all for one
Cybersecurity & Compliance

NATIVES SIEM AUS DER CLOUD

AZURE SENTINEL

Ereignisse und Bedrohungen auf Basis moderner Methodiken, in Verbindung mit der Skalierbarkeit der Cloud, schnell erkennen und effektiver untersuchen.

„Security is an ongoing battle". Effektives Security Monitoring sowie die frühzeitige Detektion und Reaktion auf Angriffe und Schadsoftware werden immer wichtiger. Es ist ein Wettlauf mit der Zeit: die wirklich wichtigen und bedrohlichen Ereignisse zu erkennen und abzuwehren ist, in immer größer werdenden IT/IoT-Landschaften, egal ob On-Premises oder in hybriden Cloud-Szenarien, eine echte Herausforderung geworden.

SecOps-Teams werden von einer riesigen Anzahl Warnungen und „False Positives" überflutet und sind außerdem mit dem Betrieb der Infrastruktur voll ausgelastet. Mit Azure Sentinel lässt sich dies ändern: ein Cloud-natives, KI-gestütztes SIEM, das Ereignisse und Bedrohungen auf Basis moderner Methodiken, in Verbindung mit der Skalierbarkeit der Cloud, schnell erkennt. Und Sicherheitsvorfälle lassen sich so effektiver untersuchen.

UNSERE DESIGNKRITERIEN FÜR EINE SECURITY MONITORING LÖSUNG (MANAGED ODER UNMANAGED)

Die primären Designkriterien für effektives Security Monitoring sind eine geringe Komplexität für den Kunden, dynamische Skalierung, Verfügbarkeit, Vertraulichkeit, Integrität, einfache Anbindung von Logquellen und ein transparentes Kostenmodell sowie Kosteneffizienz.

BEHANDELTE THEMENGEBIETE

- Compliance-Anforderungen des Kunden für Security Monitoring
- Generelle Anforderungen an die Infrastruktur und Lizenzen
- Besprechen der vorhanden Risikoanlyse des Kunden (BIA)
- Erfassen möglicher Logsourcen
- Ermitteln möglicher Use Cases
- Reporting
- Mögliche Betriebsmodelle
- Definition der Basisarchitektur

DER AZURE SENTINEL SIEM WORKSHOP

Initiale Entwicklung einer High-Level Designvariante und eines Architektur-Blueprints im Zuge des Azure Sentinel Workshops

ANGREIFER AKTIV DETEKTIEREN UND ANGEMESSEN REAGIEREN – IN IMMER GRÖSSER WERDENDEN IT/IOT-LANDSCHAFTEN EINE ECHTE HERAUSFORDERUNG. WIR UNTERSTÜTZEN SIE GERNE, EGAL OB ON-PREMISES ODER IN HYBRIDEN CLOUD-LANDSCHAFTEN.

PHILIPP HILGERS, SENIOR CONSULTANT
CYBERSECURITY & COMPLIANCE, ALL FOR ONE GROUP

IHRE VORTEILE

- Sie kennen die technischen und organisatorischen Grundlagen für das Design und den möglichen Betrieb von Azure Sentinel
- Die Anforderungen der Security Monitoring Lösung sind beschrieben in Bezug auf Unternehmen, IT-Organisation, Risiko und Compliance
- Sie erhalten eine High-Level Designvariante und einen Architektur-Blueprint
- Sie kennen die konkreten Schritte, um Azure Sentinel anzugehen, inklusive einer High-Level Timeline
- Übersicht der Kostenstruktur

UNSERE LEISTUNGEN

- Wissenstransfer über Azure Sentinel inklusive der Darlegung der Vor– und Nachteile
- Live-Demonstration: Simulierter Angriff und exemplarischer Incident Response-Prozess
- Sichtung der IST-Situation: IT-Organisation, Compliance-Anforderungen, IT-Landschaft, Risiken und Chancen
- Aufnahme bereits bekannter Anforderungen und strategischer Vorgaben
- Empfehlung des Betriebsmodells
- Ganztägiger Workshop, durchgeführt von einem erfahrenen Senior Security-Consultant als Basis für weitere konzeptionelle Ausarbeitung
- Beschreibung von Basis Use-Cases und die grobe Erfassung der risikoabgeleiteten kundenspezifischen Use Cases
- Besprechung eines möglichen Proof of Concepts (POC)
- Ausarbeitung eines Ergebnisdokuments mit individueller High-Level Designvariante und Architektur-Blueprint sowie Handlungsempfehlungen

all for one
Cybersecurity & Compliance

Gerne stehen wir Ihnen für ein
unverbindliches Gespräch zur Verfügung.

All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen

Experte kontaktieren
cc@all-for-one.com

cc.all-for-one.com