Microsoft Sentinel

Angesichts zunehmender Cyberbedrohungen sind SIEM- und SOAR-Systeme zu unverzichtbaren Instrumenten für Unternehmen und Organisationen geworden, die einen proaktiven und intelligenten Ansatz für Ihre IT-Sicherheit suchen. Microsoft Sentinel als cloudnative Lösung hilft beim Schutz vor externen Angriffen und bei der Einhaltung von Compliance-Richtlinien.

IT for innovators.

Microsoft Sentinel: SIEM- & SOAR aus Microsoft Azure

Unabhängig, ob Security oder Compliance sichergestellt werden müssen – manuell und ohne technische Hilfsmittel lässt sich die Bedrohungslage eines Unternehmens nicht mehr managen. Entsprechende Tools sind Security Information Management (SIEM) und Security Orchestration Automated Response (SOAR). Microsoft Sentinel vereint SIEM und SOAR und umfasst fortschrittliche Überwachungs- und Berichtsfunktionen. Indem Daten aus verschiedenen Quellen gesammelt werden, können Unternehmen Bedrohungsfälle rechtzeitig erkennen und angemessen reagieren.

So lassen sich einerseits mühelos Compliance-Anforderungen erfüllen, da die Unternehmensprozesse dank Sentinel nahtlos mit Branchenvorschriften und Datenschutzgesetzen in Einklang stehen. Andererseits erhöht sich durch den Einsatz von KI-gestützten Security-Tools der Schutz vor Cyberattacken.

Entlastung für Ihr IT Security Team

Durch die Automatisierung von Routineaufgaben und die Orchestrierung von Incident-Response-Prozessen ermöglicht Sentinel Ihrem IT-Sicherheitsteam, sich auf strategische Initiativen zu konzentrieren, die Reaktionszeiten zu verkürzen und die allgemeine Betriebseffizienz zu verbessern.

Integration von Microsoft Sentinel mit ACP

Wir bei ACP verfügen über umfassende Erfahrung in der Implementierung von Microsoft Sentinel. Gerne beraten wir Sie, wie die Integration am effizientesten gelingt – dabei profitieren Sie von unserem Best-Practice-Ansatz, den wir durch das Umsetzen einer Vielzahl von Projekten entwickeln konnten. Dieser gliedert sich in drei Schritte:

Wir stehen Ihnen bei der erstmaligen Einrichtung von Microsoft Sentinel zur Seite. So lassen sich diese Quellen schnell in eine Sicherheitsüberprüfung einbeziehen.

Ist-Analyse

Im ersten Schritt verschaffen wir Ihnen und uns Einblicke in den Sicherheitszustand ihrer Infrastruktur. Dazu analysieren und identifizieren wir die wichtigsten Datenquellen – egal ob On-Premises oder in der Cloud.

Technische Implementierung

Im Rahmen der initialen Einrichtung wird Microsoft Sentinel in Microsoft Azure bereitgestellt und die zuvor identifizierten Datenquellen bzw. Dienste über die verfügbaren Konnektoren verknüpft. Neben der initialen Anbindung der Dienste, werden die so gesammelten Alerts über ein Dashboard einsehbar gemacht.

Automatisierung

Umsetzung eines beispielhaften Playbooks zur Automatisierung eines Security-Prozesses.

Auf einen Blick

Dienstleistung

WIst-Analyse Ihrer Infrastruktur und Applikationslandschaft, Implementierung von Microsoft Sentinel, Automatisierung eines Security-Prozesses als Blaupause

Zielgruppe

CIOs, IT-Manager, Administratoren

Kosten

ab 3.000 €

Ihr Nutzen

- **Zentrale, KI-gestützte Security Plattform:** Sentinel ist in bestehende Microsoft 365 & Azure Umgebungen einfach integrierbar. Mithilfe von künstlicher Intelligenz reagiert die Lösung zudem schneller und smarter auf Bedrohungslagen und Events, als es mit herkömmlichen SIEM-Lösungen überhaupt möglich wäre.
- **Automatisierung:** Durch Playbooks lassen sich komplexe Worklows simpel automatisieren, was die Verwaltung erleichtert und zur besseren Übersicht beiträgt.
- **Integration:** Durch über 200 bereitgestellte Konnektoren lassen sich Cloud- aber auch On-Premises Dienste anbinden, so dass ein vollumfängliches Monitoring ihrer Umgebung sichergestellt wird.
- **Compliance & Reporting:** Durch umfassendes Monitoring der eigenen Infrastruktur (On-Premises und Cloud) erfüllen Sie durch den Einsatz von Microsoft Sentinel gesetzliche und industriespezifische Compliance-Richtlinien.

Einfach für Sie da

Sie möchten mehr über Microsoft Sentinel und SIEM sowie SOAR erfahren? Dann nehmen Sie Kontakt mit uns auf! Wir beantworten Ihre Fragen rund um unser Angebot und entwickeln für Sie ein solides Vorgehensmodell. ACP Holding Deutschland GmbH
Willy-Brandt-Platz 6
81829 München
microsoft@acp.de
www.acp-gruppe.com/de-de/partner/microsoft