

SOC-as-a-Service



Cyberangriffe früher erkennen, Risiken reduzieren und Ihre IT rund um die Uhr schützen.

Cyberangriffe kennen keine Geschäftszeiten. Mit OEDIV SOC-as-a-Service erhalten Unternehmen ein rund um die Uhr aktives Security Operations Center (SOC) zur kontinuierlichen Überwachung und Analyse sicherheitsrelevanter Ereignisse. Sicherheitsereignisse aus Microsoft Sentinel oder CrowdStrike Falcon werden durch erfahrene Analysten bewertet, priorisiert und nachvollziehbar eskaliert. Der Service wird dabei auf der bestehenden Plattform des Kunden betrieben. Der Tenant verbleibt beim Unternehmen, sodass die Datenhoheit jederzeit gewahrt bleibt. Der Service eignet sich für Unternehmen, die ihre IT- und Security-Teams entlasten, Bedrohungen früher erkennen und ihre Reaktionsfähigkeit erhöhen möchten.



Ihr Ergebnis: Wenn OEDIV SOC-as-a-Service im Einsatz ist, werden sicherheitsrelevante Ereignisse kontinuierlich überwacht, fachlich bewertet und mit klaren Handlungsempfehlungen an die richtigen Ansprechpartner eskaliert. Kunden sparen Zeit und Aufwand, weil Warnmeldungen nicht mehr isoliert und manuell durch interne Teams bewertet werden müssen. Automatisierung und standardisierte Prozesse beschleunigen die Bearbeitung und schaffen ein skalierbares Sicherheitsmodell, das mit den Anforderungen des Unternehmens wachsen kann.

24/7 Security Monitoring:

OEDIV überwacht relevante Sicherheitsereignisse 24 Stunden am Tag, 365 Tage im Jahr. So entsteht ein kontinuierlicher Blick auf Bedrohungen, auch außerhalb regulärer Geschäftszeiten.

Erfahrene Analysten statt Alarmflut:

Sicherheitsmeldungen werden nicht nur gesammelt, sondern durch Security-Experten bewertet, priorisiert und bei Bedarf eskaliert. Das reduziert Fehlalarme und schafft Orientierung im Ernstfall.

Automatisierung und klare Prozesse:

Standardisierte Abläufe und intelligente Automatisierung unterstützen eine schnellere Bewertung und Weiterleitung sicherheitsrelevanter Ereignisse. Dadurch werden interne IT-Teams entlastet und Reaktionszeiten verbessert.

Technologieoffenes Betriebsmodell:

Der Service kann mit Microsoft Sentinel oder CrowdStrike Falcon betrieben werden. Bestehende Investitionen bleiben nutzbar, während das Betriebsmodell flexibel weiterentwickelt werden kann.

Skalierbare Leistungsklassen:

Mit Gold und Platinum wählen Kunden das passende Servicelevel – vom standardisierten Security Monitoring bis zur erweiterten Analyse und individuellen Unterstützung.

Unsere Handlungsempfehlung

- Relevante Datenquellen und Security-Plattform werden im Onboarding angebunden.
- Sicherheitsereignisse laufen im SOC zusammen und werden automatisiert vorqualifiziert.
- Analysten bewerten Auffälligkeiten, priorisieren Risiken und prüfen den Kontext.
- Bei bestätigtem Handlungsbedarf erfolgt eine nachvollziehbare Eskalation mit konkreter Empfehlung.
- Im Betrieb kann der Service über Leistungsklassen, zusätzliche Datenquellen und individuelle Unterstützung erweitert werden.

So wird aus technischer Alarmierung ein belastbarer Sicherheitsprozess mit klarer Verantwortung und schnellerer Reaktion.

Leistungsklassen: Gold und Platinum

Technologievarianten: Microsoft Sentinel oder CrowdStrike Falcon

Kernbestandteile: 24/7 Monitoring, Alarmbewertung, Priorisierung, Eskalation, Handlungsempfehlungen

Optionale Erweiterungen: zusätzliche Datenquellen, erweiterte Analyse, individuelle Unterstützung, kundenspezifisches Onboarding

Verwandte Services: Endpoint Security, Zscaler, Remote Managed Firewall, Managed Public Cloud Data Platform

Wir beraten Sie gerne zu unseren umfangreichen und ergänzenden Services!



OEDIV – IT-Security



IT Security Services schützen Unternehmen mit skalierbaren Managed-Security-Leistungen, klaren Prozessen und technologieoffenen Lösungen – für mehr Resilienz, Transparenz und Handlungsfähigkeit.



Mehr zu unseren Lösungen
im Bereich IT-Security
→