Azure Sentinel – die Microsoft SIEM- & SOAR-Lösung

Einrichtung von Azure Sentinel mit Sycor

Viele gesetzliche und industriespezifische Compliance-Richtlinien verpflichten Sie zu einem umfassenden Monitoring eigener On-Premises- und Cloud-Infrastrukturen, um Sicherheitsvorfälle zeitnah zu erkennen, zu melden und geeignete Gegenmaßnahmen zu ergreifen.

SIEM/SOAR-Lösungen werden diesen Anforderungen gerecht und schützen Ihre Infrastruktur gegen aktuelle Bedrohungen. Aktivieren Sie mit einer SIEM/SOAR-Lösung die Mittel für ein proaktives Cybersecurity-Management.

Das können Sie von uns erwarten

Schnelle Implementierung

des Azure Sentinels (SIEM/SOAR-Konzeptes) zum Festpreis.

Validierte Prozesse

zur artgerechten Nachverfolgung von Sicherheits-Vorfällen (Plattformübergreifend).

Hands-on Seminar

zur Analyse der Bedrohungsszenarien und den dazugehörigen Handlungsempfehlungen.

Eine Erweiterung Ihres Sicherheitspersonals

mit dem *Sycor.Managed Security*-Service.

Erweiterung der Best Practice-Security-Strategie

auf Ihren Cloud- & on-Premises-Systemen.

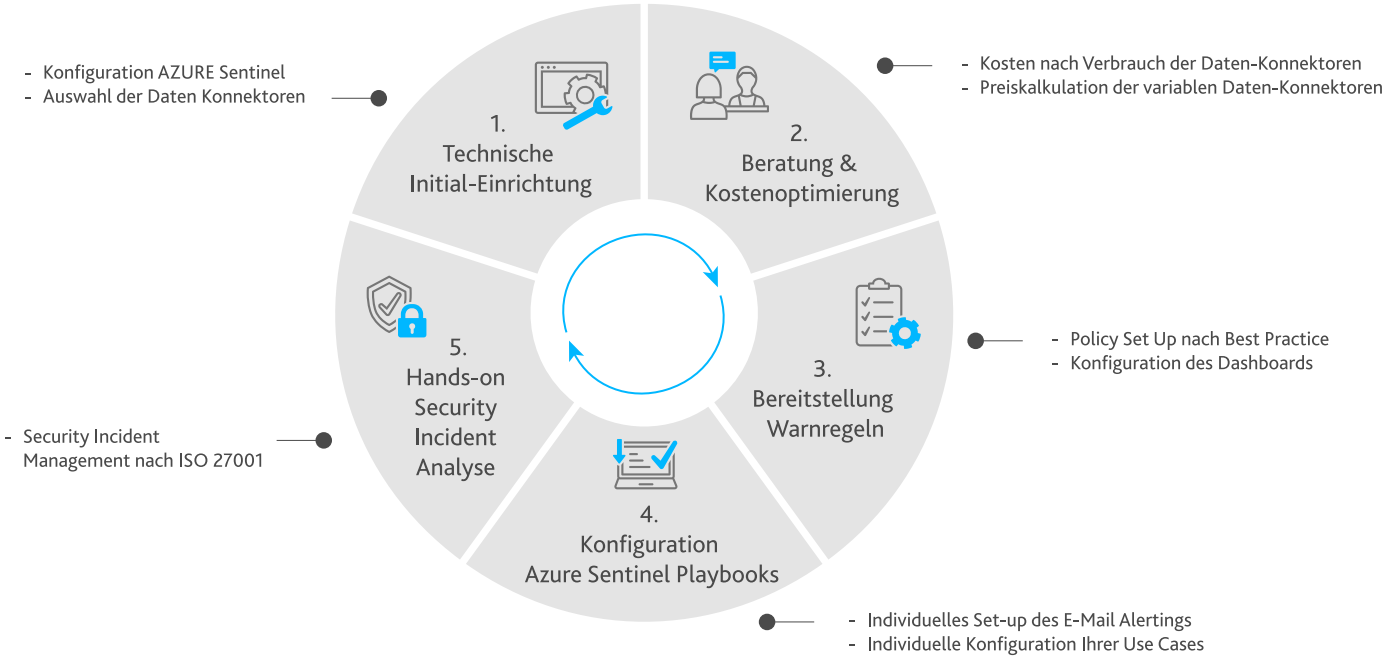
Transparente monatliche Kosten,

ausgerichtet an Ihrem Azure Konnektoren-Setup

Einrichtung von Azure Sentinel mit Sycor

Unser Expertenteam verfügt über umfangreiche Erfahrungen in der Bereitstellung von Azure Sentinel für ein breites Spektrum von Kunden, einschließlich in verschiedenen vertikalen Bereichen wie HealthCare & Life Sciences, Prozessindustrien und der Fertigungstechnik. Wir unterstützen Sie bei der initialen Bereitstellung von Azure Sentinel SIEM und erhalten sofort Einblicke in Ihre Sicherheitslage.

In der **technischen Initial-Einrichtung** erstellen und konfigurieren wir Azure Sentinel in Ihrem Tenant, verknüpfen den Dienst mit Ihrem Azure Abonnement (Subscription) und identifizieren mit Ihnen die wichtigsten Log-Datenquellen, die wir für eine sicherheitsrelevante Untersuchung mit einbeziehen. Wir beziehen uns hier auf unsere Best Practice-Empfehlungen und binden folgende Quellen mit ein: AAD, Azure Activity, Azure Security Center, Office 365 und ein 3rd Party On-Premises Konnektor Ihrer Wahl.



Beratung und Kostenoptimierung über volumenabhängige Daten Konnektoren. Preise und Abrechnung richten sich nach ausgewerteten Audit Logs über die Daten Konnektoren in Ihrem Azure Tenant.

Bereitstellung der Azure Sentinel-Warnungsregeln (Identifikation der Activity Rules) basierend auf den Azure Activity Rules und unseren Best Practice Erfahrungen. Wir stellen mit Ihnen die Sensitivität der Warnregeln für Ihre Unternehmensumgebung ein. Dabei legen wir besonderen Wert auf Ihren individuellen Nutzen der Benachrichtigung. Wir zeigen Ihnen, wie Sie die Warnregeln aus dem Dashboard interpretieren und daraus individuelle Maßnahmen für Ihre IT-Administration ableiten.

Konfiguration von Sentinel Playbooks: Ihre Use Cases im Alltag sind uns wichtig: Wir bilden Ihre individuellen Use Cases in der technischen Bereitstellung des Azure Sentinels ab und konfigurieren mit Ihnen ein angepasstes Alerting für Ihr Security-Team.

Hands On Security Incident Management: In Anlehnung an die ISO 27001 zeigen wir Ihnen, wie Sie bei Sicherheitsvorfällen in Ihrer Umgebung reagieren müssen. Festgelegte Meldewege und verschiedene Sofortmaßnahmen bilden hier zentrale Elemente, um ein proaktives Security Incident Management zu betreiben.

Wir geben IT ein Gesicht.

Wir freuen uns auf eine Zusammenarbeit!

Die Sycor steht ihren Kunden als erfahrener Partner zur Seite. Wir haben umfassendes Expertenwissen aus mehr als 20 Jahren IT-Projekten und Betriebserfahrung.

Sie profitieren von einem erprobten Vorgehensmodell, das wir gemeinsam mit unserem Partner Microsoft Deutschland erarbeitet haben auf Basis neuester Technologien und Tools.

Sprechen Sie uns an.

SYCOR GmbH
Heinrich-von-Stephan-Str. 1-5
37073 Göttingen
www.sycor.de

Geschäftführer: Thomas Ahlers, Stephan Reiss, Philip Hilgers, Ronald Geiger, Rüdiger Krumes
HR Göttingen HRB 3595

Jan Fahrenbach
Presales Consultant

jan.fahrenbach@sycor.de
+49 551 490 2520

17.12.2020