4 Wege, um mit Microsoft Sentinel die wichtigsten IT-Sicherheitsbedenken zu lösen

Maximieren Sie die Vorteile und Fähigkeiten Ihrer Sicherheitsinvestition.

Insight Microsoft

Übersicht über die Bedrohungslandschaft

Die richtige Kombination von Tools, Technologien und Kompetenzen zu finden, ist entscheidend für die Führung eines erfolgreichen Security Operations Centre (SOC). Dies gilt insbesondere, da das Volumen der Cyberangriffe in letzter Zeit rapide zugenommen hat. Berücksichtigen Sie nun, dass die durchschnittlichen Kosten einer Ransomware-Attacke im Jahr 2021 4,62 Millionen USD betrugen.[1] Das sind viele potenzielle Schäden. Es ist also keine Überraschung, dass IT-Sicherheitsteams auf der ganzen Welt unter Druck stehen, die Reaktionszeit zu verbessern und zukünftige Verluste zu verhindern.

Um diesem sich entwickelnden Trend entgegenzuwirken, wird erwartet, dass Unternehmen im Jahr 2022 im Durchschnitt 24,4 Millionen US-Dollar für das IT-Sicherheitsbudget einplanen.[2] Diejenigen, die Daten on-premises und in der Cloud speichern möchten, müssen ihre bestehenden Lösungen neu bewerten, um eine vollständige Abdeckung über alle Betriebsstandorte, Home Offices, Kommunikationssysteme und überall dazwischen zu gewährleisten.

Das Wachstum von Endgeräten und Datenvolumen erfordert skalierbare Sicherheit.

Einzellösungen bieten einen begrenzten Umfang und bringen zusätzliche Herausforderungen bei der Integration.

Die Suche und Bindung wichtiger Sicherheitsexperten ist schwieriger geworden.

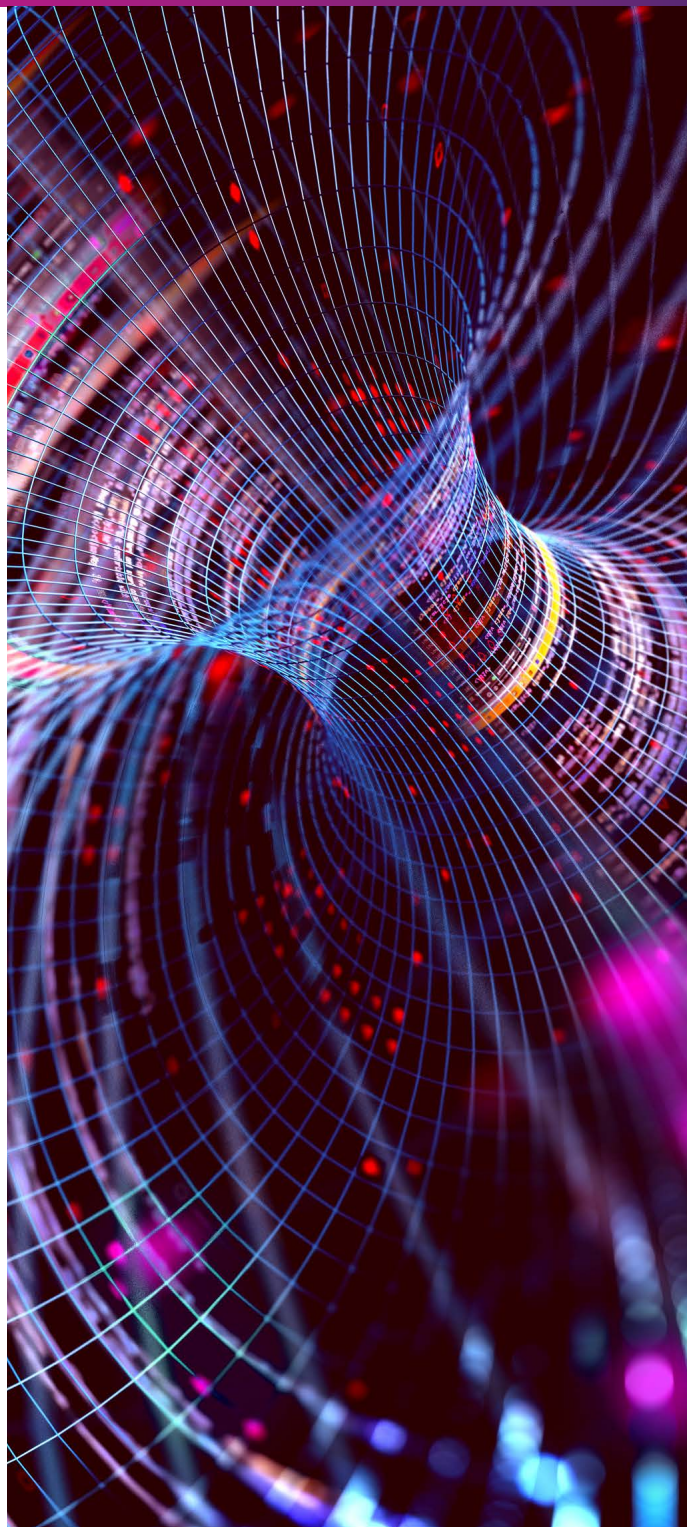
Die Komplexität von IT-Softwareumgebungen nimmt mit unzähligen Angriffsvektoren zu.

Denken Sie an Ihre Daten, Benutzer und Systeme.

Eine umfassende Transparenz ist von entscheidender Bedeutung, um potenzielle Schäden zu erkennen und zu vereiteln. Von einem einzigen Ausgangspunkt aus lassen sich mehrere Systeme angreifen und jemand kann die Kontrolle über die gesamte IT-Umgebung erlangen. Wenn es durchschnittlich 280 Tage dauert, bis Unternehmen einen Verstoß erkennen, kann eine unzählige Menge an Daten, Datensätzen und Systemen kompromittiert werden, bevor überhaupt Maßnahmen zur Bekämpfung des Eindringens ergriffen werden. Eine Möglichkeit, die Sichtbarkeit zu verbessern und dieses Hindernis zu reduzieren, ist die Implementierung von Identitäts- und Zugriffsmanagement. Wenn Unternehmen in der Lage sind, Trends im Benutzerverhalten zu verfolgen, um Muster aufzudecken, können sie das Zeitfenster für die Behebung von Problemen schließen und Schwachstellen beheben, die zuvor unbemerkt geblieben sind.

Bei der Implementierung von Identitäts- und Zugriffsmanagement sollten Sie sich die folgenden Fragen stellen:

- Wie sensibel sind Ihre Daten?
- Wer benötigt wirklich Zugriff auf bestimmte Dateien?
- Wann und wie lange wird der Zugriff benötigt?
- Müssen Sie ein Datenklassifizierungsprogramm initiieren?
- Haben Sie Benutzertypen festgelegt?
- Wann haben Sie die Berechtigungen zuletzt überprüft?
- Wie überprüfen Sie Identitäten und Zugriffspunkte?
- Welche Alternativen haben Sie zur Authentifizierung in Betracht gezogen?
- Wäre Biometrie eine lohnende Wahl?
- Haben Sie auffällige Lücken oder Muster bemerkt?
- Wie könnten Sie Ihren derzeitigen Ansatz auf einen sichereren umstellen?



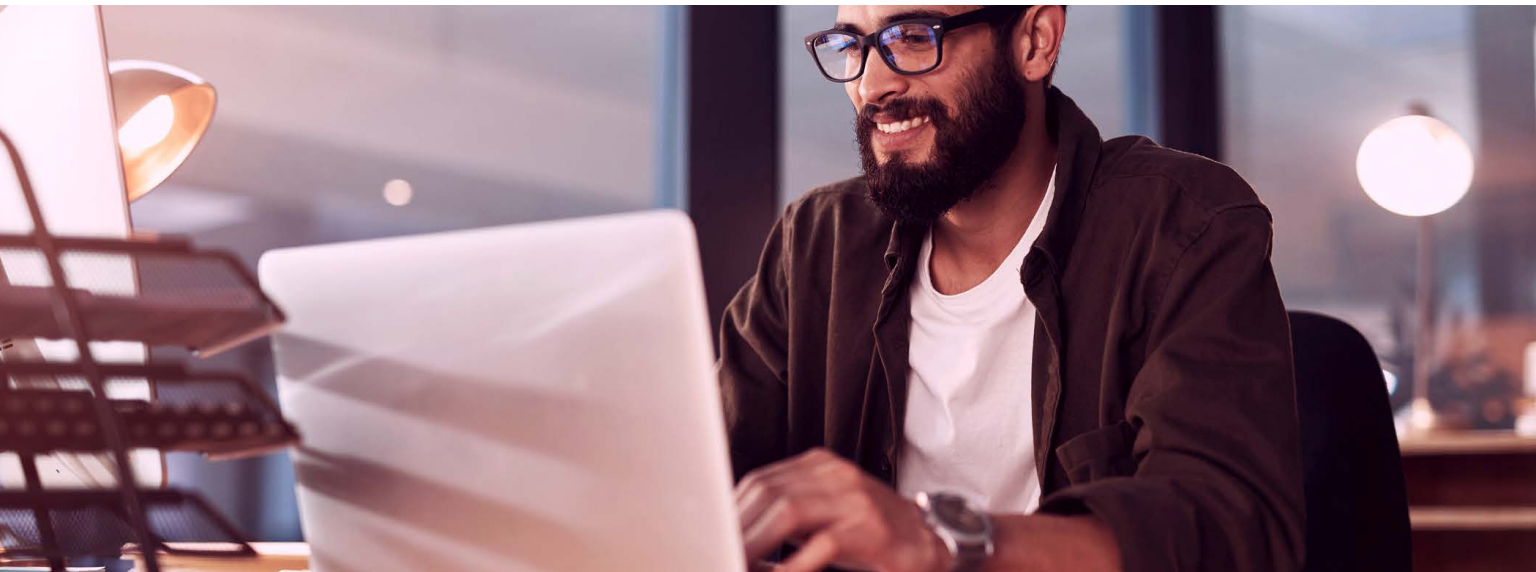
Die Voraussetzungen für ein modernes Sicherheitsprogramm

Dazu sollten Sie wissen, dass 89 % der Unternehmen bereits einen Multi-Cloud-Ansatz verfolgen oder planen.[4] Wenn Ihr Unternehmen zu dieser Mehrheit gehört, verfügen Sie möglicherweise über eine heterogene IT-Umgebung. Eine erfolgreiche Überwachung von Daten, bösartigen Hackern und mehr wird die Wirksamkeit der Präventionsmaßnahmen Ihres IT-Sicherheitsteams verbessern. Ein weiteres wichtiges Merkmal eines robusten Programms ist eine umfassende Governance, die sich mit Eigentum und Haftung befasst. Durch die Definition von Sicherheitszielen, Rollen und Prozessen können Unternehmen Richtlinien und Schulungen besser organisieren sowie Benutzer und Prozesse validieren.

Eine weitere Überlegung, die Sie im Hinterkopf behalten sollten, ist, dass 57 % der im Bericht „The State of IT Modernisation 2020" befragten Unternehmen angaben, dass die Aufrüstung der Sicherheitsinfrastruktur und -prozesse ein Haupthindernis bei der Modernisierung ihrer IT-Betriebsumgebungen darstellt.[3] Hier kann ein externer Partner durch Automatisierungsdienste einen Mehrwert bieten.

Die Automatisierung innerhalb des SOC bietet:

- Schnellere Erkennungs-, Reaktions- und Behebungsfunktionen
- Weniger Fehler und weniger „Alarmermüdung"
- Sicherheitsressourcen frei von sich wiederholenden Aufgaben
- Verbesserte Benutzererfahrung und -zufriedenheit



Investition in eine Cloud-native SIEM-Lösung

Microsoft Sentinel ist eine Cloud-native Lösung für Security Information and Event Management (SIEM) und Security Orchestration Automation and Response (SOAR), die als Cloud-Service bereitgestellt wird. Unternehmen, die die Fähigkeit nutzen, intelligente Sicherheitsanalysen für die gesamte Umgebung bereitzustellen, können Bedrohungen stoppen, bevor sie Schaden anrichten. Microsoft Sentinel ist eine skalierbare, immer verfügbare Lösung, die Ihre vorhandenen Sicherheitstools ergänzt oder ersetzt und Ihnen einen besseren Einblick in Ihre Bedrohungslandschaft verschafft.

- Verschaffen Sie sich einen Blick aus der Vogelperspektive in Ihrem gesamten Unternehmen.
- Optimieren Sie die Erkennung und Reaktion mit künstlicher Intelligenz (KI).
- Eliminieren Sie Einrichtung und Wartung der Sicherheitsinfrastruktur.
- Skalieren Sie, um sich entwickelnde Sicherheitsanforderungen zu erfüllen.

Als zusätzlicher Bonus senkt diese Lösung die Kosten um bis zu 48% und ist 67% schneller einsatzbereit als herkömmliche SIEMs.[5] Folglich können Unternehmen mehr Zeit damit verbringen, sich auf das schnelle Auffinden echter Bedrohungen zu konzentrieren, indem sie strategischere Sicherheitsabläufe kultivieren. Wie genau funktioniert es also? Wie nutzt sie KI und maschinelles Lernen, um Bedrohungen zu erkennen, zu analysieren und zu untersuchen? Wir werden uns auf der nächsten Seite näher mit dem vierstufigen Prozess befassen.

4 Schritte für Sicherheitsoperationen der nächsten Generation

1. Sammeln

Unternehmen speichern heute Dokumente, Daten, Aufzeichnungen und mehr auf einer Vielzahl von Geräten, Applikationen und Infrastrukturen, sowohl on-premises als auch in mehreren Clouds. Darüber hinaus können Benutzer praktisch jederzeit und von überall auf all diese sensiblen Dateien zugreifen. Microsoft Sentinel sammelt Daten im Cloud-Bereich und aggregiert Infrastruktur- und Sicherheitsgeräte wie Firewalls.

2. Erkennen

Regelmäßige Vorkommnisse und Muster von Cyberangriffen können Unternehmen dabei helfen, Bedrohungen zu erkennen. Analysen und Bedrohungsinformationen helfen Unternehmen sogar dabei, bisher nicht erkennbare Bedrohungen aufzudecken und die Wahrscheinlichkeit von Fehlalarmen zu minimieren. Stellen Sie sich vor, Sie könnten Millionen von Anomalien gleichzeitig überwachen und korrelieren und dann schnell Wert aus dem Bericht ziehen. Das ist es, was diese Lösung bietet.

3. Untersuchen

Microsoft Sentinel stützt sich auf die jahrzehntelange Erfahrung von Microsoft auf dem Gebiet der Cybersicherheit und jagt verdächtige Aktivitäten in großem Umfang mit Hilfe von KI – ohne Hardware oder virtuelle Maschinen. Es lernt aus täglichen Protokollen, wie man das Rauschen bewältigt, damit sich Sicherheitsteams auf die wesentlichen Signale konzentrieren können.

4. Antworten

Mit der integrierten Orchestrierung und der Automatisierung gängiger Aufgaben können Unternehmen schnell auf Vorfälle reagieren. Durch den Einsatz intelligenter Technologie spart Ihr IT-Sicherheitsteam nicht nur Zeit, sondern verbessert auch die Genauigkeit. Zum Beispiel können Playbooks, die durch Analysen oder Automatisierungsregeln ausgelöst werden, innerhalb von Microsoft Sentinel durchgeführt werden, um die Reaktionszeit zu optimieren und bösartige Akteure zu blockieren.

Warum Insight für Microsoft Sentinel?

Wir bei Insight glauben, dass es noch nie einen besseren Zeitpunkt gab, Ihre Sicherheitslage zu verbessern, insbesondere mit dem Aufkommen von Remote- und Hybrid-Arbeit. Verlassen Sie sich auf unsere jahrelange Erfahrung, um Ihr Unternehmen vor sich entwickelnden Cyberbedrohungen zu schützen. Gemeinsam helfen wir Ihrem Unternehmen, eine flexible, skalierbare Lösung zu erhalten, die modernste KI- und maschinelle Lernfunktionen nutzt. Das Ziel: verbesserte Sicherheit, Transparenz und Kontrolle Ihrer gesamten IT-Umgebung.

Wir sind ein Top-Partner von Microsoft und einer von nur 12 Partnern, die von Microsoft bezüglich der Konsultation und Bereitstellung von Microsoft Sentinel-Diensten öffentlich erwähnt werden:

- 18 Gold- und Silber-Kompetenzen von Microsoft
- Mehr als 25 Jahre als Microsoft-Partner
- Mehr als 1.000 auf Azure spezialisierte Consultants und Serviceexperten
- Ein Azure-Expert Managed Services Provider (MSP) und größter Azure-Partner
- Microsoft Security 20/20 Award-Gewinner für die Kategorie „Azure Security Deployment Partner of the Year“
- Support während der gesamten Lieferung/ Bereitstellung von Dienstleistungen

Über Insight

Insight Enterprises, Inc. ist ein Fortune-500-Lösungsintegrator mit 11.500 Mitarbeitern weltweit, der Unternehmen dabei unterstützt, ihre digitale Reise zu beschleunigen, ihr Unternehmen zu modernisieren und den Wert von Technologie zu maximieren. Wir ermöglichen eine sichere End-to-End-Transformation und erfüllen die Anforderungen unserer Kunden durch ein umfassendes Lösungsportfolio, weitreichende Partnerschaften und mehr als 33 Jahre an umfassender IT-Expertise. Wir wurden als der „Forbes World's Best Employer" eingestuft und als „Great Place to Work" zertifiziert. Wir erweitern unsere Lösungen und Dienstleistungen mit globalem Maßstab, lokaler Expertise und einem erstklassigen E-Commerce-Erlebnis und verwirklichen die digitalen Ambitionen unserer Kunden bei jeder Gelegenheit.

Insight®

ch.insight.com

Quellen:

[1] IBM Security. (2021). Kosten eines Berichts über Datenschutzverletzungen.

[2] Channel Futures. (Februar 2022). Die hohen Kosten von Ransomware.

[3] Insight. Der Stand der IT-Modernisierung 2020.

[4] Flexera. (März 2022). Bericht zum Stand der Cloud 2022.

[5] Forrester. (November 2020). Die Total Economic Impact™ von Microsoft Sentinel. Kosteneinsparungen und Unternehmensvorteile durch Microsoft Sentinel.

MKT6231