ACP

SIEM in a DAY

Mit dem SIEM in a Day Programm bekommen Sie eine schlüsselfertige Azure Sentinel Implementierung in Ihrem Azure Tenant. Dabei werden Best Practices beim Einrichten und Anbinden von definierten Datenquellen angewandt.
Sie selbst bestimmen, ob Sie unsere Expert*innen in Ihrem Tenant arbeiten lassen oder selbst das Steuer übernehmen und wir Ihnen dabei zur Seite stehen.

IT for innovators.

From Zero to SIEM

Konfiguration, Implementierung und Tuning nach Best Practices

Mit Azure Sentinel bekommen Sie eine moderne, agile und hoch flexible Lösung, welche über Automatisierung und KI Unterstützung Licht in Ihre Daten bringt. Sie können selbst oder durch unser ACP SOC Austria die weitere Analyse übernehmen, um Schaden von Ihrem Unternehmen abzuwenden. SIEM System und wir von ACP ermöglichen einen reibungslosen Start.

Provisionierung

Wir provisionieren Azure Sentinel in Ihrem Azure Tenant. Sie erhalten dabei eine schlüsselfertige Umsetzung von A-Z nach den Best Practices von ACP.

Anbindung der Datenquellen

Im Rahmen des SIEM in a Day Programms binden wir folgende Datenquellen an

- Azure AD
- Azure Audit
- Security Event Connector über Log Analytics
  Umsetzung für einen Server- Beispiel Domain Controller
- Optional: Azure AD Identity Protection
  Voraussetzung- Azure AD Premium 2 Lizenz

Umsetzen von Use Cases

Wir legen gemeinsam mit Ihnen manuell einen Use Case an, um Ihnen den Vorgang näherzubringen und importieren die weiteren Use Cases über Infrastructure as Code.

Visualisierung Ihrer Daten

Um die Daten des Systems zu visualisieren, werden folgende Workbooks deployed:

- Standard Workbooks aus den Connectoren
- Security Efficiency
- Data Connector Health

* Je nach Option und Umfang der Services für eine SIEM Implementierung variieren die Kosten ab 1.500€.

Microsoft

Ihre Optionen

1 SIEM-in-a-Day: SIEM implementieren und selbst betreiben

- ACP Durchführung und Teilnahme des Kunden in einem 1-Tages Remote Umsetzungsworkshop
- Wissenstransfer durch ACP Expert*innen
- Möglichkeit der Weiterführung durch den Kunden

2 SIEM hands-on implementieren und selbst betreiben

- Umsetzung in 2 Tagen durch den Kunden im eigenen Tenant unter Anleitung von ACP Expert*innen
- Größter Lernfaktor durch eigene Umsetzung
- Anleitung und geführte Umsetzung
- IaC (Infrastructure as Code) Deployment

Jetzt ab

€ 1.500,–*

(exkl. MwSt.)

Automatisierung

Über die integrierte SOAR Funktionalität lassen sich auf Basis von Use Cases Automatismen abbilden, um eine schnellstmögliche Reaktion auf Vorfälle zu gewährleisten. Wir implementieren einen beispielhaften Use Case in Ihrem Tenant.

Vorteile durch den Einsatz des SOC von ACP

Wir verfügen über ausgebildete Analyst*innen, welche für Sie die Erstanalyse und Bewertung von Vorfällen übernehmen und bei der Behandlung von Vorfällen durch priorisierte Maßnahmen unterstützen.

Darüber hinaus beraten Sie unsere SOC Consultants bei der Aufnahme neuer Datenquellen, erarbeiten Use Cases und unterstützen Sie beim Umgang mit Incidents.

Durch die Möglichkeiten von Azure Sentinel ist es uns auch möglich, Aktionen zu Automatisieren, um bei erkannten Vorfällen die Reaktionszeit auf ein Minimum zu reduzieren.

- Bewertung von Vorfällen
- Alert Triage und Beseitigung von False Positives
- Erstellen von umsetzungsfähigen und bewerteten Maßnahmen
- Beratung und Unterstützung

Wir bieten aus dem SOC auch Services in anderen Bereichen an, wie Vulnerability Management, Managed EDR auf Basis von Microsoft Defender for Endpoints sowie XDR auf Basis von Microsoft 365 Defender.

Mehr Information dazu finden Sie unter https://www.acp.at/soc

Starten Sie mit uns Ihre Reise in eine sichere IT Zukunft „in a Day“

* Je nach Art und Umfang der zu analysierenden Daten variiert der monatliche Preis des SOC Services..

Microsoft

Ihre Optionen

3 Full SOC Service: SIEM implementieren und als Full Managed SOC Service beziehen

- Erleben Sie die Vorteile von Azure Sentinel und die Analyse durch die Expert*innen des SOC der ACP, welche im Fall der Fälle die richtigen Schritte einleiten.
- Aufbau eines SIEM Systems nach Best Practices ohne Aufwand
- Voll lesender Zugriff auf die Daten
- Management und Analyse durch das SOC der ACP
- Dauer der Umsetzung
  6 Stunden- Remote Umsetzung & Dokumentation 6 Stunden-Service Onboarding

› **Laufende monatliche Kosten für das SOC Analyse Service im Umfang der beschriebenen Leistung**

Jetzt ab

€ 1.500,–*

(exkl. MwSt.)

Sie möchten mehr über unsere Security-Lösungen erfahren?
Dann wenden Sie sich bitte an:

security@acp.at
www.acp.at