MICROSOFT SENTINEL CONSULTING
WORKSHOP & PROOF OF CONCEPT

Unternehmen werden angegriffen. Fakt!

Um sich gegen Angreifer zu schützen, laufende Angriffe zu erkennen und Gegenmaßnahmen einleiten zu können, führen Unternehmen üblicherweise SIEM Systeme ein. SIEM Systeme sind Tools die Logdaten zusammenführen, analysieren und bei Auffälligkeiten Alarm schlagen.

In IT-Infrastrukturen die sich über Private Clouds, Public-Clouds, Containercluster, Multi- und Hybrid Clouds erstrecken, wird es für Unternehmen jedoch immer herausfordernder Angriffe zu erkennen. Oft fehlt es an den entsprechenden Tools. Oder es gibt zu viele davon, für jede Umgebung eins. Beides steht einer effektiven Angriffserkennung im Wege. Dazu kommen unterschiedliche Logformate, die alle manuelle vereinheitlicht werden müssen. Das bedeutet Aufwände und benötigt Ressourcen. Ressourcen, die üblicherweise knapp sind, seien es Budgets, personelle Ressourcen oder andere.

Die Antwort auf diese Herausforderungen ist Microsoft Sentinel.

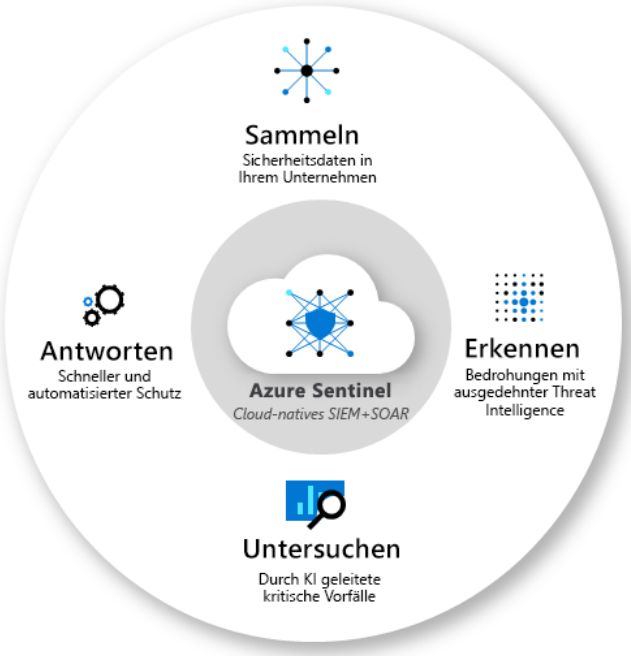

Abbildung 1 - Microsoft Sentinel strukturelle Übersicht

Microsoft Sentinel ist eine skalierbare, Cloud-native Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Microsoft Sentinel liefert intelligente Sicherheitsanalysen und Bedrohungsdaten für das gesamte Unternehmen und bietet eine integrierte Lösung für die Erkennung von Angriffen, die Erzeugung von Transparenz, die proaktive Suche und die Reaktion auf Bedrohungen.

Im Rahmen eines Workshops gemeinsam mit dem Kunden, gibt Computacenter einen Überblick über die Möglichkeiten, die sich mit einem Einsatz von Microsoft Sentinel ergeben.

Der Computacenter Service beinhaltet folgende Abschnitte:

Computacenter

- Anforderungsaufnahme
- Azure Sentinel Workshop
- Proof of Concept (PoC)
- Ergebnispräsentation

SERVICE DETAILS

Anforderungsaufnahme

Das primäre Ziel der Anforderungsaufnahme ist die vom Kunden gewünschten Ziele zu verstehen, die mit Azure Sentinel erreicht werden sollen. Ebenfalls im Fokus stehen aber auch die eventuellen Probleme, die der Kunde mit seiner aktuellen Lösung im Rahmen seiner Cloud Strategie erfährt. Es werden alle notwendigen Informationen ausgetauscht, um in dem zeitlich nachfolgenden Azure Sentinel Workshop optimal auf den Kunden und seine Bedürfnisse eingehen zu können.

Ziel des von Computacenter durchgeführten Workshops ist es dem Kunden einen Überblick über Microsoft Sentinel zu verschaffen und einen Einblick in aktive Bedrohungen in lokalen und Cloud-Workloads zu vermitteln.

Am Ende des Workshops wird der Kunde:

- ein besseres Verständnis der Funktionen und Vorteile von Microsoft Sentinel, einem cloudbasierten SIEM haben.
- Er wird potenzielle Bedrohungen, die während des Einsatzes gefunden wurden, besser verstehen, priorisieren und entschärfen können.
- Gemeinsam wurden die nächsten Schritte auf der Grundlage der Kunden Bedürfnisse und Ziele definiert.

Der halbtägige Workshop kann als Microsoft Teams Session oder vor Ort beim Kunden durchgeführt werden.

Proof of Concept

Es ist immer einfacher die Vorteile eines Produktes zu erkennen, wenn man dieser Live und in Farbe in seiner eigenen Umgebung in Aktion sieht. Der Proof of Concept kann nach dem durchgeführten Microsoft Sentinel Workshop gemeinsam mit dem Kunden gestartet werden.

Dabei ist das Ziel der PoC Phase ist die Erstellung und Konfiguration von Microsoft Sentinel im Kunden-Tenant, Die folgenden Punkte:

- Bereitstellen eines Microsoft Sentinel-Testabonnements im Kunden-Tenant, dass für die Speicherung der Daten und die Erstellung der für das Engagement erforderlichen Azure-Ressourcen erforderlich ist.
- Aktivieren von Microsoft Sentinel im Kunden-Tenant, einschließlich der Erstellung eines neuen dedizierten Azure Log Analytics-Arbeitsbereichs
- Einrichten einer dedizierten virtuelle Azure-Maschine (VM) mit Ubuntu Linux ein, die als Syslog-Agent für die Verbindung externer Datenquellen wie Netzwerk-Firewalls oder Proxy-Server im Kunden-Tenant fungiert
- Konfiguration einer im Workshop vereinbarten Microsoft Sentinel-Datenquellen (Konnektoren) im Kunden-Tenant.
- Erstellung einer im Workshop vereinbarten Microsoft Sentinel-Analyseregeln im Kunden-Tenant.
- Einrichtung einer im Workshop vereinbarten lokalen oder Cloud-basierte Quellen ein, um Protokolle an Microsoft Sentinel zu senden (direkt oder über die Syslog-Agent-VM).
- Konfiguration eines im Workshop vereinbarten Microsoft Sentinel-Automatisierungs-Playbooks und -Regeln im Kunden-Tenant.
- Konfiguration und Überwachung mit Microsoft Sentinel mit Microsoft Sentinel Workbooks.

Im Rahmen einer Ergebnispräsentation werden dem Kunden die von Microsoft Sentinel entdeckten Vorfälle vorgestellt, so das Computacenter dem Kunden die Verwendung, aber auch die Untersuchung und Reaktion vorstellen kann. Gemeinsam mit dem Kunden werden die nächsten notwendigen Schritte für einen produktiven Einsatz im Rahmen einer Roadmap vorgestellt.

WARUM COMPUTACENTER

Cloud ist mehr als eine IT-Plattform, Cloud ist ein Ökosystem. Computacenter beherrscht klassische IT Infrastrukturen UND Cloud Plattformen im Enterprise-Umfeld und ist damit der ideale Partner für Cloud-Transformationen bei Kunden

Wir bieten moderne Security-Konzepte für Multi- und Hybrid-Cloud Umgebungen wobei Zentralisierung administrative Aufwände minimiert und übergreifende Transparenz schafft. Wir vermitteln dabei zwiswchen der Security und anderen Abteilungen und begleitet Ende-zu-Ende von der Entwicklung von Sicherheitsvorgaben, über Produktauswahl und Implementierung bis zum Betrieb. Mittels Automatisierung beschleunigen wir Prozesse und implementieren Cloud-native und Third-Party Security-Lösungen mittels Security as Code.

Computacenter ist ein führender IT-Dienstleister in Europa, der Kunden und deren Anwender weltweit unterstützt. Unsere Mission ist es, Europas bevorzugter IT-Anbieter zu sein, und unser strategischer Schwerpunkt ist "Enable User and their Business in a Digital World". Wir bieten ein komplettes Portfolio an Dienstleistungen, von der Beschaffung und Optimierung von Technologie bis hin zu komplexen Transformationen und Managed Services.

Computacenter berät, liefert und integriert seit mehr als 20 Jahren Rechenzentrumslösungen und modernisiert und passt sich kontinuierlich den modernen IT-Anforderungen an. Heute deckt unser Data Center-Portfolio alle wichtigen Anforderungen ab und basiert auf dem zentralen Architekturdesign, dass die IT-Infrastruktur-Services über alle Assets des Unternehmens hinweg konsistent sein müssen - das reicht von On Premises - Private Cloud - bis hin zu Public Cloud und SaaS-Anwendungen.

Computacenter