

Microsoft Sentinel Workshop

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

Workshop highlights



Verstehen Sie die Funktionen und Vorteile von Azure Sentinel



Verschaffen Sie sich einen Überblick über Bedrohungen in den Bereichen E-Mail, Identität und Daten



Verstehen, priorisieren und reduzieren Sie potenzielle Risiken besser



Erstellen Sie einen Bereitstellungsplan auf der Grundlage Ihrer Umgebung und Ziele



Entwickeln Sie gemeinsame Pläne und nächste Schritte

“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 Eventmanagement (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 vollständiges Cloud-natives SIEM.

Erkennen und stoppen Sie Bedrohungen, bevor sie Schaden anrichten – mit einem Microsoft Sentinel Workshop

Microsoft Sentinel liefert intelligente Sicherheitsanalysen und Bedrohungsdaten für das gesamte Unternehmen und bietet eine umfassende Lösung für die Erkennung von Warnungen, die Transparenz von Bedrohungen, die proaktive Suche und die Reaktion auf Gefahren.

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

Wählen Sie den für Sie am besten geeigneten Ansatz

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

Remote Monitoring

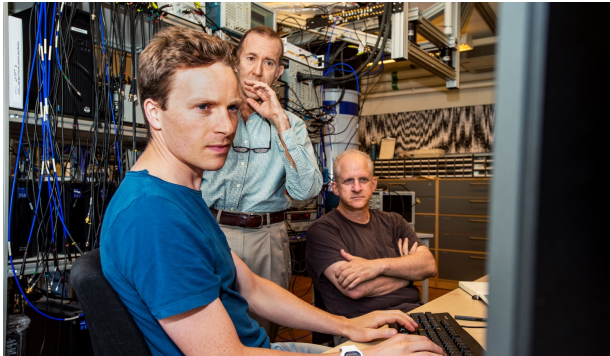
Wenn Ihr Unternehmen nicht über ein eigenes Security Operations Center (SOC) verfügt oder wenn Sie einige Überwachungsaufgaben auslagern möchten, zeigen wir Ihnen, wie Swiss IT Security das Remote Monitoring und Bedrohungssuche für Sie durchführen kann.

Gemeinsame Untersuchung von Gefahren

Wenn Ihr Unternehmen daran interessiert ist, zu erfahren, wie Azure 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.

Ziele des Workshops

In diesem Workshop werden wir mit Ihnen zusammenarbeiten, um:



- **Bedrohungen** für Ihre Microsoft 365 Cloud- und lokalen Umgebungen in den Bereichen E-Mail, Identität und Daten **zu entdecken**.
- aufzuzeigen, wie **Sie Bedrohungen reduzieren** und wie Microsoft 365- und Azure-Sicherheitsprodukte helfen können, gefundene Bedrohungen zu reduzieren und Sie zu schützen.
- **die nächsten Schritte** zu planen und Informationen zur Verfügung zu stellen, um einen Business Case für eine Produktionsbereitstellung von Azure Sentinel zu erstellen, einschließlich eines technischen Bereitstellungsplans.

Außerdem werden Sie je nach gewähltem Szenario auch:

die Vorteile eines gemanagten SIEMs mit einem echten cloudbasierten SIEM erleben, das von unseren Cybersecurity-Experten verwaltet und überwacht wird.
(Szenario Remote Monitoring)

praktische mitarbeiten und lernen, wie Sie mit Azure Sentinel Bedrohungen entdecken und analysieren und wie Sie Ihre Sicherheitsabläufe automatisieren können, um sie effektiver zu gestalten. (Gemeinsames Szenario zur Erforschung von Bedrohungen)

Was wir tun werden



Ihre Anforderungen und Prioritäten für eine SIEM-Einführung analysieren



Den Umfang definieren und Azure Sentinel in Ihrer Produktionsumgebung bereitstellen



Remote Monitoring* und proaktive Bedrohungssuche zur Erkennung von Angriffssindikatoren

*optionale Komponente



Bedrohungen entdecken und demonstrieren, wie Sie Antworten automatisieren können.



Empfehlung der nächsten Schritte für eine produktive Implementierung von Azure Sentinel

Warum Swiss IT Security?

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.