



IT Security



Managed SOC Service

Detection & Prevention für mehr IT-Sicherheit

Cyberangriffe stellen laut Allianz Risk Barometer 2023 die größte Bedrohung für Unternehmen dar. Ein Ransomware-Angriff kann die gesamte Produktion zum Stillstand bringen. Um dieser Gefahr angemessen zu begegnen, reichen übliche Sicherheitsvorkehrungen nicht mehr aus. Raffinierte Attacken lassen sich erst entschärfen, wenn sie durch eine leistungsfähige Sensorik erkannt worden sind. Ein Security Operation Center (SOC) erfüllt die höchsten Anforderungen an Ihre IT-Security.

Hauptmerkmale und Vorteile

Bei einem Managed SOC Service kümmern sich erfahrene IT-Experten 24/7 um Ihre Cybersicherheit. So können Sie sich auf Ihr Kerngeschäft konzentrieren.



Sichtbarkeit und Transparenz

Sie schaffen Sichtbarkeit und Transparenz in Ihrer IT-Infrastruktur hinsichtlich IT-Sicherheit.



Angriffsflächen reduzieren

Sie reduzieren die Angriffsflächen für Cyberkriminelle, Saboteure und Spione im hohen Maße.



Reaktionsgeschwindigkeit erhöhen

Sie verkürzen die Zeit bis zum Erkennen von potenziellen Angriffen und können angemessen reagieren.

Die Modul-Angebote im Überblick

Leistungsmodul	Basis	Business	Optimal
Einrichtung und Betrieb SIEM	✓	✓	✓
Lizenzen für die Laufzeit	✓	✓	✓
2nd Level Support & Ticketing	✓	✓	✓
Unterstützte Logquellen	Firewalls, Webfilter, User-VPN-Einwahlsysteme, Active Directory & Entra ID, DNS	Basis + WAF, EDR, PKI, Exchange & Exchange Online, Fileserver, DHCP	Business + Individuelle Logquellen
Logquellen	X Systeme	X Systeme	X Systeme
Anzahl Use Cases (Reports oder Alarme)	10	15	15 (erweiterbar)
Events pro Sekunde (EPS)	750 EPS inklusive (erweiterbar)	1000 EPS inklusive (erweiterbar)	1500 EPS inklusive (erweiterbar)
Aufbewahrungszeitraum	30 Tage (erweiterbar)	60 Tage (erweiterbar)	90 Tage (erweiterbar)
Zugang zum Dashboard	3 User Inklusive	3 User Inklusive	3 User Inklusive
Alarmierung kritischer Alarme	10x5 (24x7 Optional)	10x5 (24x7 Optional)	10x5 (24x7 Optional)
Monatliches Threat Hunting	✗ zubuchbar	✗ zubuchbar	✗ zubuchbar
Service Manager	✓	✓	✓
Servicemeeting	jährlich	halbjährlich	quartalsweise

Schutz vor Angriffen 24/7 – sicher, verlässlich und datenschutzkonform

Der Managed SOC Service enthält:

- Cyber Security Monitoring
- Alerting & Reporting
- Service Management
- Incident Response (individuelle Vereinbarung)

Unsere Lösung ermittelt kritische Zustände, die von Bordmitteln nicht erfasst werden können. Sie haben die volle Transparenz über die Abläufe im Netzwerk. Wir haben Ihr Interesse geweckt? Dann kontaktieren Sie uns unter sales@medialine.ag.

Änderungen und Irrtümer vorbehalten. Es gelten unsere allgemeinen Geschäftsbedingungen in der jeweils aktuellen Fassung. Die Produktbeschreibung stellt noch kein verbindliches Angebot dar und dient ausschließlich der Information. Vertragsdetails sind aus Angeboten und Leistungsverzeichnissen zu entnehmen, welche wir gerne für Sie erstellen. Stand: 02/2025