Insight®

Top Tipps für Sicherheitsumgebungen mit mehreren Anbietern

Ein Leitfaden zur Überwindung von Sicherheits-Burnout und zur Stärkung Ihrer Verteidigung mit Insight und Microsoft Sentinel

Sicherheit unter Stress

42%

der Befragten in der CISO Benchmark-Umfrage 2020 von Cisco geben an, dass sie unter Cybersecurity-Müdigkeit leiden (definiert als die Tatsache, dass sie die proaktive Verteidigung gegen bösartige Akteure praktisch aufgegeben haben).

93 % der Betroffenen erhalten täglich mehr als

5.000 Warnungen,

was darauf hinweist, dass Komplexität eine der Hauptursachen für ein Sicherheits-Burnout zu sein scheint.[1]

Zur Bewältigung einer komplexen Bedrohungslage setzen die meisten Unternehmen mehrere Sicherheitslösungen ein. Aber das Management und die Orchestrierung von Alarmen aus verschiedenen Quellen ist nicht nur eine Herausforderung, sondern setzt Unternehmen auch weiteren Risiken aus.

Eine zu große Anzahl von Alarmen bedeutet, dass es einfach zu viele sind, um sie zu bearbeiten. Das beeinträchtigt das Bewusstsein und die Sichtbarkeit des Teams und setzt das Unternehmen möglicherweise größeren, schädlicheren Bedrohungen aus.

Nach Ansicht von Fady Younes, Cybersecurity Director bei Cisco, „kann die fehlende Integration mehrerer Sicherheitslösungen auch zu Lücken bei der Abdeckung führen oder eine Situation schaffen, in der das IT-Team nicht richtig versteht, welchen Schutz eine bestimmte Lösung bietet oder wie sie funktioniert, was sich auf die Sichtbarkeit und das Bewusstsein für den tatsächlichen Sicherheitsstatus des Netzwerks auswirkt."[2]

In diesen IT-Landschaften wird weniger klar, welche Risiken und Warnungen priorisiert werden müssen.

Nicht alle Warnungen haben den gleichen Schweregrad, und die besten Sicherheitsstrategien passen die Sicherheitskontrollen an und weisen Ressourcen basierend auf dem Risikoniveau zu.

In heterogenen Multi-Cloud-Umgebungen wird die Notfallwiederherstellung unglaublich komplex und erfordert eine proaktive, gegenüber einer reaktiven, Sicherheitskultur.

„Der Umgang mit Integrationsproblemen und einer großen Menge an Sicherheitswarnungen kann Sicherheitsfachkräfte davon abhalten, andere Herausforderungen anzugehen..."

— **Fady Younes, Cybersecurity Director, Naher Osten und Afrika bei Cisco**

SIEM und SOAR

Sicherheitsteams müssen vor allem zwei Ziele verfolgen: Sie müssen wissen, was in ihren IT-Umgebungen vor sich geht, und sie müssen auf diese Informationen reagieren. Es gibt Lösungen für Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR), um diese Ziele zu erreichen.

SIEM-Tools sammeln und aggregieren Ereignisdaten aus verschiedenen Quellen innerhalb einer IT-Umgebung und analysieren und ordnen Ereignisse dann nach Priorität oder Wichtigkeit. Sicherheitsteams tragen die Verantwortung für die Bedrohungsjagd und -reaktion sowie für die Einstellung und Wiederherstellung der SIEM-Plattform.

SOAR-Tools bieten fortschrittliche Analysen und Automatisierung, die auf den Fähigkeiten von SIEM-Tools für eine autonomere Bedrohungsreaktion aufbauen. SOAR-Tools nutzen so viele Echtzeitdaten wie möglich und sind sensibel für die Kompetenz von Managern – diese Tools sind je nach Art ihrer Verwendung mehr oder weniger effektiv.

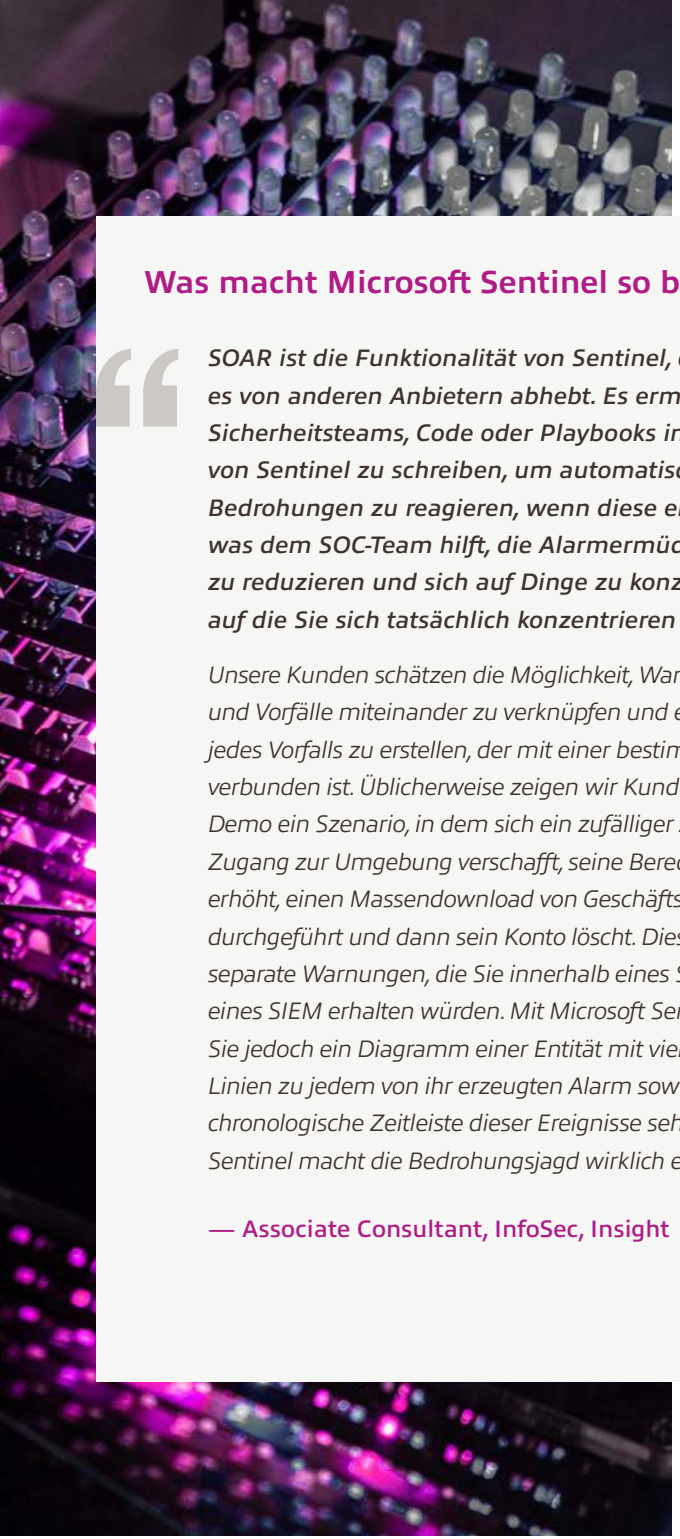
sagen, dass SOAR für die allgemeine Sicherheitslage ihres Unternehmens sehr oder extrem wichtig ist.

Wichtige Anwendungsfälle für SOAR:

- 65% SIEM-Triage
- 62% Phishing-Angriffe
- 62% Bedrohungsanalyse

Ergebnisse von SOAR-Bereitstellungen:

- Schnellere Behebung von Vorfällen
- Verbesserte Mitarbeitereffizienz
- Reduzierte Gesamtkosten[3]



Was macht Microsoft Sentinel so besonders?

SOAR ist die Funktionalität von Sentinel, die es von anderen Anbietern abhebt. Es ermöglicht Sicherheitsteams, Code oder Playbooks innerhalb von Sentinel zu schreiben, um automatisch auf Bedrohungen zu reagieren, wenn diese eintreffen – was dem SOC-Team hilft, die Alarmermüdung zu reduzieren und sich auf Dinge zu konzentrieren, auf die Sie sich tatsächlich konzentrieren müssen.

Unsere Kunden schätzen die Möglichkeit, Warnmeldungen und Vorfälle miteinander zu verknüpfen und eine Karte jedes Vorfalls zu erstellen, der mit einer bestimmten Entität verbunden ist. Üblicherweise zeigen wir Kunden in einer Demo ein Szenario, in dem sich ein zufälliger Angreifer Zugang zur Umgebung verschafft, seine Berechtigungen erhöht, einen Massendownload von Geschäftsdaten durchgeführt und dann sein Konto löscht. Dies sind vier separate Warnungen, die Sie innerhalb eines SOAR oder eines SIEM erhalten würden. Mit Microsoft Sentinel können Sie jedoch ein Diagramm einer Entität mit vier verschiedenen Linien zu jedem von ihr erzeugten Alarm sowie eine chronologische Zeitleiste dieser Ereignisse sehen. Microsoft Sentinel macht die Bedrohungsjagd wirklich einfacher."

— **Associate Consultant, InfoSec, Insight**

Das Argument für Microsoft Sentinel

Microsoft Sentinel™ kombiniert die Leistungsfähigkeit eines SIEM und eines SOAR in einer Lösung. Wenn Sie bereits in Microsoft® Sentinel investiert haben, sind Sie auf dem Weg zu mehr Sicherheit.

Die Sentinel-Plattform kann Ihnen helfen:

Identifizieren Sie Bedrohungen, bevor sie sich auf Ihr Unternehmen auswirken.

Reagieren Sie schnell und präziser.

Vereinfachen Sie die Sicherheit in Hybrid-, Multicloud-, serverlosen und anderen modernen IT-Umgebungen.

Senken Sie die Kosten gegenüber älteren SIEM-Lösungen für Bedrohungsuntersuchung, Lizenzierung, Storage, Infrastruktur, Management und Bereitstellung.

Das Tool basiert auf der umfassenden Erfahrung von Microsoft in Sachen Sicherheit und den neuesten Funktionen für künstliche Intelligenz und funktioniert harmonisch mit anderen Microsoft-Produkten. Es ist schnell einzurichten und einfach zu skalieren.

Ein Hub, viele Datenpunkte

Die Verwaltung von IT-Umgebungen mit Lösungen mehrerer Anbieter wird mit Microsoft Sentinel einfacher. Die Fähigkeit von Sentinel, Datenquellen aus dem gesamten Ökosystem von Sicherheitslösungen mehrerer Anbieter zu beziehen, bietet Unternehmen Transparenz und Kontrolle, um die Bedrohungsjagd zu vereinfachen, Alarmermüdung zu reduzieren und ein wahres Bild Ihrer Sicherheitslage zu erfassen.

Best Practices für die Implementierung

Die ersten Schritte mit Microsoft Sentinel sind relativ einfach. Vor der Implementierung empfehlen wir, klare Governance und Richtlinien festzulegen. Zu den Überlegungen gehören Compliance-Standards, Kostenanforderungen, Pläne für Storage, Notfallwiederherstellung, Personalbesetzung des Sicherheitsteams und Pläne zur Reaktion auf Vorfälle.

Tag 1:

Aktivieren Sie Microsoft Sentinel.

Verbinden Sie Datenquellen.

Beginnen Sie mit dem Erstellen von Abfragen, um die Daten zu untersuchen.

Wie viele andere SIEM-Tools dienen Syslog und CEF als Aufnahmepunkte. Sie können jede beliebige Linux®-Distribution verwenden, einschließlich Microsofts eigener Linux-Distribution, und CEF- und Syslog-Forwarder installieren, um Protokolle zur Erfassung an Microsoft Sentinel weiterzuleiten.

Microsoft hat Sentinel entwickelt, um generische Formatierungsprotokolle auch im gängigen Ereignisformat aufzunehmen, sodass sogar Protokolle von älteren oder spezialisierten Geräten integriert und analysiert werden können.

Sicher in allen Bereichen.

Die größte Wirkung entfaltet Microsoft Sentinel, wenn es Teil eines umfassenderen, systematischen Konzepts für Cybersicherheit ist. Stellen Sie sicher, dass Ihr Unternehmen über das gesamte Cybersicherheitsspektrum hinweg Best Practices einsetzt: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

INSIGHT LÖSUNG

Risiken mindern und Ihr Unternehmen schützen.

Insight verfügt über eine solide Sicherheitspraxis und ist am Puls der IT-Sicherheitslandschaft. Wir unterstützen Unternehmen seit mehr als 30 Jahren bei der Sicherung ihrer Daten und Netzwerke. Als eine Gruppe von Beratern, Lösungsanbietern und technischen Spezialisten halten wir die Zertifizierung und das Eintauchen in die neuesten Sicherheitstechnologien und Best Practices aufrecht.

Tag 2+:

Die Flexibilität und Dynamik der Plattform wird an dieser Stelle deutlich. Hier sind mehrere Möglichkeiten, wie Sie die Vorteile von Microsoft Sentinel für die spezifischen Anforderungen und das Risikoprofil Ihres Unternehmens erheblich optimieren können.

1.

Überprüfen Sie Ihre Protokoll-Forwarder.

Wenn Sie nicht genau auf den Zustand Ihres Log-Forwarders und die Kapazität Ihres VAR-Protokollverzeichnisses achten, kann es schnell zu einem Zusammenbruch kommen und die Aufnahme von Protokollen wird unterbrochen. Wenn die Berater von Insight Microsoft Sentinel implementieren, verwenden wir Linux-Distributionen mit einer vom Betriebssystem getrennten Partition für den VAR-Log-Mountpoint. Auf diese Weise wirkt sich die Speicherkapazität des Verzeichnisses nicht so stark auf das Betriebssystem aus.

2.

Sehen Sie sich Ihre Aufnahmeraten an.

Es ist schwierig, zu schätzen, wie viele Protokolle Sie am Anfang aufnehmen können – aber nach ein oder zwei Monaten werden Sie genügend historische Daten haben, um eine bessere Entscheidungsfindung bezüglich einer angemessenen Datenaufnahmerate zu unterstützen. Dies wird Ihnen helfen, ein besseres Kostenergebnis zu erzielen.

3.

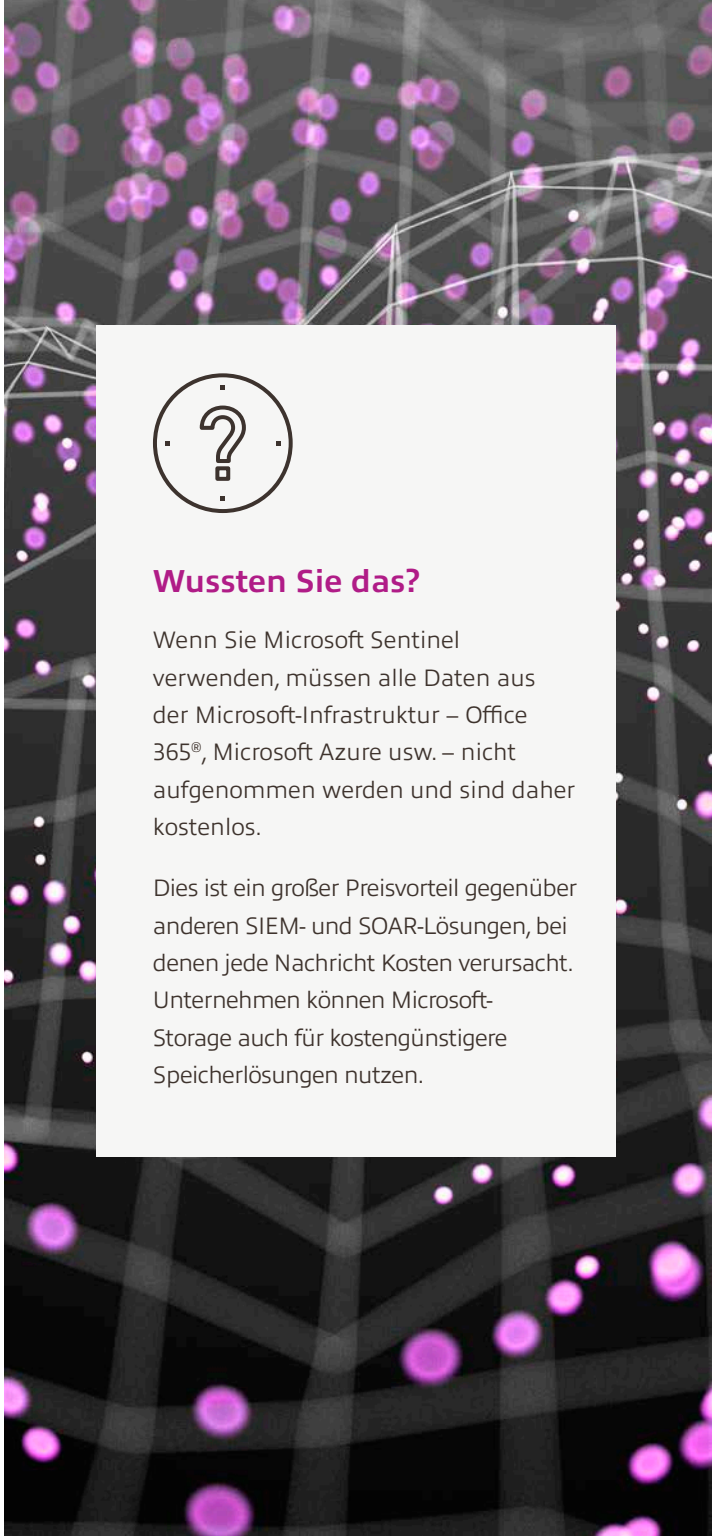
Minimierung von Fehlalarmen.

Viele sofort einsatzbereite Regeln, die mithilfe von Verhaltensanalysen über administrative Funktionen berichten, können Ergebnisse zu Fehlalarmen generieren. Microsoft hat eine Sentinel-Funktion namens Watchlist veröffentlicht, um diese Fehlalarme, das daraus resultierende Rauschen und die Alarmermüdung zu reduzieren. Mit Watchlist können Sie Abfragen (oder CSVs mit verschiedenen Attributen) in Analyseregeln einbinden, die eine Watchlist oder ein Schlüsselidentifikator-Paar untersuchen und bei bestimmten Aktivitäten keinen Alarm auslösen.

4.

Verwenden Sie einen zentralen Tenant.

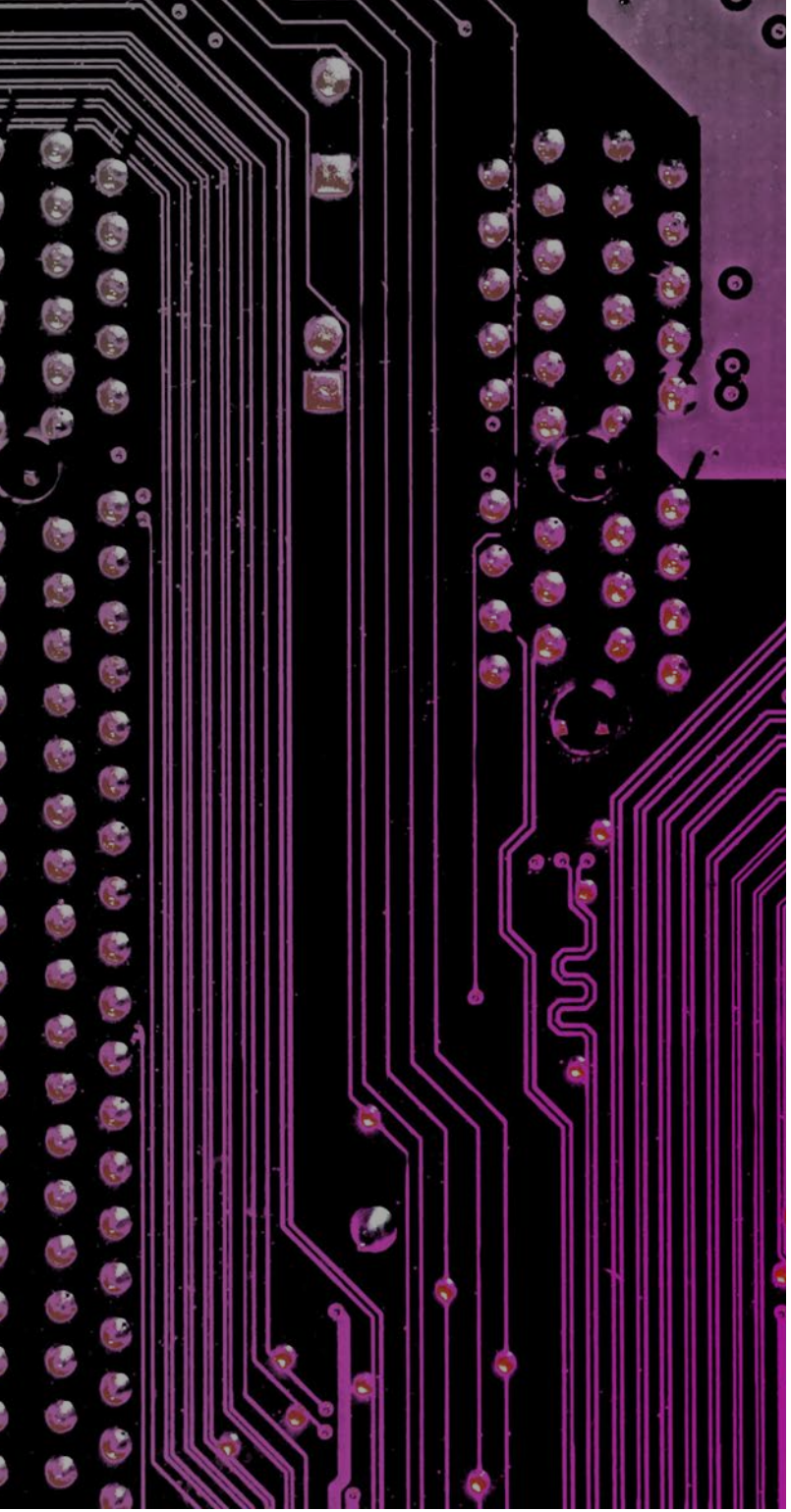
Wenn Sie verschiedene Azure®-Tenants überwachen, müssen Sie in jedem dieser Tenants verschiedene Microsoft Sentinel-Installationen erstellen und Analyse-Arbeitsbereiche protokollieren. Wenn Sie Azure Lighthouse zur Überwachung dieser Arbeitsbereiche in einem zentralen Tenant verwenden, können Sie Analyseregeln abstimmen, die Quelle der Wahrheit finden und Regeln für alle Tenants bereitstellen. Dies hilft Ihnen, eine konsistente Basis für Schwellenwerte, Lauffrequenz und andere Einstellungen festzulegen.



Wussten Sie das?

Wenn Sie Microsoft Sentinel verwenden, müssen alle Daten aus der Microsoft-Infrastruktur – Office 365®, Microsoft Azure usw. – nicht aufgenommen werden und sind daher kostenlos.

Dies ist ein großer Preisvorteil gegenüber anderen SIEM- und SOAR-Lösungen, bei denen jede Nachricht Kosten verursacht. Unternehmen können Microsoft-Storage auch für kostengünstigere Speicherlösungen nutzen.



5.

Führen Sie Out-of-the-Box Detuning durch.

Microsoft Sentinel bietet den deutlichen Vorteil einer reibungslosen Integration in Ihr Microsoft-Ökosystem. Unsere Berater empfehlen Kunden regelmäßig, Microsoft Defender for Identity (MDI) beispielsweise für on-premises Active Directory® (AD) zu verwenden. Wenn Sie jedoch MDI in Sentinel aktivieren, leitet die Standardeinstellung automatisch alle Warnungen weiter, die aus MDI kommen. Wahrscheinlich möchten Sie den Plugin-Connector so einstellen, dass Sie nicht zu unwichtigen Informationen benachrichtigt werden und nur Benachrichtigungen innerhalb eines bestimmten Schweregrads erhalten.

Untersuchen Sie auch die Schweregrade bestehender analytischer Regeln und eskalieren, deeskalieren oder entfernen Sie diese, basierend auf Ihren Anforderungen. Viele sofort einsatzbereite Analyseregeln werden mit einer festgelegten Häufigkeit ausgeführt, möglicherweise zu oft, um verwaltet zu werden. Wir empfehlen die Verwendung von Analyseregeln, die alle 15 oder 30 Minuten für Warnmeldungen mit hohem Schweregrad ausgeführt werden, und deren Ausführung nur einmal täglich für Warnmeldungen mit geringem Schweregrad oder für Warnmeldungen mit wenig Einfluss auf das Unternehmen. Letztendlich hilft Ihnen das Deaktivieren dabei, Alarmermüdung und Rauschen zu minimieren.

6.

Bewerten Sie auf Parität.

Was haben Sie verwendet, um Ihre IT-Umgebung vor Microsoft Sentinel zu sichern? Was sind die Ähnlichkeiten und Unterschiede? Unsere Berater empfehlen, Seite an Seite auf Ihr altes System und die Microsoft-Sentinel-Umgebung zu schauen und visuelle Ergebnisse, Dashboards, Warnungen, Protokollquellen und andere wichtige Attribute zu vergleichen, um sicherzustellen, dass Sie Parität erhalten. Es sollte keine Datenquelle übersehen werden. Auf diese Weise können Sie auch sicherstellen, dass Sie den neuen Umfang der täglichen Aufgaben, die Pflege und Versorgung sowie den Personalbedarf für die Unterstützung der neuen Plattform vollständig verstehen.

7.

Berücksichtigen Sie die Empfehlungen von Microsoft.

Microsoft hat Empfehlungen für regelmäßige Aktivitäten veröffentlicht, um sicherzustellen, dass Sentinel Ihnen die bestmögliche Sicherheit bietet. Überprüfen Sie sie auf Vorschläge zu täglichen, wöchentlichen und monatlichen Aufgaben, zu erstellenden Integrationen und Prozessen zum Managen und zur Reaktion auf Vorfälle.

Möglichkeiten der Automatisierung

Eine der Stärken der Microsoft Sentinel-Plattform sind ihre Automatisierungsfunktionen. Nutzen Sie die Vorteile der Automatisierung, um optimale Effizienz und Sicherheit zu erreichen.

Hier sind einige Möglichkeiten, wie Sie mit Sentinel automatisieren können:

Retention

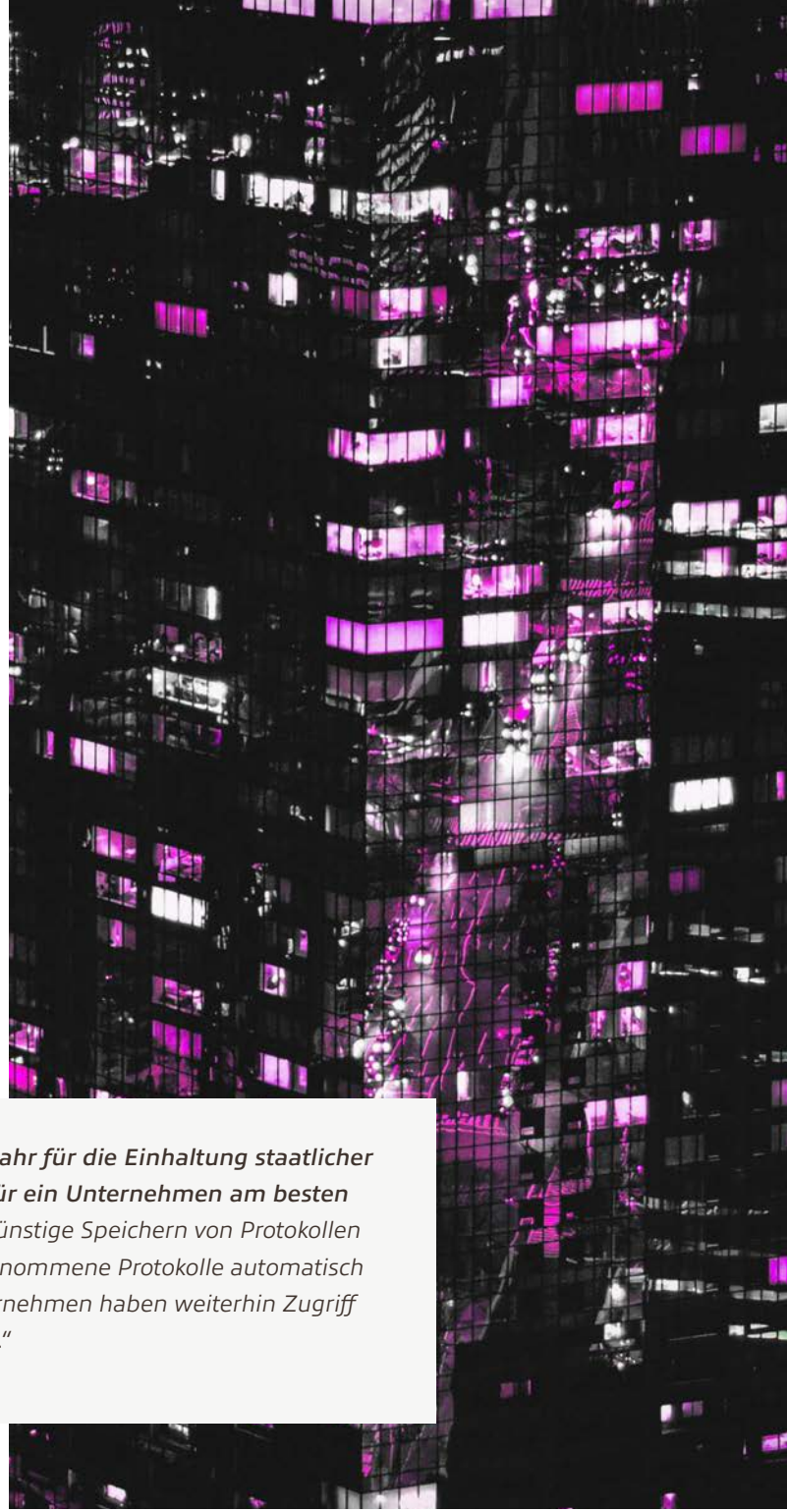
Jedes Unternehmen hat unterschiedliche Anforderungen im Zusammenhang mit der Datenspeicherung, basierend auf Branchen- und Rechts- und Compliance-Vorschriften. Microsoft Sentinel bietet die Möglichkeit, Storage für festgelegte Zeiträume zu automatisieren – was es Ihrem Team unglaublich einfach macht, dieses Kästchen anzukreuzen, ohne Erinnerungen festlegen oder sich um die Kapazität sorgen zu müssen.

Playbooks

Für komplexere Automatisierungen sind Playbooks eine ausgezeichnete Option. Playbooks in Microsoft Sentinel können für eine Reihe von Aufgaben eingerichtet werden, wie z. B.:

- Sperren eines Benutzers nach einer fehlgeschlagenen Anmeldewarnung
- Erstellen eines ServiceNow®-Vorfalls, der in Ihr Ticketsystem eingespeist wird
- Änderung der CMDB in ServiceNow bei Änderungen an gesperrten Geräten im Netzwerk

Das Microsoft-eigene GitHub enthält viele Playbooks und Ideen für Anpassungen sowie anbieterspezifische Automatisierungen innerhalb von Microsoft Sentinel, die Sie erkunden können.



> ***Einige unserer Kunden verlangen eine siebenjährige Datenaufbewahrung für HIPAA oder ein Jahr für die Einhaltung staatlicher Vorschriften, z. B. NIST. Es ist eine Herausforderung herauszufinden, welches Speicherschema für ein Unternehmen am besten funktioniert.*** *Der Blob Storage von Microsoft ist eine gute Option – er ermöglicht Ihnen das kostengünstige Speichern von Protokollen für bis zu sieben oder acht Jahre. Um dies zu vereinfachen, erstellen wir Azure Logic Apps, die aufgenommene Protokolle automatisch von Microsoft Sentinel zu Blob Storage verschieben, um sie sieben Jahre lang aufzubewahren. Unternehmen haben weiterhin Zugriff auf die Protokolle, wenn sie für eine Sicherheitsuntersuchung oder -nachforschung benötigt werden.*“
>
> **— Associate Consultant, InfoSec, Insight**

Blick in die Zukunft

Es gibt unzählige Möglichkeiten, Microsoft Sentinel zu erweitern und zu verbessern – und die Möglichkeiten wachsen mit zunehmender Weiterentwicklung der Plattform und der Benutzer-Community.

BYO ML

Bring Your Own Machine Learning (BYO ML) ist ein Bereich, der viel Aufmerksamkeit erregt. Diese Microsoft GitHub-Seite dient als Speicherort für die neuesten Informationen und eine wachsende Bibliothek von Beispiel-Schulungs-Notebooks. Unternehmen verwenden BYO ML, um Databricks zu starten und Schulungen und Analysen über eine Spark-Umgebung durchzuführen, die alle Daten von Sentinel abruft, Modelle für Remote-Zugriff oder anomales Verhalten erstellt und vieles mehr.

> ***Sie müssen kein Doktor sein, um dies zu tun.*** *Viele der gemeinschaftsbasierten Schulungen und Modelle sind eine ziemlich gute Annäherung, die nur an Ihre IT-Umgebung angepasst werden muss. Andere SIEMs haben etwas Ähnliches, aber die Idee, dass man eine rein datenwissenschaftliche Erfahrung haben kann, wo man im Grunde genommen ein Jupiter-Notebook, eine Reihe von Python-Datenwissenschaftsbibliotheken hat und Daten direkt aus der Softwareumgebung zieht, in der das Notebook ausgeführt wird – das ist für mich ziemlich interessant.“*
>
> **— Principal Architect (Cybersicherheit, Networking, Datenwissenschaft), Insight**

Erweiterte Visualisierung

Azure Monitor Workbooks in Microsoft Sentinel bieten eine umfassende Datenvisualisierung. Natürlich ist dies für Sicherheitsteams äußerst nützlich. Die Einsicht in die Daten kann es einfacher machen, Schwachstellen und Anfälligkeiten zu identifizieren, was Sicherheitsteams bei der Priorisierung hilft. Die Visualisierung kann Sicherheitsteams auch dabei helfen, Budgets schnell für die C-Suite zu rechtfertigen. Wir glauben, dass die Datenvisualisierung in Zukunft ein wichtiger Schwerpunkt sein wird, da Benutzer-Communities nutzerdefinierte Arbeitsmappen entwickeln, um alle Sicherheits- oder Unternehmensanforderungen zu erfüllen.

INSIGHT LÖSUNG

Unsere Security-Services-Berater können Ihnen dabei helfen, die Auswirkungen Ihrer Geschäftsaktivitäten auf die Sicherheit zu berücksichtigen und Lösungen zu übernehmen, die auf Ihre Bedürfnisse und Ziele abgestimmt sind. Wir beginnen mit dem Assessment Ihrer aktuellen IT-Umgebung, Herausforderungen und Anforderungen.

Managed Services

Aufgrund von Zeit- und Ressourcenmangel sind die heutigen Organisationen nur in der Lage,

50%

der legitimen Sicherheitsbedrohungen zu beseitigen.[1]

Viele Unternehmen finden es schwierig, erfahrene Sicherheitsexperten anzuziehen und zu binden, die über die neuesten SIEM-, SOAR- und Security Operations Center (SOC)-Toolsets auf dem Laufenden sind. Bereits jetzt beobachten wir eine allgemeine Konsolidierung von Sicherheitsexperten innerhalb von Dienstleistungsunternehmen, die Sicherheitsumgebungen kompetent verwalten können – und auch wichtige Unterstützung in Bezug auf Ransomware-Bereitschaft, Sicherheitsarchitektur, Reaktion auf Vorfälle und Abhilfemaßnahmen bieten.

In vielen Fällen ist das Zeitmanagement die zentrale Herausforderung. Die unzähligen alltäglichen Anforderungen an ein Sicherheitsteam können den Blick auf die Möglichkeiten der Automatisierung oder des maschinellen Lernens zur Verbesserung der Bedrohungsjagd trüben.

Der Schlüssel zur Erhöhung Ihrer Sicherheit? Managed Services.

Insight bietet Managed Security Services (MSS), die auf den Funktionen von Microsoft Sentinel aufbauen und eine Rund-um-die-Uhr-Überwachung Ihrer IT-Umgebung bieten. Indem wir branchenerprobte Best Practices mit hochmodernen Techniken zur Risikominimierung kombinieren, helfen wir unseren Kunden, die schwere Last der Pflege und Verbesserung einer dynamischen Sicherheitsumgebung abzunehmen.

Ein fortschrittlicher Ansatz.

Unsere Security-Services-Berater können Ihnen dabei helfen, die Auswirkungen Ihrer Geschäftsaktivitäten auf die Sicherheit zu berücksichtigen und Lösungen zu übernehmen, die auf Ihre Bedürfnisse und Ziele abgestimmt sind. Wir beginnen mit dem Assessment Ihrer aktuellen IT-Umgebung, Herausforderungen und Anforderungen.

16 Jahre

an Erfahrung im Vorfalls- und Bedrohungsmanagement

Über 1.500

Architekten, Consultants und Fachgebietsexperten für Sicherheit und Servicebereitstellung

Gemanagte Sicherheitsergebnisse:

Schnellere Reaktionszeiten

Stärkere Governance und Compliance

Größerer Kontext und verbesserte Transparenz

Bessere Bedrohungserkennung

Geringere Belastung des Sicherheitsteams

Alles ist möglich

Microsoft Sentinel ist einfach zu implementieren – aber es erfordert zusätzliche Fähigkeiten, um es gut zu optimieren.

Glücklicherweise gibt es nur wenige Grenzen, wie weit die Plattform Sie auf dem Weg zu vollständiger Sicherheit bringen kann – und mit einem vertrauenswürdigen Team wie Insight ist es einfacher denn je, den Wert Ihrer Investition zu ermitteln. Unsere Berater, Techniker und Architekten verfügen über branchenführendes Fachwissen rund um Microsoft Sentinel in einer Vielzahl von Kunden-Umgebungen.

Unabhängig davon, wo Sie sich auf dem Sentinel-Pfad befinden, können Sie Insight für Folgendes nutzen:

- Bewertung Ihrer aktuellen Sicherheits-Umgebung
- Ein Microsoft Sentinel Readiness Assessment
- Bereitstellung, Integration und Anpassung von Microsoft Sentinel
- Managed Security Services zum Management von Microsoft Sentinel
- Microsoft Sentinel Optimierung, Automatisierungen und erweitertes Feature-Tuning

Kontaktieren Sie noch heute unser Team, um Ihre Anforderungen zu besprechen

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.

Weitere Informationen unter: **at.insight.com**

Insight®

Quellen:
[1] Cisco. (2020). Sichern, was jetzt ist und was als Nächstes kommt: 20 Überlegungen zur Cybersicherheit für 2020. CISO Benchmark-Umfrage.
[2] Younes, F. (2021, 21. Januar). Komplexität bleibt immer noch der schlimmste Feind der Cybersicherheit. Techeconomy.ng.
[3] Rockett, J. (2020, 25. Juni). Der SOAR-Bericht 2020 hebt die wichtigsten Treiber und Auswirkungen hervor. Swimlane.