ACP


# SIEM in a Day Premium

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

IT for innovators.

# From Zero to SIEM.

### Variante Premium: Konfiguration, Implementierung und Tuning nach Best Practices

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

### Anbindung der Datenquelle - Variante Premium

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

Alle Datenquellen der Basic- und Advanced Variante

- Azure AD
- Azure Audit
- Office 365
- Optional: Azure AD Identity Protection (Voraussetzung: Azure AD Premium 2 Lizenz)
- Advanced Datenquellen: Microsoft 365 Defender

Premium Datenquellen beinhalten beispielsweise:

- Firewall Systeme
- Endpoint Security
- Security Event Connector über Log Analytics
- und viele mehr nach Abstimmung

### 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

* Der Preis beinhaltet die Implementierung in der Variante Advanced und das Onboarding in das SOC der ACP. Ein reines Implementierungsangebot kann auf Anfrage erstellt werden.

## Ihre Optionen

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

- ACP Setup von Microsoft Sentinel in Ihrem Tenant und anschließender Einführungs-Workshop
- Wissenstransfer durch ACP Expert*innen
- Möglichkeit der Weiterführung durch den Kunden

**2** SIEM Hands-On implementieren und selbst betreiben.

- Sie führen die Umsetzung selbst, im eigenen Tenant, unter Anleitung von ACP Expert*innen durch
- Größter Lernfaktor durch eigene Umsetzung
- Anleitung und geführte Umsetzung
- IaC (Infrastructure as Code) Deployment
- Möglichkeit der Übernahme in ein fortlaufendes Analyse Service durch das SOC der ACP

**Jetzt ab**

**€ 7.000,-***

**(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.

## Fortlaufende Analyse durch das SOC der 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 Microsoft 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".**

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

Microsoft

# Ihre Optionen

**3** Microsoft Sentinel als Full Managed SOC Service beziehen

- Management und Analyse durch das SOC von ACP
- 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.
- Sie erhalten den vollen Lesezugriff
- Fortlaufende Anpassung zur Steigerung der Qualität

**Jetzt ab**

**€ 3.000,-***
**(exkl. MwSt.)**

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

**security@acp.at**
www.acp.at