.000 Assets	from 1,000 Assets
Log storage included	100 GB	150 GB	1,500 GB
Price per month	upon request	upon request	upon request
Set-up costs (one-time expense)	upon request	upon request	upon request
TopMDR SIEM – extensions (excerpt)			
Increase in storage quota per 100 GB	upon request	upon request	upon request

¹⁾ SLA Economy included, SLA Business and First Class (24/7) optional. For more information, please refer to the TopSLA datasheet. It is available upon request.

Notes:

- Log data is stored for up to three months by default. Alternative retention periods can be agreed upon individually.
- Minimum contract period of 36 months.
- For customers who are not currently using a conova Managed Service, access to the dashboard requires either a VPN connection or whitelisting of the customer's static IP address.
- Joint onboarding, alert tuning and validation, ticketing system integrations and SOC operational optimizations can be booked via the service hours account.

Further options can be found in our current price list.

