Microsoft Security

MODERN SecOps ENGAGEMENT

Verschaffen Sie sich einen Überblick über Ihr Unternehmen aus der Vogelperspektive mit SIEM für eine moderne Welt

Da alles über Microsoft Sentinel läuft, haben wir den Zeitaufwand für das Fallmanagement und die Lösung von Warnmeldungen um etwa 50 Prozent reduziert."

-Stuart Gregg, Cyber Security Operations Lead, ASOS

Da die IT immer strategischer wird, nimmt die Bedeutung der Sicherheit täglich zu. Sicherheitsinformations- und Event-management (SIEM) Lösungen, die für die Umgebungen von gestern entwickelt wurden, können mit den Herausforderungen von heute nicht mehr Schritt halten – ganz zu schweigen von den ungeahnten Risiken von morgen.

Aus diesem Grund wurde Microsoft Sentinel entwickelt, ein vollständig Cloud-natives SIEM.

Erkennen und stoppen Sie Bedrohungen, bevor sie Schaden anrichten – mit einem Modern SecOps Engagement

Verschaffen Sie sich einen Überblick über alle erfassten Daten und erkennen Sie Bedrohungen durch Analyse und Threat Intelligence von Microsoft. Untersuchen Sie Bedrohungen mit künstlicher Intelligenz und suchen Sie nach verdächtigen Aktivitäten.

Verschaffen Sie sich in diesem Engagement einen Überblick über Microsoft Sentinel und erhalten Sie Einblicke in aktuelle Bedrohungen für Ihre Microsoft 365 Cloud- und On-Premises-Umgebungen.

Engagement Highlights

- Verstehen Sie die Funktionen und Vorteile von Microsoft Sentinel und der Unifed SecOps Plattform
- Verschaffen Sie sich einen Überblick über Bedrohungen aus den Bereichen E-Mail, Identität und Daten
- Verstehen, priorisieren und reduzieren Sie potenzielle Risiken
- Erstellen Sie einen Bereitstellungsplan auf der Grundlage Ihrer Umgebung und Ziele
- Entwickeln Sie mit uns gemeinsame Pläne und nächste Schritte

Wählen Sie den für Sie am besten geeigneten Ansatz

Da jedes Unternehmen anders ist, kann dieses Engagement an Ihr Umfeld und Ihre Ziele angepasst werden. Wir können eines von zwei Szenarien anbieten:

Analyse von Bedrohungen

Wenn Ihr Unternehmen daran interessiert ist, zu erfahren, wie Microsoft Sentinel in Ihr bestehendes SOC integriert werden kann, indem ein bestehendes SIEM ersetzt oder ergänzt wird, arbeiten wir mit Ihrem SecOps-Team zusammen und bieten zusätzliche Angebote, um es auf den neuesten Stand zu bringen.

Remote monitoring (optional)

Wenn Ihr Unternehmen nicht über ein eigenes Security Operations Center (SOC) verfügt oder wenn Sie einige Überwachungsaufgaben auslagern möchten, zeigen wir Ihnen, wie Swiss IT Security das Remote Monitoring und Bedrohungssuche für Sie durchführen kann.

Sources: Microsoft Data Security Index report / First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

Engagement Ziele

In diesem Engagement arbeiten wir mit Ihnen zusammen, um:

- **praktische Erfahrungen zu sammeln** praktische Erfahrungen zu sammeln und zu verstehen, wie Sie mit Microsoft Sentinel und der Unified SecOps Platform Bedrohungen erkennen und analysieren können. Lernen Sie, wie Sie Ihre Sicherheitsabläufe automatisieren können, um sie effektiver zu gestalten..
- **einen Überblick über Bedrohungen zu bekommen,** für Ihre Microsoft 365-, Azure-Clouds, und Ihre lokalen Umgebungen, in den Bereichen E-Mail, Identität, Endpunkte und Daten von Drittanbietern, um potenzielle Cyberangriffsvektoren besser zu verstehen, zu priorisieren und zu behandeln.
- **Ein Verständnis zu entwickeln,** wie Ihnen die Sicherheitsprodukte Microsoft Sentinel und Defender XDR dabei helfen können, Bedrohungen, die während des Zeitraums dieses Engagements gefunden wurden, zu behandeln und sich dagegen zu schützen.

Außerdem werden Sie je nach gewähltem Szenario auch:

Vorteile eines gemanagten SIEM erleben mit einem echten cloudbasierten SIEM, das von unseren Cybersecurity-Experten verwaltet und überwacht wird.

Praktische Erfahrungen sammeln ,und lernen, wie Sie mit Microsoft Sentinel Bedrohungen entdecken und analysieren, sowie Ihre Sicherheitsabläufe automatisieren können, um diese effektiver zu gestalten.

Was wir tun werden

Analyse Ihrer Anforderungen und Prioritäten für eine SIEM-Einführung und Definition von Erfolgskriterien

Definieren des Scopes und Bereitstellen von Microsoft Sentinel in der Produktions-umgebung mit Integration von Microsoft- und Nicht-Microsoft-Lösungen

Fernüberwachung* von Microsoft Sentinel-Vorfällen und proaktives Threat-Hunting zur Erkennung von Angriffsindikatoren

*optionale Komponente

Bedrohungen für On-Premises und Cloud-Umgebungen in den Bereichen E-Mail, Identität, Endgeräte und Daten von Drittan-bietern erkennen

Empfehlung für die nächsten Schritte und für eine produktive Einführung von Microsoft Sentinel und der Unified SecOps Plattform

Warum SITS

Wenn es um Sicherheit, Compliance und die Cloud-Transformation geht, brauchen Sie einen erfahrenen Partner.

Die digitale Transformation ist ein Erfolgsfaktor für jedes Unternehmen. Damit Sie die Chancen nutzen und Ihre Geschäftsziele erreichen können, bieten wir strategische und operative Beratung, damit Sie Risiken minimieren, Daten schützen und Compliance-Anforderungen einhalten können.