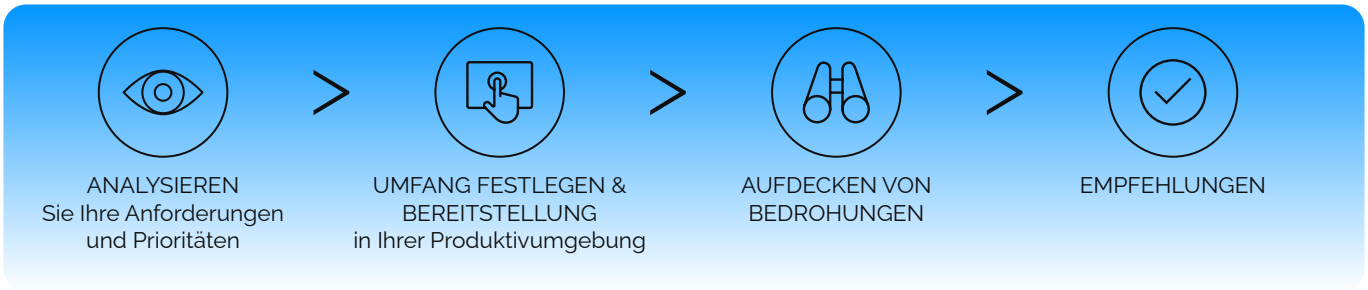
Microsoft Partner | Gold Security

Microsoft Sentinel
Value Insights

Mit unserer **Value Insights Methodik** zeigen unsere Experten Ihnen die Mehrwerte der eingebetteten Sicherheitslösungen Ihrer Microsoft Cloud Umgebung.



Im Leistungsumfang

- Bereitstellung von M365-Testlizenzen
- Konfiguration der M365-Sicherheits-tools entsprechend des Standard-leitfadens für Value Insights
- Aufdecken aktiver Bedrohungen für die Kundenumgebung
- Zuordnung entdeckter Bedrohungen zu empfohlenen Schadensbegrenzungs-Methoden

Nicht im Leistungsumfang

- Incident Response
- PoC- oder Labor-Bereitstellung
- Tiefgreifende/forensische Analysen
- Konfiguration der M365-Sicherheits-tools über den Standardleitfaden für Value Insights hinaus

"Durch den Einsatz von Azure Sentinel, wurde der Zeitaufwand für das Vorfallmanagement und die Bearbeitung von Alarmen um etwa 50 Prozent reduziert."

Stuart Gregg, Leiter der Cybersicherheitsabteilung, ASOS

Mit der zunehmend strategischen Bedeutung der IT wächst insbesondere auch die Bedeutung der IT-Sicherheit. Lösungen zur Sicherheitsinformation und Ereignisverwaltung (SIEM), die für althergebrachte Umgebungen entwickelt wurden, können mit den Herausforderungen von heute nicht mehr Schritt halten - ganz zu schweigen von den ungeahnten Risiken von morgen.

Erkennen und stoppen Sie Bedrohungen, bevor sie Schaden anrichten - mit Microsoft Sentinel *Value Insights*.

Microsoft Sentinel liefert über das gesamte Unternehmen hinweg intelligente Sicherheitsanalysen, Informationen zu Bedrohungen und bietet eine integrierte Lösung für Erkennung, Alarmierung, Transparenz von Bedrohungen, proaktive Suche und Reaktion auf Bedrohungen.

Microsoft Dienste

- Microsoft Sentinel
- Azure Active Directory Identity Protection
- Defender for Office 365
- Microsoft Cloud App Security

Atos

Microsoft Sentinel *Value Insights*

ANALYSIEREN Sie Ihre Anforderungen und Prioritäten > UMFANG FESTLEGEN & BEREITSTELLUNG in Ihrer Produktivumgebung > AUFDECKEN VON BEDROHUNGEN > EMPFEHLUNGEN

Was Sie erwartet

Erkennen von Bedrohungen für Ihre Microsoft 365 Cloud- und On-Premises-Umgebungen in den Bereichen E-Mail, Identität und Daten.

Verstehen, wie Bedrohungen begegnet werden kann, indem aufgezeigt wird, wie Microsoft 365- und Azure-Sicherheitsprodukte helfen können, gefundene Bedrohungen zu entschärfen und davor zu schützen.

Empfehlungen zur Planung der nächsten Schritte und Bereitstellung von Informationen, um einen Business Case für eine Produktivbereitstellung von Microsoft Sentinel zu erstellen, einschließlich einer technischen Bereitstellungs-Roadmap.

Grober Zeitrahmen

Abgleich der Erwartungen, Abstimmen des Grobumfangs und der Zeitplanung. Analysieren Sie Ihre Anforderungen und Prioritäten für eine SIEM-Einführung.

Kick-Off, Konkretisieren des Umfangs und Einrichtung der relevanten Dienste in Ihrer Produktivumgebung.

Begrenzte Remote-Überwachung und proaktive Bedrohungssuche zur Erkennung von Angriffsindikatoren (2 Stunden/Woche).

in WOCHE 1
Vorbereitungs-gespräch &
Ihre Anforderungen, und Prioritäten

in WOCHE 2
Abstimmung und Einrichten der Umgebung

in WOCHE 2-4
Automatisierte Datensammlung
Bedrohungen aufdecken & Berichtserstellung

in WOCHE 5
Ergebnisse, Empfehlungen, nächste Schritte

Erkundung von Bedrohungen und Aufzeigen von Möglichkeiten zur automatisierten Reaktion.

Empfehlung der nächsten Schritte für eine Produktivimplementierung von Microsoft Sentinel.

Value Insights Highlights

- Verstehen Sie die Funktionen und Mehrwerte von Microsoft Sentinel.
- Erhalten Sie Einblick in Bedrohungen in den Bereichen E-Mail, Identität und Daten.
- Erstellen Sie einen definierten Bereitstellungsplan auf der Grundlage Ihrer Umgebung und Ziele.
- Verbessern Sie Ihr Verständnis für potenzielle Bedrohungsvektoren, sowie deren Priorisierung und Entschärfung.
- Entwickeln Sie mit uns gemeinsam Pläne und legen Sie die nächsten Schritte fest.

CT-220322-EM-Onepagers-Microsoft-Security-SENTINEL