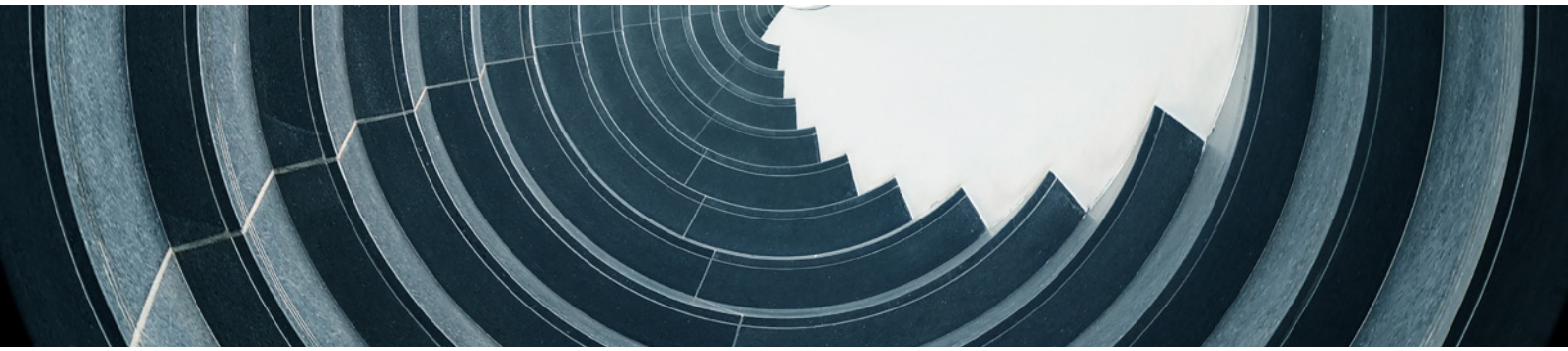
avanade

Azure Sentinel: Die cloud-native SIEM/SOAR-Lösung der nächsten Generation für moderne digitale Bestände

Eine umfassende Komplettlösung für Sicherheitsteams

Steigende Komplexität bei sicherheitsrelevanten Informationen und Incident Response



Moderne Unternehmen müssen einen enormen Aufwand betreiben, um ihre Kompetenzen im Bereich Cybersicherheit weiterzuentwickeln. Dabei stellt sie die zunehmende Komplexität der digitalen Bestände fortwährend vor neue Herausforderungen. IT-Abteilungen sind für den Schutz der IT-Technologien verantwortlich, also auch für SaaS-Anbieter, öffentliche Cloud-Services und IoT-Geräte, selbst wenn sie nicht im Eigentum des Unternehmens sind oder nur begrenzt Zugriff besteht. Im iDefense Bericht[1] aus dem Jahr 2019 betont Accenture zum dritten Mal in Folge, wie wichtig es für Unternehmen ist, Cyberbedrohungen proaktiv zu begegnen und nicht erst dann auf der Basis von Notfallplänen zu reagieren, wenn die Netzwerke bereits angegriffen wurden.

Bedrohungen basieren heute auf Taktiken, die es ihnen erlauben, lange Zeit unentdeckt zu bleiben. IBM schätzt in seinem Bericht „Cost of a Data Breach Report"[2] aus dem Jahr 2019, dass der durchschnittliche Zeitbedarf zur Aufdeckung eines Sicherheitsverstoßes 279 Tage beträgt und die entsprechenden Kosten für Unternehmen bei durchschnittlich 3,9 Millionen Dollar liegen. Das repräsentiert einen erheblichen Anstieg im Vergleich zu den 206 Tagen, die noch 2017 genannt wurden und zeigt einen äußerst negativen Trend in der Wirksamkeit der von den Unternehmen angewandten Taktiken. Angriffe, die sich gegen Personen richten, wie Phishing, Stehlen von Anmeldedaten und Social Engineering, verursachen bei Unternehmen weltweit Schäden in Milliardenhöhe[3]. Das unterstreicht, wie entscheidend die Erkennung und die Reaktionszeit für die Minimierung und Eindämmung eines Sicherheitsverstoßes ist.

Die Absicherung nur des internen Netzwerks ist heute nicht mehr ausreichend. Ein zeitgemäßer Schutz macht nicht nur ausgezeichnete Produkte zur Sicherung der Arbeitsumgebung erforderlich, sondern auch komplexe Analysen und Security Operations Center (SOC) neben hochqualifizierten Fachleuten zur Implementierung und zum Betrieb der umfassenden Prozesse, die zur Sicherung der digitalen Vermögenswerte des Unternehmens erforderlich sind. Obwohl eine solche Sicherheitslösung beträchtliche Investitionen erfordert, sind die Kosten für zuverlässige Sicherheit weitaus geringer als die Kosten eines Sicherheitsverstoßes.

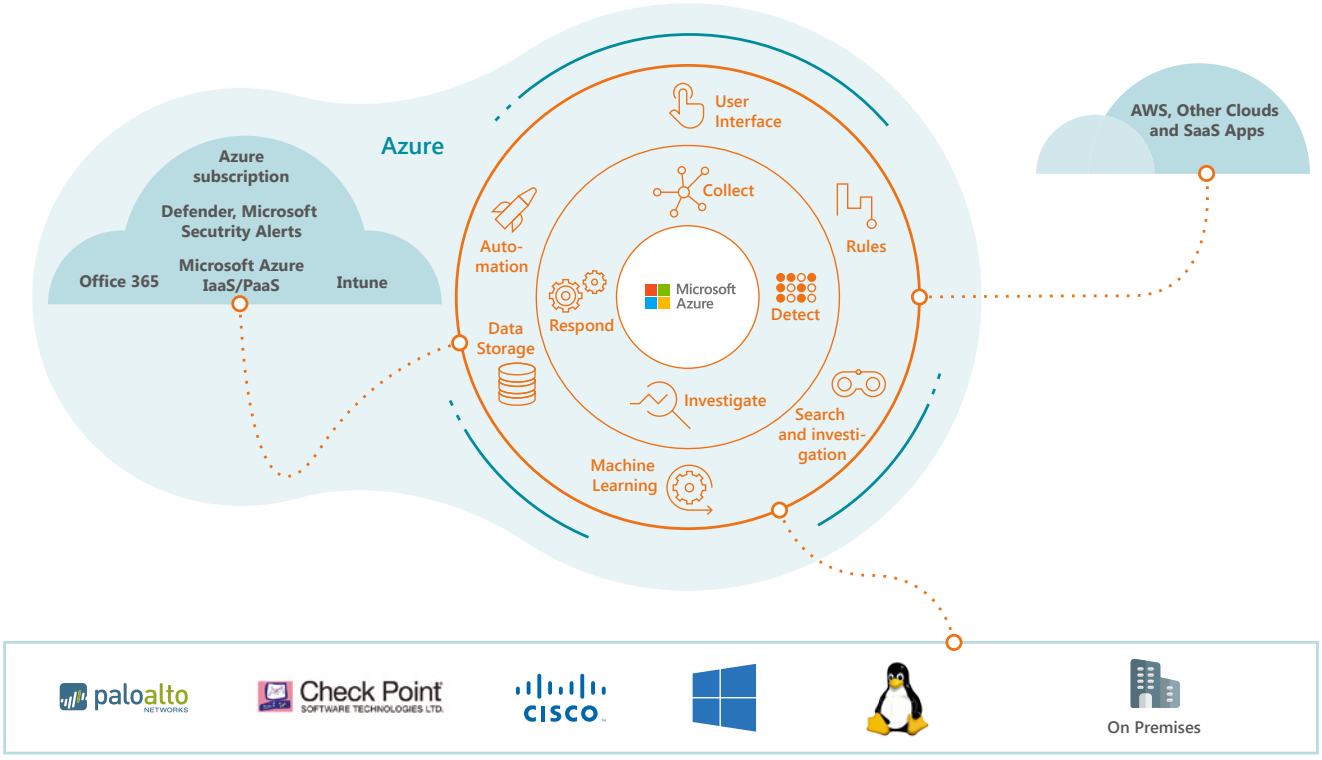
Eine der Herausforderungen für die Sicherheitsinfrastruktur ist die exponentielle Zunahme von Signalen aus der erweiterten digitalen Umgebung von modernen Unternehmen. Diese Signale stellen für Sicherheitsteams einen enormen Arbeitsaufwand dar und können Hinweise auf Cyberangriffe sogar überlagern. Der aktuellste Microsoft Security Intelligence Report[4] zeigt auf, dass 76 % der Unternehmen eine Zunahme von Sicherheitsinformationen vermelden, mit denen sie nicht in der Lage sind umzugehen, und dass 44 % der Warnungen aufgrund fehlender operativer Ressourcen nie untersucht werden. Die operative Belastung der SOCs wird voraussichtlich noch weiter zunehmen. So hat das globale Cyberwirtschaft-Forschungsunternehmen Cybersecurity Ventures in seinem Bericht aus dem Jahr 2020[5] prognostiziert, dass es bis 2021 weltweit mehr als 3,5 Millionen unbesetzte Positionen für Sicherheitsexperten geben wird, davon mehr als 400.000 in Europa.

Ein Cyber-Intelligence-System, das in der Lage ist, alle Warnmeldungen und -angriffe im Unternehmensumfeld aufzudecken und automatisch Maßnahmen zur Bewältigung der Folgen eines Cyberangriffs zu ergreifen, würde die Belastung der SOCs deutlich verringern.

[1] [LiDefense]
[2] [LIBM]
[3] [LACOC]
[4] [LMTIR]
[5] [LMCJR]

In vielen Fällen wird eine SIEM-Lösung nicht nur empfohlen, sondern ist für Unternehmen zwingend erforderlich, um lokale Vorschriften zur Datensicherheit und zum Datenschutz bzw. Industriestandards einzuhalten. Artikel 34 der EU-Datenschutz-Grundverordnung (DSGVO) verpflichtet Unternehmen bei Verletzungen des Schutzes personenbezogener Daten die betroffenen Personen **unverzüglich** zu informieren, da ansonsten seitens der Regulierungsbehörden eine hohe Geldstrafe droht. Wenn eine Organisation eine Zertifizierung nach der internationalen Norm für Informationssicherheit ISO 27001 erhalten möchte, muss sie die entsprechenden Anforderungen an die Protokollierung und Überwachung kritischer Systeme erfüllen. Um die vielen Vorschriften und Standards zu Datenschutz und -sicherheit einhalten zu können, müssen Organisationen daher eine moderne und leistungsfähige SIEM/SOAR-Lösung einsetzen, die sie in die Lage versetzt, Bedrohungen schnell zu erkennen und darauf zu reagieren.

Azure Sentinel ist Microsofts Antwort auf die zunehmende Komplexität der Sicherheitsanforderungen und den Umgang mit Incidents. Als cloud-native Lösung für Security Information Event Management (Verwaltung von Sicherheitsinformationen und -ereignissen – SIEM) und Security Orchestration Automated Response (Sicherheitsorchestrierung mit automatisierter Reaktion – SOAR) verhilft Azure Sentinel Unternehmen dazu, Warnungen aus dem digitalen Umfeld des gesamten Unternehmens zu erkennen und darauf zu reagieren.



Avanades Ansatz

Das Angebot des in Seattle, Washington, ansässigen Unternehmens Avanade umfasst IT-Beratung und -Dienstleistungen in den Bereichen Künstliche Intelligenz, Business Analysis, Application Services, digitale Transformation und Sicherheit. Über 38.000 Fachleute bieten weltweit Kunden aus 25 Ländern sachkundige Beratung. Als Microsoft-Partner und Softwareintegrator mit Gold-Kompetenz im Bereich Security baut das Unternehmen seine Fachkompetenzen in Bezug auf die verschiedenen Microsoft-Plattformen aus. Avanade kann einen großen Umfang an Erfahrung weitergeben und bewährte Verfahren in Kundenprojekte einbringen, um Unternehmen dabei zu unterstützen im Bereich Cybersecurity führend zu werden.

Für Azure Sentinel bietet das Expertenteam von Avanade Kunden auf der ganzen Welt ein einzigartiges Programm zur schnellen Umsetzung an. Dieser Ansatz basiert auf der Kombination von Avanades Kompetenz im Sicherheitsbereich, der umfassenden Erfahrung mit Microsoft-Technologie und einem tiefgehenden Verständnis für die IT-Umgebung des Kunden. Es gibt viele Unternehmen, die sich einer Cloud-first-Strategie verschrieben haben, aber ihre Cyber-Intelligence-Systeme noch immer On-Premises betreiben. Um diese Kunden beim Übergang zu Azure Sentinel – dem SIEM/SOAR-System der nächsten Generation – zu unterstützen, nutzt Avanade seinen internen Wissenspool mit globalen Anwendungsszenarien.

Avanade empfiehlt Unternehmen, die derzeit Azure AD, Office 365, Teams und andere Microsoft-Produkte einsetzen, die cloud-native SIEM/SOAR-Lösung Azure Sentinel. Durch die Bereitstellung eines integrierten Dashboards, das über neue Bedrohungen und Schwachstellen informiert, verbessert sich die Sicherheit und Transparenz. Das Team von Avanade bietet Beratung für Bedrohungsszenarien, wie sie im Zusammenhang mit den Herausforderungen eines modernen Arbeitsumfelds, wie z. B. ortsunabhängiges Arbeiten, auftreten, und kann maßgeschneiderte Lösungen anbieten, die sich an den Bedürfnissen der Unternehmen ausrichten. Avanades Team von Sicherheitsexperten bietet seinen Kunden die Möglichkeit, die Integration der Azure-Sentinel-Plattform mit anderen Microsoft-Sicherheitsprodukten wie Microsoft 365 Defender, Cloud App Security, Azure Security Center und anderen zu testen. Avanade unterstützt seine Kunden auch bei der Integration von Sicherheitsanwendungen und -tools von Drittanbietern und stellt auf diese Weise auf Basis der Microsoft-Plattform einen integrierten Überblick der Situation zur Identifizierung neuer Bedrohungen und Schwachstellen bereit. Mit Azure Sentinel können Organisationen ihre sicherheitsrelevanten Daten verwalten, den Grad an Automatisierung verbessern und ihre IT-Ressourcen auf wertschöpfende Projekte verlagern, ohne die Anforderungen ihrer Kunden zu vernachlässigen.

Bedrohung und Sicherheitslücken Dashboard

Beratung zu Bedrohungsinformationen

Integration der Microsoft-Sicherheitslösungen

Integration von Sicherheitstools Dritter

Security Operations Center

„Dadurch, dass wir uns sehr früh mit neuen Microsoft-Technologien beschäftigen, ist unser Beraterteam immer auf dem neuesten Stand. Wir profitieren von einem großen Erfahrungsschatz aus unterschiedlichen Projekten, so dass wir Best Practices für unsere Kunden zu entwickeln und ihnen sachkundige Ratschläge geben können“,

stellt Kyle Carlson, Verantwortlicher für die SIEM-Plattform bei Avanade, fest.

Die Digitalisierung verändert die Welt, wie wir sie kennen. Avanade hilft Unternehmen, in dieser sich schnell verändernden Umgebung performant zu sein. Als führender digitaler Innovator setzt Avanade mithilfe seiner Mitarbeiter und auf Basis des Microsoft-Ökosystems erfolgreich Projekte für seine Kunden und deren Kunden um.

avanade

Eine leistungsfähige cloud-native SIEM/SOAR-Lösung der nächsten Generation

Einsatz von Azure Sentinel

Azure Sentinel ist vollständig cloud-basiert und erfordert **keine hohen Anfangsinvestitionen,** da keine Infrastruktur vor Ort erforderlich ist. Sentinel baut auf der Azure-Plattform auf und bietet allen Nutzern die gleiche hervorragende Benutzererfahrung, unabhängig von der Unternehmensgröße. Azure Sentinel weist praktisch keinerlei Beschränkungen auf, wenn es um die Anzahl der verbundenen Datenquellen von Sicherheitsanwendungen und -diensten geht oder um die Anzahl der erfassten Protokolle und Nutzer. Das macht die Lösung für Unternehmen aller Größenordnungen zu einer interessanten Sicherheitsinfrastruktur. Einerseits, für kleine Unternehmen, die mit nur wenigen Mitarbeitern vollständig in der Cloud arbeiten. Andererseits, für große internationale Unternehmen, die in komplexen hybriden Umgebungen eine Vielzahl von Sicherheitsprodukten und -diensten einsetzen, um alle Bereiche ihrer riesigen IT-Infrastruktur zu schützen. Als cloud-basiertes SIEM-System unterliegt Sentinel nahezu **keinen Einschränkungen bezüglich der Skalierbarkeit** und Verarbeitungsgeschwindigkeit – im Gegensatz zu herkömmlichen On-Premise-Lösungen, die einen hohen Kosten- und Zeitaufwand für Bereitstellung, Wartung und Skalierung erfordern.

Sentinel-Kunden zahlen nur „für den Umfang, den sie nutzen", wobei die Kosten auf der Grundlage des erfassten Datenvolumens und der Aufbewahrungsdauer berechnet werden. Azure Sentinel bietet kostenlose Speicherung und Analyse von Office-365-Daten und Azure-Kunden profitieren von einer **kostengünstigen und planbaren Abrechnung** sowie flexiblen Abonnements.

Herkömmliche SIEM-Lösungen müssen auf die individuelle Bedrohungssituation, den Reifegrad und die Bedürfnisse einer Organisation zugeschnitten sein. Im Gegensatz dazu nutzt Azure Sentinel einen vollständig integrierten Ansatz. Dabei wird auf Basis des Azure-Portals eine Verbindung zu bestehenden Azure- und Microsoft-365-Quellen hergestellt, einschließlich Office 365, Azure AD, Azure Security Center, **Microsoft Defender for Identity,** Microsoft Cloud App Security und **Microsoft 365 Defender.** Darüber hinaus gibt es **integrierte Connectors,** die eine Anbindung an das breite Angebot von Sicherheitslösungen anderer Hersteller erlauben.

Azure Sentinel Features

Sentinel **nutzt cloud-basierte Intelligenz** und die nativ integrierten Möglichkeiten der Azure- und Azure-Data-Services-Plattform, um die Reaktion des Unternehmens auf Sicherheitsverletzungen intelligenter, schneller und einfacher zu gestalten.

Während herkömmliche SIEM-Lösungen oft keinen Kontext zu Warnungen liefern, bietet Sentinel die Möglichkeit, Ereignisse und Warnungen in einem **interaktiven und vollständig anpassbaren Dashboard** anzuzeigen, sodass das Sicherheitspersonal Vorfälle untersuchen und zueinander in Beziehung setzen kann. Die Sicherheitsanalysen werden durch den Einsatz der interaktiven, **ausgeklügelten Triage-Möglichkeiten** von Azure Sentinel ergänzt, um versteckte Zusammenhänge und die Ursachen von Warnungen zu erforschen.

Azure Sentinel bietet durch die integrierten Azure Logic Apps weitere Möglichkeiten, die eine **automatische Reaktion** auf Warnungen und potenzielle Sicherheitsvorfälle ermöglichen, um so die operative Belastung der SOCs zu reduzieren.

Azure Sentinel: Security Analytics und Operations zu Zeiten des Cloud Computings

Azure Sentinel bietet eine SIEM/SOAR-Komplettlösung für Unternehmen, die sowohl mit Systemen vor Ort als auch mit cloud-basierten Lösungen arbeiten mit folgenden Vorteilen für die IT-Teams:

Datensammlung	Aufdecken		Untersuchen	Reagieren
Übersichtlichkeit	Analyse	Suchanfragen	Vorfälle	Automatisierung

avanade

Datensammlung – Speicherung der Protokolle der gesamten digitalen Umgebung an einem Ort

Azure Sentinel ermöglicht es Anwendern, Signale, die von nativen Microsoft-Plattformen wie Office 365, Azure Active Directory, Microsoft Defender for Identity und Microsoft Cloud App Security kommen, auf einfache Weise mit SaaS-, IaaS- und PaaS- und IOT-Cloud-Lösungen sowie mit Sicherheitsinfrastrukturen vor Ort wie Firewalls, Router und Plattformen für Endpunkt-Sicherheit zusammenzuführen.

Sentinel bietet einfach konfigurierbare Connectors[6], die Protokolle erfassen und Datenquellen von Anbietern wie Cisco, Symantec, Citrix, AWS und vielen weiteren anbinden können und dadurch vollständige Sicherheitsanalysen über den gesamten digitalen Bestand des Unternehmens erlauben.

Übersichtlichkeit – eine Vielzahl von Möglichkeiten, Ereignisse zu überwachen

Azure Sentinel bietet eine Vielzahl von Möglichkeiten, Verbindungen zu anderen Datenquellen herzustellen und Sicherheitsdaten aus dem gesamten digitalen Bestand des Unternehmens zu sammeln. Als cloud-native skalierbare Anwendung passt sich Azure Sentinel automatisch der Größe des Unternehmens an und eignet sich somit für Organisationen jeder Größenordnung.

- Die integrierten Connectors[7] ermöglichen es den Benutzern, eine Vielzahl von Datenquellen mit wenigen Klicks direkt von Azure Sentinel aus zu verbinden und zu verwalten. Es gibt mehrere Microsoft-Lösungen, die „out of the box" verfügbar sind, darunter Microsoft 365 Defender und Microsoft 365-Lösungen, wie Office 365, Azure AD, Microsoft Defender for Identity und Microsoft Cloud App Security und viele andere. Darüber hinaus existiert eine wachsende Anzahl an Anbietern von Cloud- und Sicherheitssystemen, die bereits eine Integration mit Azure Sentinel bieten und es erlauben, Daten direkt an die cloud-native SIEM/SOAR-Lösung zu senden.
- Microsoft nutzt die Integration von Azure, Microsoft 365 und Office 365, um eine einfache Erfassung von Protokollen von Microsoft Services und Anwendungen[8] zu ermöglichen. Selbst wenn ein Dienst nicht unter den Connectors in Sentinel aufgeführt ist, bedeutet dies nicht, dass Sentinel die jeweilige Azure- oder Microsoft-Lösung nicht unterstützt.

  Azure Sentinel arbeitet mit Azure Monitor und dem zugehörigen Log Analytics-Modul. Das heißt, wenn eine Datenquelle das Senden von Protokollen an Azure Monitor oder Log Analytics unterstützt, dann kann Azure Sentinel ebenfalls mit diesen Daten arbeiten.
- Der Azure Sentinel Log Analytics Agent[9] kann sowohl auf Servern vor Ort als auch auf IaaS-Servern installiert werden, um Daten von Windows-Endpunkten und Servern zu sammeln, wie beispielsweise Windows-Ereignisse von AD, Sysmon, SQL Server, DNS, Windows Firewall und vielen anderen. Ein Einsatz auf Linux ist ebenfalls möglich, sofern der Agent Linux-Syslog-Daten erfasst.
- Eine Vielzahl von Drittanbieter-Connectors, die Syslog und CEF-Ereignisse an Azure Sentinel[10] weiterleiten, werden ebenfalls unterstützt.
- Und für jede sonstige firmeninterne Anwendung gibt es die Möglichkeit, mit dem Log Analytics Agent, Logstash, Azure Logic Apps und PowerShell-Skripten benutzerdefinierte Connectors[11] zu erstellen, um auf diese Weise sämtlichen geschäftlichen Anforderungen gerecht werden zu können.

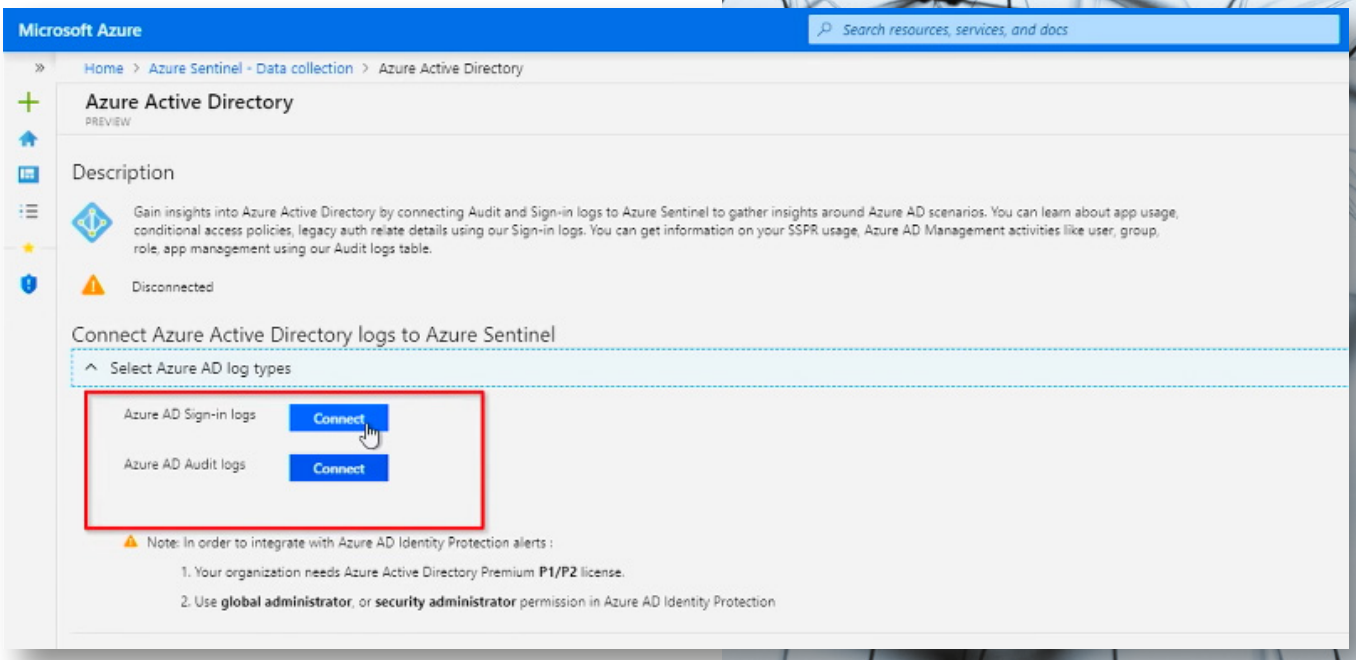
---

[6] [THCG]
[7] [LMCDS]
[8] [LMCL]
[9] [LMCS]
[10] [LMSC]
[11] [LMCC]

Praxisszenario: Tracking der digitalen Identität

Die Identität steht im Mittelpunkt der Sicherheitsbemühungen. Der Schutz des digitalen Umfelds vor Identitätsangriffen wie der missbräuchlichen Verwendung von Zugangsdaten ist in einem modernen digitalen Umfeld besonders wichtig. Unternehmen betreiben daher sehr viel Aufwand, um kritische Assets in ihren Systemen und in der Cloud zu schützen. Wenn es zu einer Datenschutzverletzung kommt, konzentrieren sich die Untersuchungen und Abhilfemaßnahmen hauptsächlich auf die Identität: Wer hat den Angriff verübt? Wer wurde kompromittiert? Woher kam der Angriff? Worauf wurde oder worauf hätte zugegriffen werden können? Bei einer Vielzahl von Sicherheitsprodukten liegt der Schwerpunkt auf dem Schutz der digitalen Identität von Einzelpersonen und Unternehmen in Form der Bereitstellung von Identitäts- und Zugriffsmanagementlösungen. Ein leistungsstarkes Werkzeug zur Verwaltung von Identitäten in einer hybriden Umgebung ist Azure Active Directory und daher von entscheidender Bedeutung für eine SIEM/SOAR-Lösung wie Sentinel.

Um Azure Active Directory einzubinden, muss der Kunde eine Azure-AD-P1- oder -P2-Lizenz besitzen und der Nutzer muss über globale oder Sicherheits-Administrator-Berechtigungen verfügen. Um die Protokolldaten in Sentinel einzubinden, muss Azure Active Directory als Datenquelle im Menü **Data connectors** unter **Configuration** ausgewählt werden. Azure Sentinel kann dann die AD-Sign-in- und -Audit-Logs sammeln, die in den späteren Abschnitten dieser Unterlage noch ausführlicher behandelt werden. Andere nützliche Datenquellen, die weitere Hintergrundinformationen zur digitalen Identität liefern, wie Syslog-Daten, Office 365, Azure Monitor, sowie weitere Quellen, wie AWS, Cisco ASA, Google Admin Console etc., können über die vielen Connectors, die Azure Sentinel unterstützt, oder über den Log Analytics Agent verbunden werden.



Aufdecken – mehr Sichtbarkeit im modernen digitalen Umfeld erlangen

Azure Sentinel enthält Analyseregeln und Vorlagen, die von Microsoft-Sicherheitsexperten entwickelt wurden. Diese ermöglichen es Ihnen, Ihre gesamte Umgebung anhand von bestimmten Kriterien zu durchsuchen, um verdächtige Aktivitäten und Bedrohungen auf der Grundlage bekannter Angriffsvektoren und Schwachstellen zu identifizieren und Vorfälle zur weiteren Analyse zu generieren, sobald bestimmte Parameter erfüllt sind. Sentinel-Benutzer können auch benutzerdefinierte Regeln entsprechend den speziellen Anforderungen ihres jeweiligen digitalen Umfelds erstellen.

Um die Datenanalyse übersichtlicher zu gestalten, verwendet Azure Sentinel einfach konfigurierbare Dashboards mit Sicherheitsmetriken, die Workbooks genannt werden. Mithilfe umfangreicher visueller Berichte können Analysten Sicherheitsereignisse und -warnungen, potenziell schädliche Aktivitäten, Vorfälle und Datenanomalien einer oder mehrerer Datenquellen leicht nachverfolgen. Sentinel-Benutzer können aus einer Auswahl vordefinierter Workbooks wählen oder eigene Workbooks erstellen.

Sentinel bietet als besonderen Ansatz die proaktive Auswertung von Bedrohungsinformationen zum Aufspüren von Sicherheitsvorfällen und unentdeckten Bedrohungen. Die cloud-native SIEM/SOAR-Lösung profitiert auch von der Flexibilität fortgeschrittener Abfragen in KQL und Programmiersprachen wie Python und R. Sentinel-Daten können mit allen externen Datenquellen mithilfe von Azure Notebooks, einer kostenlosen cloud-basierten Implementierung von Jupyter Notebook, verknüpft werden.

Analyse – Warnmeldungen bei anomalen Verhaltensweisen und verdächtigen Aktivitäten und Nutzung der KI-gestützten Fusion-Technologie

Nach der Erfassung der Daten setzt Azure Sentinel fortschrittliche Analyseregeln ein, um Warnmeldungen und Vorfälle zu generieren. Damit die Korrelationsregeln ordnungsgemäß abgearbeitet und Warnungen untersucht werden können, ist eine permanente Überwachung erforderlich. Die Regeln können dabei auf Datenabfragen, Microsoft-Sicherheitswarnungen oder der hochmodernen, von Microsoft speziell für die Azure-Plattform entwickelten und auf maschinellem Lernen basierenden Technologie namens Fusion basieren.

Maschinelles Lernen ist ein datenwissenschaftlicher Ansatz, der es Computern ermöglicht, bestehende Daten zu nutzen, um Vorhersagen über zukünftiges Verhalten, Ergebnisse und Trends zu treffen, indem sie Algorithmen aus dem Bereich des maschinellen Lernens verwenden, um nach einer anfänglichen Dateneingabe im Laufe der Zeit aus Erfahrungen zu lernen.

Mittels Fusion kann Azure Sentinel mehrstufige Angriffe automatisch erkennen, indem anomale Verhaltensweisen und verdächtige Aktivitäten in Echtzeit kombiniert werden. Auf der Grundlage dieser Informationen generiert Azure Sentinel Vorfälle, die auf andere Weise nur schwer hätten ermittelt werden können. Sentinel-Benutzer können das KI-gestützte Fusion nutzen, indem sie die Analyseregel Advanced Multistage Attack Detection in Azure Sentinel erstellen. Wenn die Datenquellen **Azure AD Identity Protection** und **Microsoft Cloud App Security** mit Sentinel verbunden sind, kann Fusion Warnungen aus diesen Quellen korrelieren und unzählige Warnungen über verdächtige Aktivitäten mit geringerer Qualität zu Dutzenden von korrelierten Untersuchungsfällen mit höherer Qualität zusammenfassen. Das bedeutet, dass z. B. die folgenden Warnungen:

- Unmöglicher Ortswechsel zu einem atypischen Ort, gefolgt von einer verdächtigen Office-365-Aktivität
- Anmeldeereignis von einem unbekannten Ort, gefolgt von einer verdächtigen Office-365-Aktivität
- Anmeldeereignis mit einem infizierten Gerät, gefolgt von einer verdächtigen Office-365-Aktivität
- Anmeldeereignis von einer anonymen IP-Adresse, gefolgt von einer verdächtigen Office-365-Aktivität
- Anmeldeereignis eines Benutzers mit kompromittierten Anmeldeinformationen, gefolgt von einer verdächtigen Office-365-Aktivität

mit verwandten Sicherheitsvorfällen korreliert würden, sodass Analysten einen Angreifer, der sich Zugang verschafft hat, erkennen und seine Bewegung im Netzwerk verfolgen können, um die volle Tragweite der Sicherheitsverletzung aufzudecken. Microsoft plant, das maschinelle Lernen in Azure Sentinel zu erweitern, indem das Know-how und die Erkennungsmuster der Microsoft-Sicherheitsaufklärungsteams genutzt werden, um noch mehr KI-gestützte Korrelationsinformationen in Fusion zu integrieren, und in Zukunft Azure-Sentinel-Benutzer in die Lage zu versetzen, eigene maschinelle Lernmodelle zu implementieren, damit die Erkennung perfekt auf die Organisation zugeschnitten werden kann. Durch den Einsatz der Fusion-Technologie minimiert Sentinel die Belastung der SOCs, da es die „Warnungsermüdungserscheinungen", die bei herkömmlichen On-Premise-SIEM-Lösungen häufig auftreten, exponentiell verringert. Die Korrelation von zusammenhängenden Ereignissen und Warnungen ermöglicht auch eine tiefe gehende Untersuchung von Sicherheitsvorfällen.

Sentinel-Benutzer können auch auf die mehr als 100 integrierten Analyseregeln[12], die von der Microsoft-Community bereitgestellt werden, mit wenigen Klicks zugreifen. Zusätzlich zu den leistungsstarken integrierten Abfragen können Sentinel-Benutzer, unter Verwendung der Abfragesprache Kusto eigene Regeln erstellen[13] bzw. anzupassen oder die wachsende Azure-Sentinel-Community auf GitHub[14] nutzen. Sentinel greift zusätzlich auf die integrierten Sicherheitsfeatures von Microsoft 365 und Azure zu, um Warnungen mit anderen Bedrohungsereignissen aus dem erweiterten digitalen Bestand des Unternehmens zu korrelieren. Sicherheitsexperten profitieren von der automatischen URL-Analyse in Sentinel und den integrierten Funktionen zum maschinellen Lernen und können Vorfälle dadurch noch schneller und genauer aufdecken.

Um Sicherheitsvorfälle zu erkennen und zu korrelieren, können Sicherheitsexperten Arbeitsmappen in Sentinel[15] einsetzen, um die Ergebnisse der Abfragen grafisch darzustellen. Arbeitsmappen sind im Wesentlichen Dashboards, die es den Sicherheitsverantwortlichen ermöglichen, die Sicherheit der Systemlandschaft proaktiv zu überwachen. Der Benutzer kann vorkonfigurierte Dashboards über die Registerkarte Arbeitsmappen auswählen, wenn die erforderlichen Datenquellen bereits verbunden sind, oder eigene Arbeitsmappen erstellen, indem er die Regeln für Abfragen definiert und die Art und Weise auswählt, wie die Ergebnisse visualisiert werden sollen. Darüber hinaus sind viele weitere Dashboards auf Sentinels GitHub verfügbar, die von einer großen IT-Community bereitgestellt werden.

[12] [LMDT]
[13] [LMDT]
[14] [LGASIC]
[15] [LMVA]

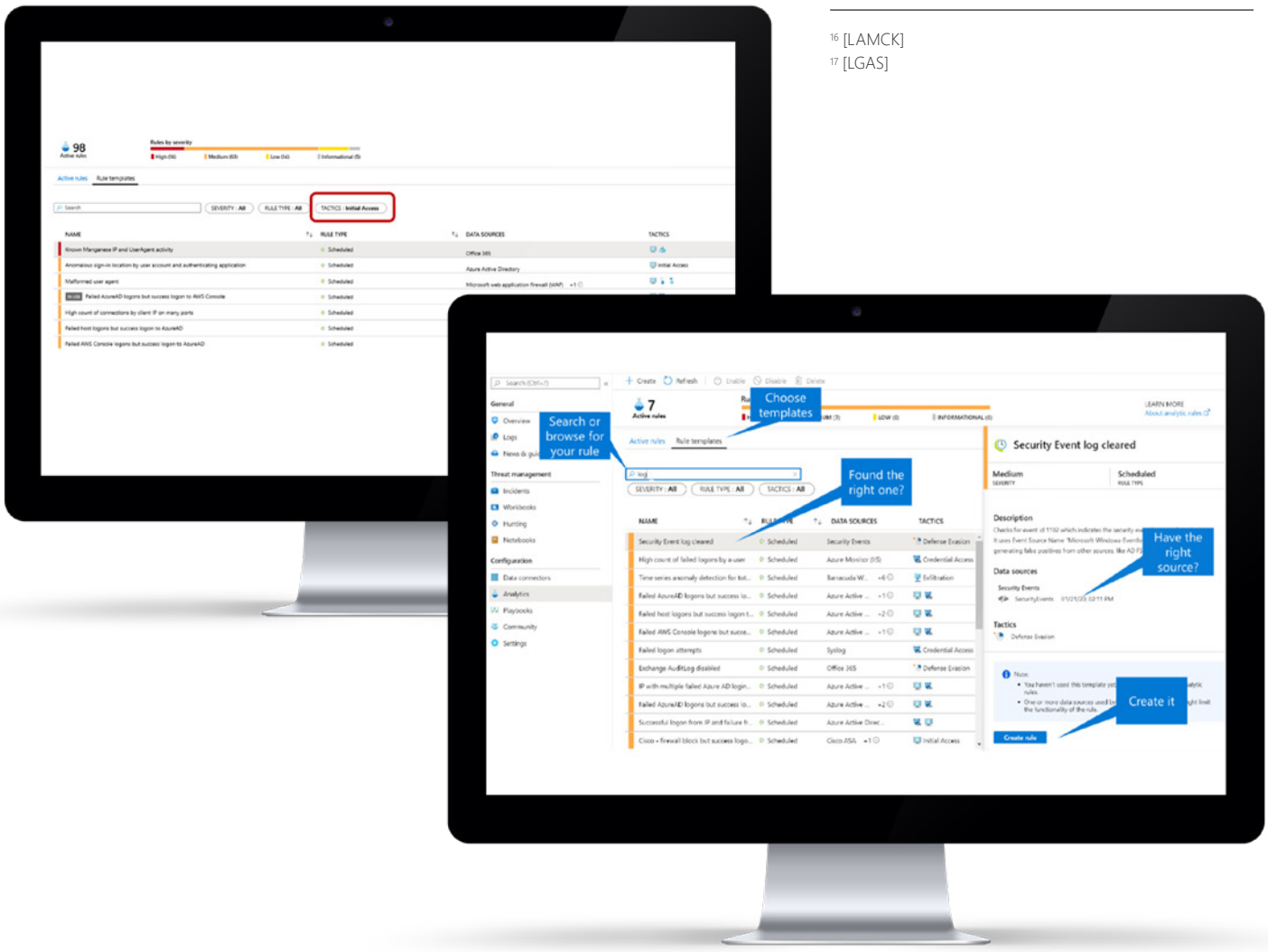
Praxisszenario: Erzeugen von Warnungen bei Identitätsangriffen

Wie bereits in einem früheren Abschnitt erwähnt, ist der Missbrauch der Identität eine der verbreitetsten Bedrohungen, und ein erheblicher Prozentsatz aller Sicherheitsverstöße wird durch den Diebstahl von Zugangsdaten verursacht. Eine unmittelbare Reaktion, die die Auswirkungen einer Datenschutzverletzung minimal hält, erfordert ein schnelles Erkennen des Angriffs, sodass die Sicherheitsteams die Möglichkeit haben, das bedrohte Konto zu identifizieren und ein weiteres Ausbreiten des Angreifers im Netzwerk zu verhindern.

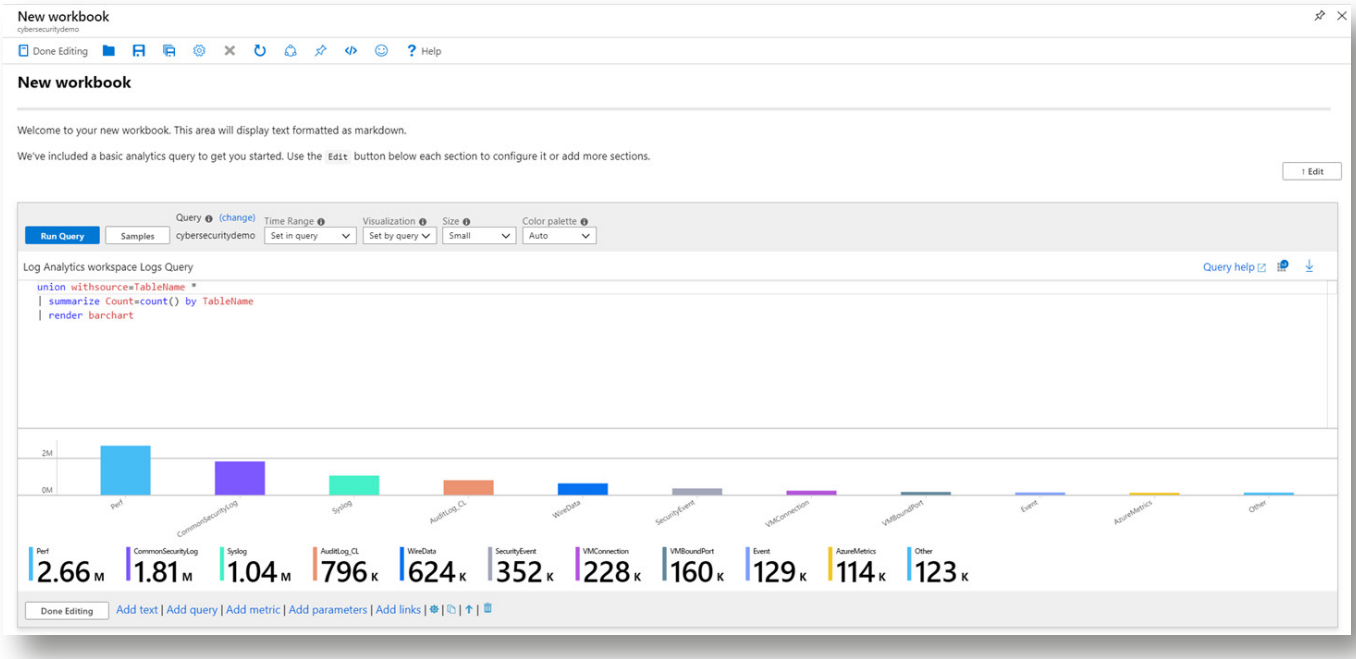
Sentinel-Benutzer können dazu integrierte Regeln anwenden, indem sie die entsprechende Liste nach dem Typ **„Initial Access"** filtern. Die Taktiken für die Regeln wie auch für die Suchabfragen basieren auf dem weltweit anerkannten Rahmenwerk MITRE ATT&CK® [16], das eine Datenbank mit Taktiken und Techniken enthält.

Die vorgefertigte Regel **„Anmeldeereignis von einem unbekannten Ort durch Benutzerkonto und authentifizierende Anwendung"** erzeugt eine Warnung, wenn es ungewöhnliche Anmeldungen durch einen Benutzer von Orten gibt, von denen aus er sich noch nie zuvor angemeldet hat. Dies könnte auf kompromittierte Zugangsdaten des Benutzers hindeuten, und dank der Korrelationsfunktionen von Fusion wird jede weitere schädliche Aktivität, die von dem betreffenden Konto ausgeht, korreliert und gemeldet.

Eine weitere Taktik zur Erkennung eines Identitätsmissbrauchs, ist die Überwachung auf Anmeldeversuche bei deaktivierten Konten. Dies kann darauf hindeuten, dass ein Angreifer versucht, eine missbräuchlich erlangte Datenbank mit Anmeldeinformationen zu nutzen, und auch wenn das Konto, das den Alarm ausgelöst hat, deaktiviert war, kann die Datenbank aktive Konten enthalten, die der Angreifer ausnutzen könnte. Durch den Einsatz fortschrittlicher Analyseregeln zur Überwachung der Azure AD-Anmeldungen oder anderer verbundener Online-Account-Verzeichnisdienste kann der Angriff einfach aufgespürt und mit erfolgreichen Anmeldungen seitens der IP des Angreifers korreliert werden, um festzustellen, ob der Sicherheitsbereich durchbrochen wurde. Die entsprechende Analyseregel ist bereits auf GitHub verfügbar.[17]



[16] [LAMCK]
[17] [LGAS]



Arbeitsmappen können auch dazu verwendet werden, Daten aus verschiedenen Quellen in einem Gesamtbericht darzustellen. Auf diese Weise können Übersichten zu komplexen Ressourcen oder Verknüpfungen zwischen verschiedenen Ressourcen leicht erstellt werden und angereicherte Daten und Einblicke liefern, die sonst nicht möglich wären. Eine Liste der in Azure Sentinel integrierten Arbeitsmappen findet sich unter **Templates** im Bereich Arbeitsmappen. Der Benutzer hat auch die Möglichkeit, eigene Arbeitsmappen zu erstellen, indem er unter **Workbooks** den Befehl **Add Workbook** auswählt.

Eine nützliche Arbeitsmappe ist die grafische Übersicht der Geolokalisierung von angreifenden IPs oder eine Karte mit Quellen der eingehenden Angriffe. Sicherheitsexperten können die Vorfälle korrelieren und herausfinden, ob es sich um einen koordinierten Angriff handelt, indem sie die Geolokalisierungsdaten[18] der IPs von potenziell böswilligen Ereignissen kartieren, wie z. B. den Versuch von bestimmten IPs aus, auf deaktivierte Konten zuzugreifen.

Suchanfragen – proaktive Suche und Aufdeckung von Bedrohungen und Schwachstellen in den Systemen

Eine weitere Möglichkeit, Bedrohungen und bestehende Schwachstellen aufzudecken, besteht darin, die vorhandenen, mit Azure Sentinel verbundenen Datenquellen zu nutzen, um mithilfe von Suchabfragen[19] einen tieferen Einblick in die Sicherheitslage und die Gefährdung zu gewinnen. Sicherheitsexperten sollten bei der Suche nach Bedrohungen und Schwachstellen proaktiv vorgehen. Aus diesem Grund bietet Azure Sentinel leistungsstarke Abfragetools, mit denen Benutzer in allen verbundenen Datensätzen nach Spuren suchen können, die auf aktive Bedrohungen und Schwachstellen hindeuten. Eine solche Suchabfrage kann den Analysten auch dabei helfen, den Datenstrom von den mit Azure Sentinel verbundenen Systemen und Sicherheitseinrichtungen besser zu verstehen. Das Ergebnis der Suchabfrage liefert zwar wertvolle Hintergrundinformationen zur Sicherheitslage der Organisation, es ist jedoch nicht besonders einfach, diese Daten zu analysieren und aussagekräftige Ereignisse aus ihnen herauszufiltern, die eine konkrete Warnung begründen können. Ein praktisches Beispiel hierfür ist eine Abfrage, die prüft, ob ungewöhnliche Prozesse auf Endpunkten im Netzwerk ausgeführt werden. Die Abfrageergebnisse können nicht unbedingt in eine Warnung überführt werden, aber sie wären im Rahmen einer Suchabfrage wertvoll, mit deren Hilfe der Sicherheitsexperte die Daten analysieren und die Prozesse untersuchen könnte.

Sentinel-Benutzer können die von Microsoft-Sicherheitsexperten erstellten integrierten Abfragen einsetzen, die sie dabei unterstützen, die richtigen Möglichkeiten zu nutzen, um Probleme im gesamten digitalen Bestand des Unternehmens aufzudecken. Fortgeschrittene Benutzer können auch die von der Sentinel-Community auf GitHub[20] bereitgestellten Open-Source-Abfragen anwenden, um proaktiv nach Bedrohungen zu suchen, und auf diese Weise ihre Sicherheitsbemühungen ausbauen, ohne dass sie über tiefer gehende Erfahrung mit Abfragen verfügen müssen. Die Ergebnisse der Suchabfragen können auch als Bookmark abgelegt[21] werden, um im Rahmen der Triage und weiteren Untersuchung verwendet zu werden.

Eine weitere Möglichkeit, auf den Azure Sentinel-Datenbestand zuzugreifen, sind die bereits integrierten Azure-API-Aufrufe in Jupyter Notebooks und Python. Sentinel-Anwender können die in Azure integrierte Jupyter-Funktionalität einsetzen, indem sie Azure Notebooks[22] verwenden, aber sie können ihre Azure Sentinel-Daten auch mit allen anderen Jupyter- oder Python-Tools verbinden, indem sie die API-Hooks für Azure einbinden.

---

[18] [LTHT]
[19] [LMHF]
[20] [LGASIC]
[21] [LMB]
[22] [LMAN]

Die Vorteile der Verwendung der fortschrittlichen Skripting- und Programmierumgebung liegen darin, dass sie einen flexibleren Ansatz für die Datenhaltung und die Möglichkeit der Anbindung anderer externer Quellen und Datenbanken bietet und eine breite Palette an Bibliotheken wie msticpy[23] (Microsoft Threat Intelligence Python Security Tools) und leistungsstarken Data-Engineering-Bibliotheken wie Pandas, NumPy und SciPy nutzt, um fortschrittliche Visualisierungen und Modelle für maschinelles Lernen zu managen und Daten auf einfache Weise in gängige Formate wie HTML, JSON und andere zu exportieren.

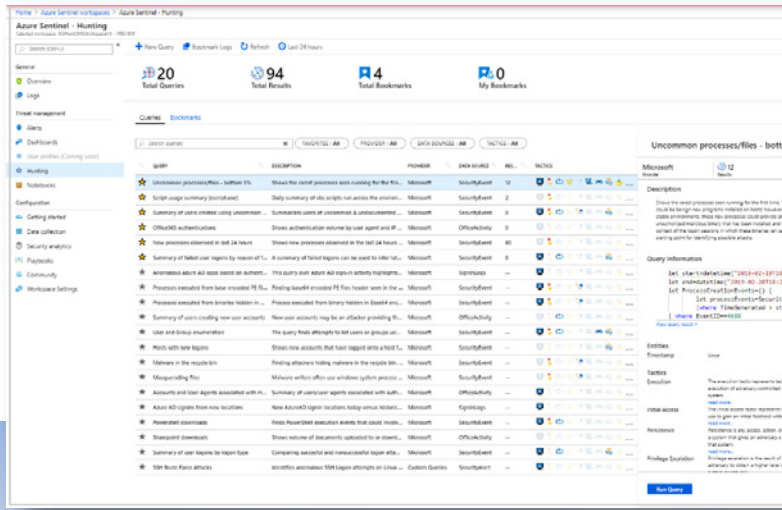
Praxisszenario:
Aufspüren von Malware

Wie bereits erwähnt, ist bei der Suche nach Sicherheitsbedrohungen ein proaktiver Ansatz erforderlich. Azure Sentinel-Anwender können auf die integrierten KQL-Suchabfragen zugreifen, indem sie den Eintrag Hunting unter Threat Management auswählen. Die Abfrage: Uncommon processes/files – bottom 5 %, durchsucht beispielsweise die Protokolle von Endpunkten und Servern, die mit Azure Sentinel verbunden sind, um auffällige Prozesse auf diesen Rechnern zu ermitteln, die zum ersten Mal ausgeführt wurden. Das Ergebnis dieser Abfrage kann aber auch harmlose, neu installierte Programme oder Anwendungen auf Hosts enthalten. Allerdings können diese Prozesse auch zur Verbreitung von Malware, Ransomware und anderen bösartigen ausführbaren Programmen führen, die in den Sicherheitsbereich eingedrungen sind. Wenn ein Sicherheitsexperte feststellt, dass einer dieser Prozesse tatsächlich schädlich ist, kann eine Liste der Computer, auf denen dieser Prozess läuft, erstellt und diese im nächsten Schritt auf verdächtige Logins untersucht werden, um festzustellen, wann und wie sie kompromittiert wurden.

Zur weiteren Untersuchung von potenziellen Schwachstellen können SOCs Azure Notebooks einsetzen, um eine Verbindung zu den Daten aus Sentinel herzustellen und komplexe Datenquellen mit leistungsstarken Skriptsprachen wie Python zu managen. In einem realen Szenario würde Azure Notebook für den mehrfachen Einsatz von einem Sicherheitsexperten oder einem Analysten der Stufe 3 eingerichtet und dann von Analysten der Stufen 1 und 2 von Fall zu Fall wiederverwendet bzw. angepasst werden. Dieses leistungsstarke Tool vereinfacht die Bewertung und Untersuchung von Schwachstellen durch die Bereitstellung eines fertigen Workflows. Notebooks können dabei individuell an die Bedürfnisse der Organisation angepasst werden. In Azure Sentinel finden Benutzer dazu Beispiele unter Notebooks im Abschnitt Threat Management. Viele weitere Notebooks sind auch in der Azure Sentinel-Community auf GitHub[24] zu finden. Ein gutes Beispiel für die Vorteile von Azure Notebooks ist die Korrelation der IP-Verbindungen verdächtiger bösartiger Prozesse, die im vorigen Beispiel erwähnt wurden, mit externen Quellen wie der Datenbank bekannter bösartiger Quellen von Malware und den Ransomware-Command- und -Control-Servern von VirusTotal. Dies kann den Sicherheitsexperten dabei helfen, Malware zu identifizieren, die in das Netzwerk eingedrungen ist, und es ermöglichen, den Angriff durch Blockieren der bösartigen IP in der Firewall zu unterbinden.

[23] [LMMS]

[24] [LGASIC]



Untersuchen – Triage von Sicherheitsvorfällen

Sobald Warnungen in der Erkennungsphase ausgelöst werden, generiert die leistungsstarke Korrelationsfunktionalität von Sentinel Vorfälle, die von Sicherheitsexperten detailliert analysiert werden können, indem sie die Ursache, die Auswirkungen und den Schweregrad einer Sicherheitsverletzung ermitteln. Ein Untersuchungsdiagramm macht es möglich, festzustellen, wie die betroffenen Elemente miteinander verbunden sind und wie sich die Ausbreitung des Angriffs darstellt.

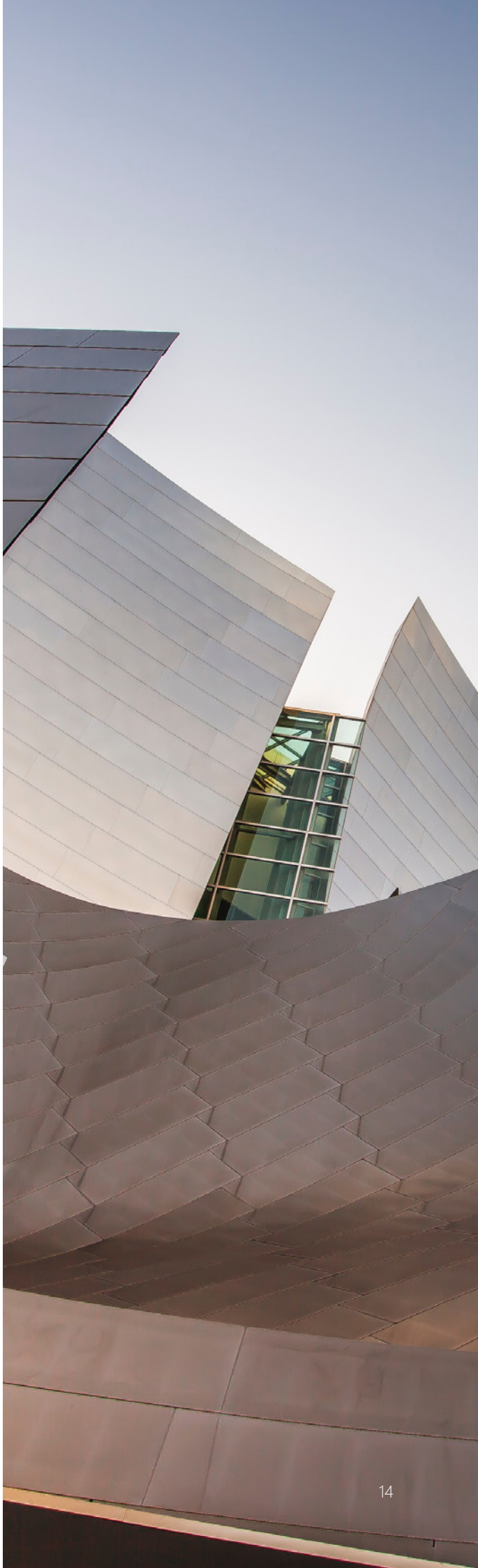
Vorfälle – Verbindung der Ansatzpunkte eines Sicherheitsverstoßes im Untersuchungsdiagramm

Das Aufdecken einer Sicherheitsbedrohung durch regelbasierte Warnungen und Suchabfragen ist für Sicherheitsteams nur ein Teil der Herausforderungen. Vorfälle werden automatisch auf der Basis von Warnungen generiert, die aufgrund von in der Sicherheitsanalyse definierten Merkmalen ausgelöst werden.

Mit Azure Sentinel können IT-Teams tiefe Einblicke in die Beziehungen und Verbindungen zwischen Warnungen, Bookmarks und Entitäten gewinnen. Die weitere Untersuchung kann durch Öffnen des Menüs **Incidents** eingeleitet werden, wo eine Reihe registrierter Sicherheitsvorfälle zu finden ist. Ein Vorfall[25] kann mehrere Warnungen enthalten und umfasst eine Zusammenstellung relevanter Anhaltspunkte und Verbindungen für die Analyse. Vorfälle werden automatisch in ihrem Schweregrad bewertet und kategorisiert und können Analysten zur detaillierten Untersuchung zugewiesen werden.

Um einen Vorfall im Detail zu untersuchen, kann ein Analyst ein **Untersuchungsdiagramm** verwenden, um den Angriffsvektor, die betroffenen Benutzer, Systeme und Anwendungen mithilfe von integrierten Untersuchungsschritten und Abfragen zu visualisieren. Das Untersuchungsdiagramm ist auch nützlich, um Benutzer und Domänen in der Infrastruktur des Unternehmens in Zusammenhang mit dem Vorfall zu bringen, um das Ausmaß der Kompromittierung zu ermitteln. Abfragen können direkt im Diagramm ausgeführt werden, um dadurch den Umfang der Untersuchung zu erweitern und weitere Anomalien aufzudecken. Anwender können die automatische URL-Detonation[26] von Sentinel nutzen, um Links zu untersuchen, die an die Organisation gesendet wurden, um auf diese Weise Phishing-Versuche und Malware zu erkennen.

[25] [LMMI]
[26] [LMURL]

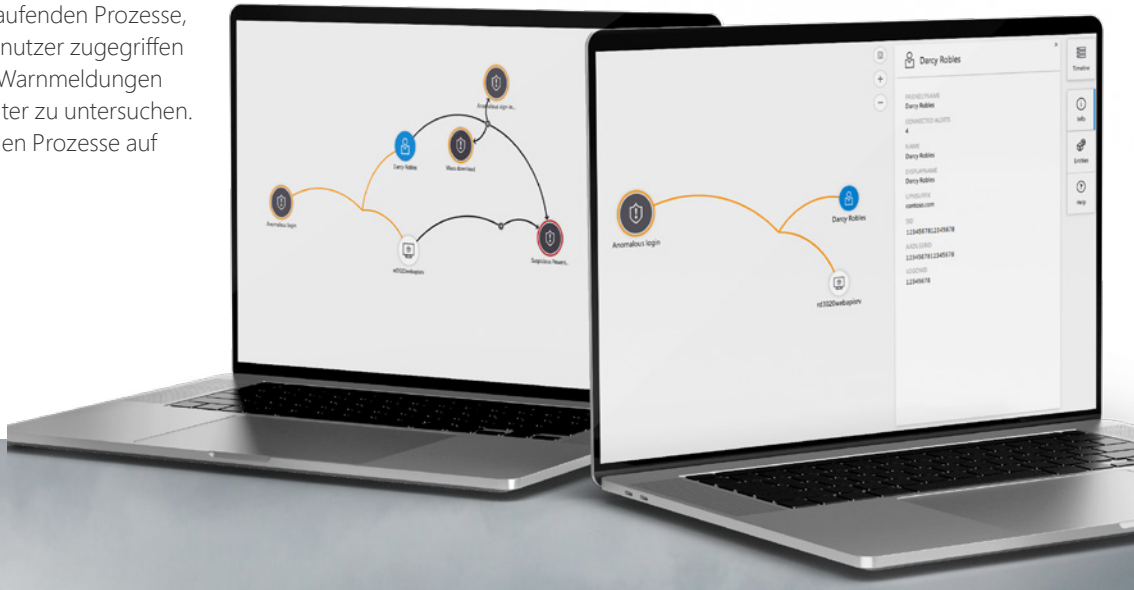


Praxisszenario:
Aufdecken einer Datenschutzverletzung

Sentinel leitet Benutzer an, die richtigen Fragen zu stellen, um den Umfang, die Ursache und die potenziellen Auswirkungen der Sicherheitsverletzung besser zu verstehen, indem die Anwendung einen visuellen Kontext zu den Rohdaten der Warnung liefert und es den Benutzern ermöglicht, Verbindungen zwischen verschiedenen Datenquellen zu erkennen. Analysten können Vorfälle in einem Schritt verfolgen und miteinander verbinden. Zum Beispiel würde ein Sicherheitsexperte, der eine Warnung zu einem Vorfall untersucht, die von einem verdächtigen Anmeldevorgang aus Azure-Active-Directory-Protokollen stammt, im Untersuchungsdiagramm die Identität des Benutzers, der die Warnung ausgelöst hat, und die Anwendung oder den Computer, auf dem der Benutzer angemeldet ist, erkennen.

Von dort aus wäre der Sicherheitsexperte in der Lage, die auf dem Zielcomputer laufenden Prozesse, weitere Endpunkte, auf die der Benutzer zugegriffen hat, und alle damit verbundenen Warnmeldungen für den Benutzer oder die Computer zu untersuchen. Bei der Untersuchung der laufenden Prozesse auf Zielcomputern kann ein Sicherheitsexperte verwandte Warnmeldungen ermitteln, wie z. B. Warnmeldungen der Endpoint Security Center, d. h. Warnmeldungen zu verdächtiger Software oder Skripten, die auf dem Computer ausgeführt werden. Bei der Untersuchung der digitalen Identität eines Benutzers können Sicherheitsexperten verwandte Warnmeldungen von Office 365 identifizieren, wie z. B. die Warnmeldung „Massendownload" von SharePoint, die ein Hinweis auf einen Datendiebstahl sein kann.

Mittels Triage können Sicherheitsexperten schnell einen vollständigen Bericht über die Sicherheitsverletzung erstellen, indem sie die durch das Untersuchungsdiagramm bereitgestellten Möglichkeiten und Tools nutzen.



Reagieren – Beschleunigen und verbessern Sie die Reaktion Ihres SOC

Sentinel ermöglicht es IT-Teams, Reaktionen auf Sicherheitsvorfälle zu automatisieren, indem die integrierten Azure Logic Apps und die Fähigkeit genutzt werden, eine automatische Reaktion auf eine Warnung oder die Untersuchung eines Vorfalls auszulösen. Benutzer können dabei Bedingungen definieren, die eine Reihe von Prozeduren als Reaktion auf eine Warnung ausführen. Ein Sicherheits-Playbook ermöglicht dabei die Automatisierung und Orchestrierung der Reaktion.

Automatisierung – Playbooks für die fortgeschrittene Orchestrierung

Die schnelle Reaktion auf Sicherheitsbedrohungen erfordert einen hohen Grad an Automatisierung, um einen Angriff zu stoppen und einzudämmen. Azure Sentinel nutzt integrierte Azure Logic Apps[27], um die Bedrohungsreaktion zu orchestrieren und automatisch zu starten, sobald bestimmte Warnungen ausgelöst werden. Sentinel-Anwender können Playbooks erstellen, um komplexe Abläufe zu steuern, die das Versenden von Benachrichtigungen, das Erstellen von Vorfällen und das Anfordern von Freigaben umfassen, oder Vorfälle automatisch bearbeiten, indem sie Konten sperren und Kennwörter zurücksetzen. Die Playbook-Funktion nutzt den Logic App Designer, um mehrere vom Benutzer definierte Aktionen in einem Ablauf zusammenzufassen. Der Logic App Designer macht die Erstellung und Bearbeitung von Playbooks besonders einfach und benutzerfreundlich.

Beispiel aus der Praxis

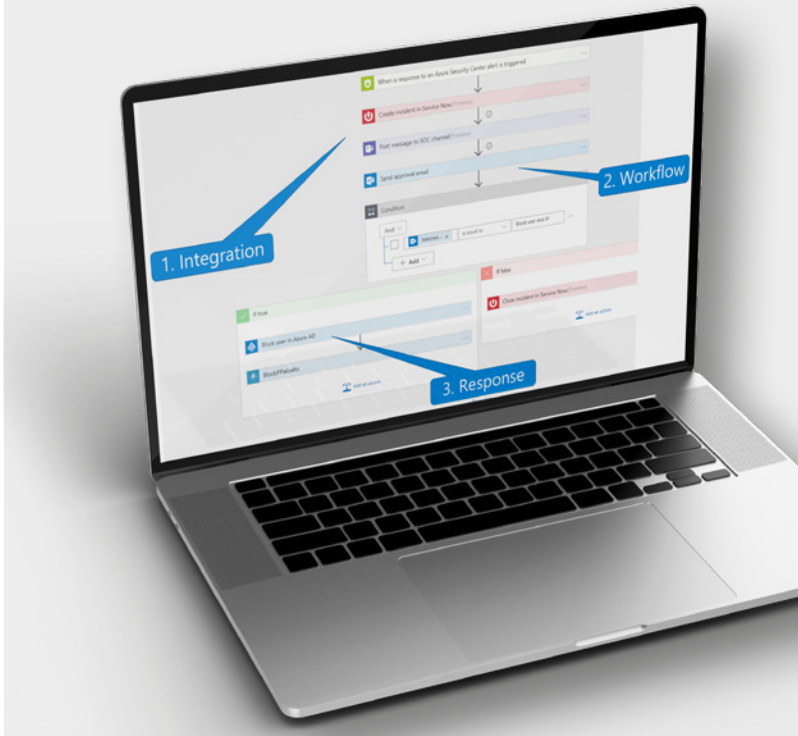
Um ein Playbook zu erstellen[28], muss der Benutzer das Menü **Playbooks** auswählen und eine Logic App erstellen, die den Anforderungen und der Struktur der Organisation entspricht, oder prüfen, ob bereits eine Lösung auf Azure Sentinels GitHub[29] existiert. Sentinel-Playbooks können dann manuell über das Playbook-Menü ausgeführt werden oder so konfiguriert werden, dass sie beim Auftreten eines Vorfalls automatisch ausgeführt werden.

Ein Playbook hilft dem SOC bei der automatischen Bearbeitung eines Vorfalls und ermöglicht eine schnelle und zuverlässige Reaktion. Ein Beispiel für die umfassenden Möglichkeiten von Azure Sentinel ist das folgende Szenario:

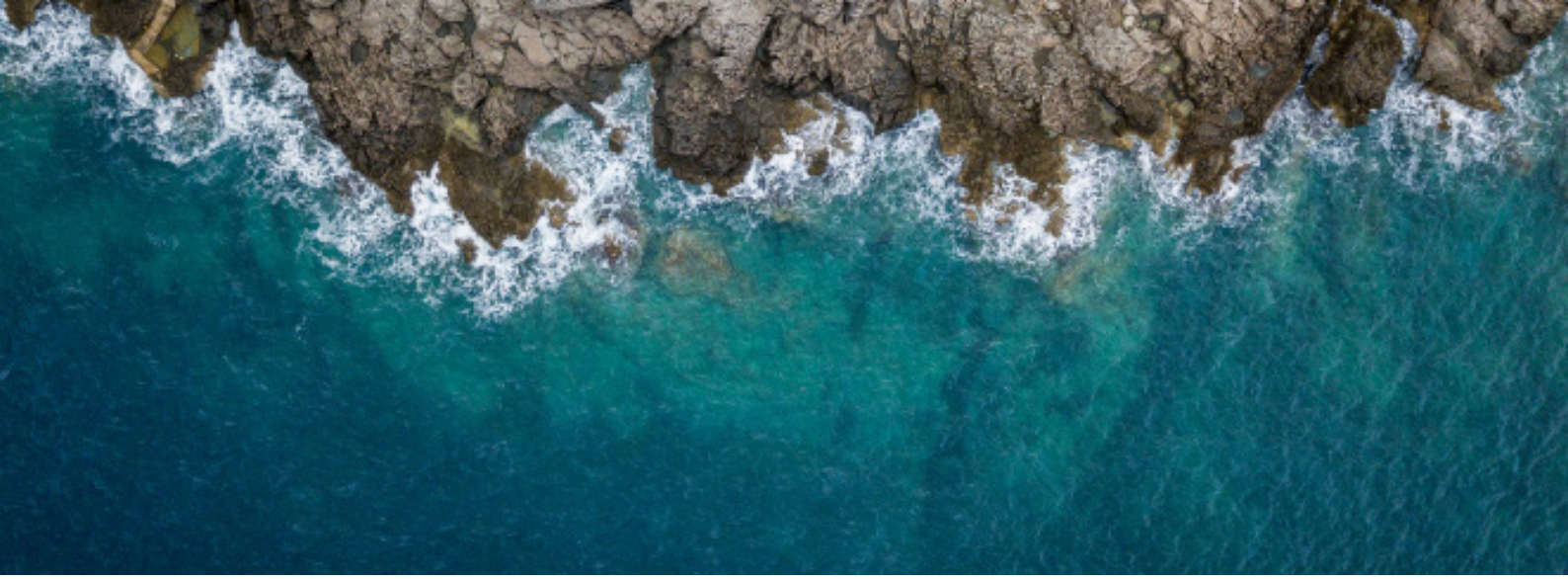
Bei einer Suchabfrage hat ein Sicherheitsexperte eine böswillige IP identifiziert, über die mehrfach gescheiterte Anmeldeversuche initiiert wurden,[30] um auf ein internes Konto zuzugreifen. In diesem Fall kann ein Playbook entweder automatisch oder manuell durch einen Analysten ausgelöst werden und folgende Schritte ausführen:

1. Erstellen eines Vorfalls in der ITSM-Lösung des Unternehmens und Senden einer Nachricht an Microsoft Teams oder einen anderen Messaging-Service, um das SOC-Team über den Angriff zu informieren.

2. Senden einer E-Mail mit der Nummer des Vorfalls und begleitenden Informationen der Warnmeldung an das Netzwerkadministrationsteam. Die E-Mail-Nachricht enthält auch zwei Schaltflächen mit den Optionen „Blockieren" oder „Ignorieren". Wenn die Administratoren „Blockieren" wählen, wird die IP-Adresse in der Firewall blockiert und der Benutzer in Azure AD deaktiviert. Bei der Wahl von „Ignorieren" wird die Warnung in Azure Sentinel geschlossen, ebenso wie das betreffende Ticket im ITSM-System.



[27] [LMOLA]
[28] [LMSAT]
[29] [LGASP]
[30] [LGPB]

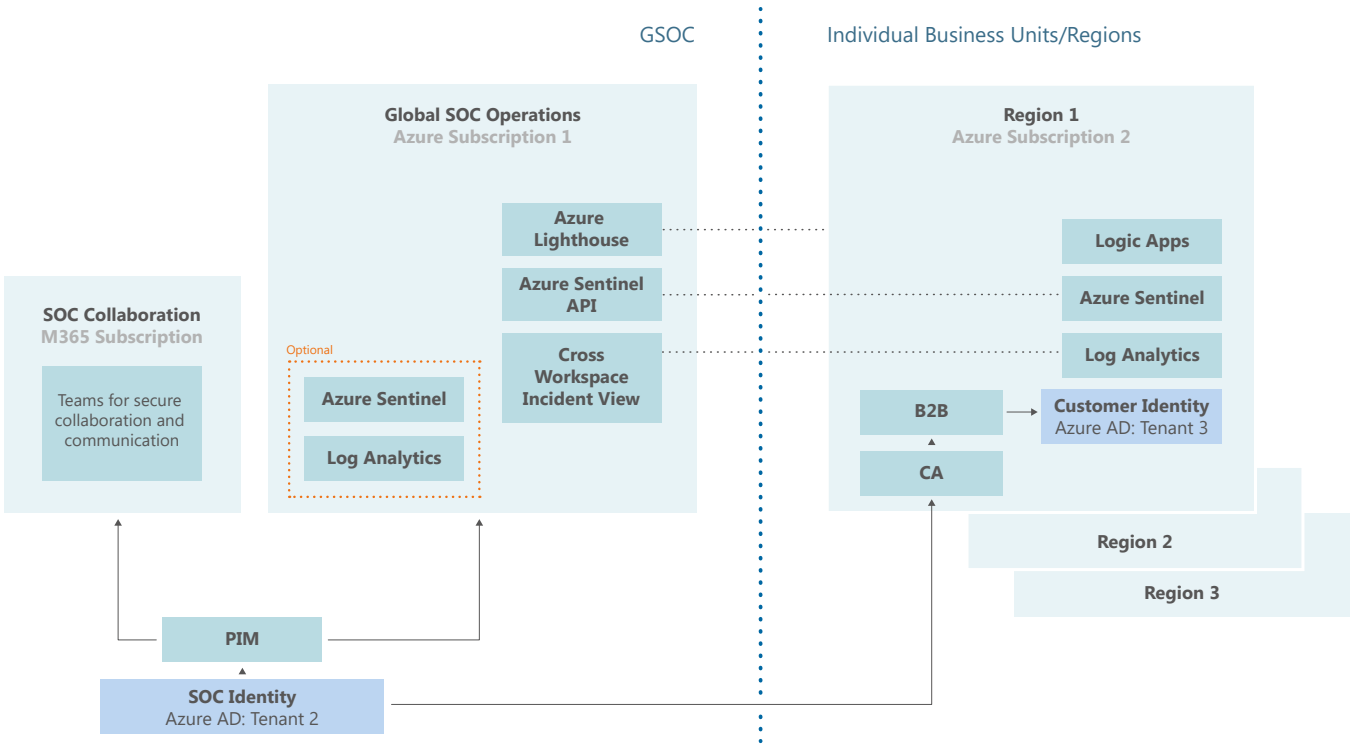


Integration in ein bestehendes Security Operations Center

Azure Sentinel ist so konzipiert, dass mithilfe der umfassenden Sentinel-API[31] eine einfache Integration in bestehende SOC-Infrastrukturen möglich ist. Zudem ist Azure Sentinel mandantenfähig[32], sodass es Unternehmen, die über mehrere Azure-Abonnements verfügen, möglich ist, die Datenerfassung von Microsoft- und Azure-SaaS-Ressourcen über die Grenzen des Azure Active Directory (Azure AD) hinweg innerhalb von Azure abzudecken. Auf diese Weise kann ein global arbeitendes SOC Ressourcen aus anderen Geschäftsbereichen oder Regionen integrieren, die über ein eigenes Azure-Abonnement verfügen.

Darüber hinaus können Managed Security Service Provider (MSSP) die Azure-Sentinel-Daten ihrer Kunden in ihren eigenen Mandanten integrieren[33], ohne sich über die Azure-Lighthouse[34]-Technologie direkt mit dem ausländischen Mandanten verbinden zu müssen.

Dies ermöglicht es global arbeitenden SOCs oder MSSPs, Vorfälle über mehrere Azure Sentinel-Workspaces hinweg zu verfolgen, ohne direkt auf Kundendaten zugreifen zu müssen, wodurch eine detaillierte Zugriffssteuerung möglich ist.



[31] [LIBAPI]
[32] [LIBSWT]
[33] [LIBMSSP]
[34] [LIBAZL]

Azure Sentinel unterstützt ein dreistufiges SOC-Modell auf der Basis einer rollenbasierten Zugriffskontrolle (Azure RBAC), um Zugriffsberechtigungen für Benutzer, Gruppen und Anwendungen innerhalb von Azure Sentinel zu gewähren. Dies ermöglicht es, den Sicherheitsteams selektiv die Rechte zuzuweisen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Modelle stellen sich wie folgt dar:

Tier	Operations	Azure-Sentinel-Rolle	Erstellen und ausführen von Playbooks	Erstellen und Bearbeiten von Playbooks, Analyseregeln und anderen Azure Sentinel-Ressourcen	Verwalten von Vorfällen (Verwerfen, Zuweisen usw.)	Daten, Vorfälle, Arbeitsmappen und andere Azure Sentinel-Ressourcen anzeigen
Tier 1 **High-Speed-Abhilfe**	Sicherheitsexperten, die Vorfälle priorisieren und aktuelle Warnungen prüfen, um deren Relevanz und Dringlichkeit zu bestimmen.	Azure Sentinel Reader	X	X	X	✓
Tier 2 **Tiefer gehende Analyse und Abhilfe**	Tier-2-Analysten, die Warnungen überprüfen und Untersuchungen durchführen, um betroffene Systeme und das Ausmaß des Angriffs zu identifizieren.	Azure Sentinel Responder	X	X	✓	✓
Tier 3 **Proaktive Suche und fortgeschrittene Forensik**	Sicherheitsexperten, die den gesamten digitalen Bestand untersuchen, um verborgene Bedrohungen aufzudecken und Schwachstellentests durchzuführen.	Azure Sentinel Contributor + Logic App Contributor	✓	✓	✓	✓

Kosten von Azure Sentinel

Mit dem cloud-nativen Azure Sentinel müssen Unternehmen nicht mehr in kostspielige SIEM-Lizenzgebühren investieren und tragen keine hohen Anfangskosten wie bei On-Premise-Lösungen in Form von physischer Infrastruktur wie Server, Speicher, Patch-Management usw. und die damit verbundenen Virtualisierungs- und Betriebssystem-Lizenzkosten.

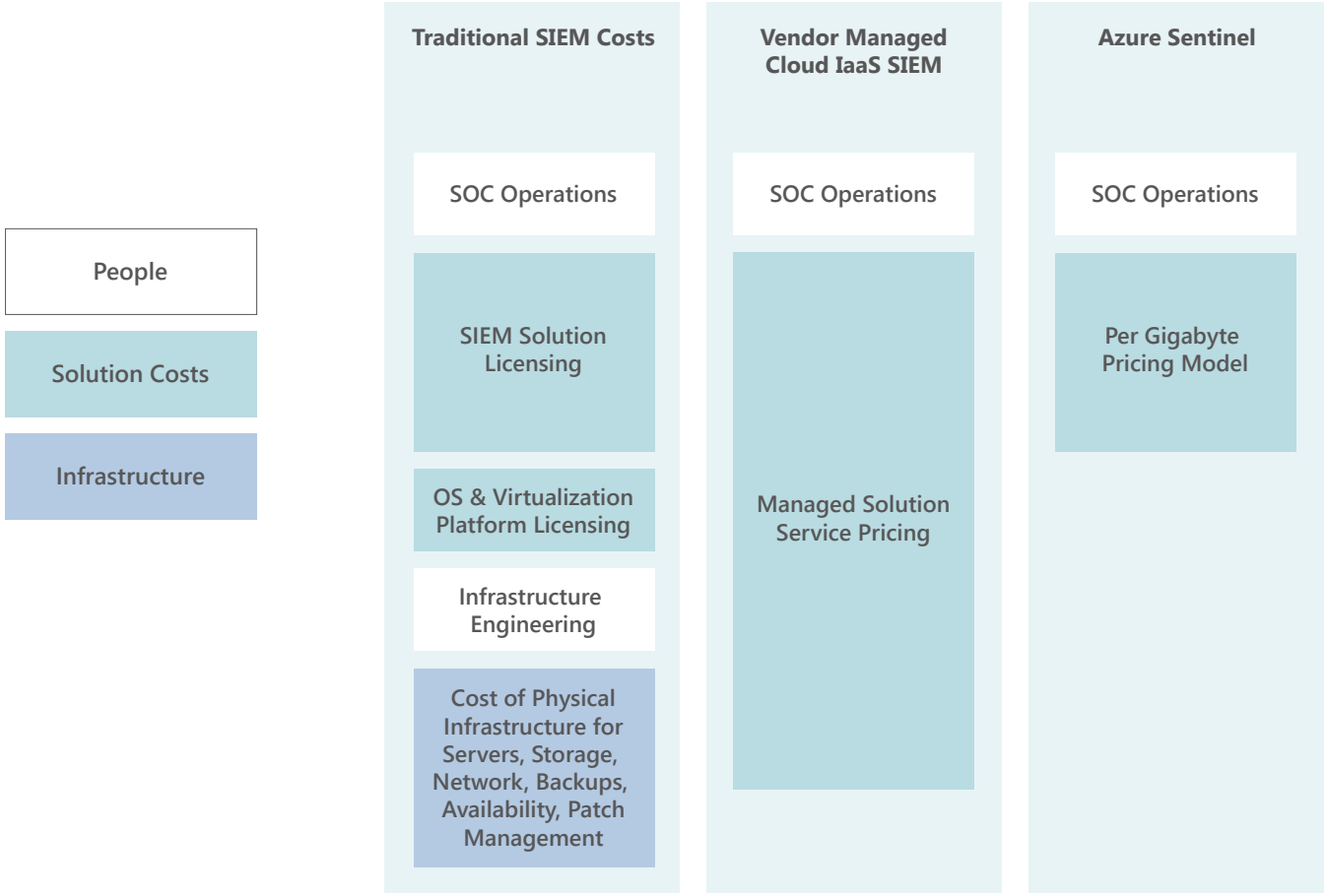
Azure Sentinel beruht auf dem Prinzip „bezahle für das, was du nutzt". Die Kosten basieren ausschließlich auf dem Volumen erfasster Daten, die in Azure Sentinel analysiert und im Log-Analytics-Arbeitsbereich gespeichert werden. Sentinel-Anwender können mit Hilfe des Kostenrechners die Höhe der nächsten Rechnung ermitteln.

Zudem besteht die Möglichkeit einer Preisgestaltung auf der Basis von reservierten Kapazitäten. Dabei handelt es sich um Lizenzen mit fester Gebühr, die für die genutzte Kapazität anfällt. Die Kapazität umfasst die Menge der pro Tag erfassten Daten.

Auf der Grundlage dieser Preisgestaltung können auch kleinere Organisationen von den Vorteilen profitieren, indem sie einerseits die Kosten im Auge behalten und andererseits einen sicheren Betrieb gewährleisten. Größere Organisationen und Unternehmen sollten auch die Preisnachlässe berücksichtigen, die mit der Nutzung von reservierten Kapazitäten einhergehen, was dieses Modell besonders für Produktionsumgebungen vorteilhaft macht. Azure Sentinel kann ohne zusätzliche Kosten auf einer Azure Monitor Log Analytics Workstation für 31 Tage kostenlos aktiviert werden. Die Gebühren, die bei Azure Monitor Log Analytics für die Datenerfassung und die zusätzlichen Funktionen zur Automatisierung und die Einbindung eigener Funktionen zum maschinellen Lernen anfallen, werden auch während der kostenlosen Testphase in Rechnung gestellt.

Zudem ist es erforderlich, die entsprechenden Lizenzen zu erwerben, um Daten aus den Audit-Logs von Office 365, den Azure Activity-Logs und den Warnmeldungen von Microsoft-Lösungen zum Schutz vor Bedrohungen in Azure Sentinel zu erfassen. Azure Sentinel kann nur dann Daten aus Berichten erfassen, wenn die erforderlichen Lizenzen verfügbar sind.

Die Azure AD Audit-Logs können im Azure-Portal eingesehen und mit der kostenlosen Testversion von Azure AD in Azure Sentinel erfasst werden. Darüber hinaus ist eine Azure-AD-Premium-1- oder -Premium-2-Lizenz für die Azure-AD-Anmeldeprotokolle erforderlich.



In Zukunft erfordern Sicherheitsanalysen einen höheren Grad an Automatisierung und maschinellem Lernen

Angesichts der heutigen Cyberbedrohungen sind Sicherheitsteams mit einer ständigen Flut eingehender Risiken konfrontiert. Um damit fertig zu werden und um Angriffe schnell und genau erkennen, aber auch angemessen darauf reagieren zu können, ist ein datengestütztes und von Mitarbeitern gesteuertes Sicherheitskonzept notwendig.

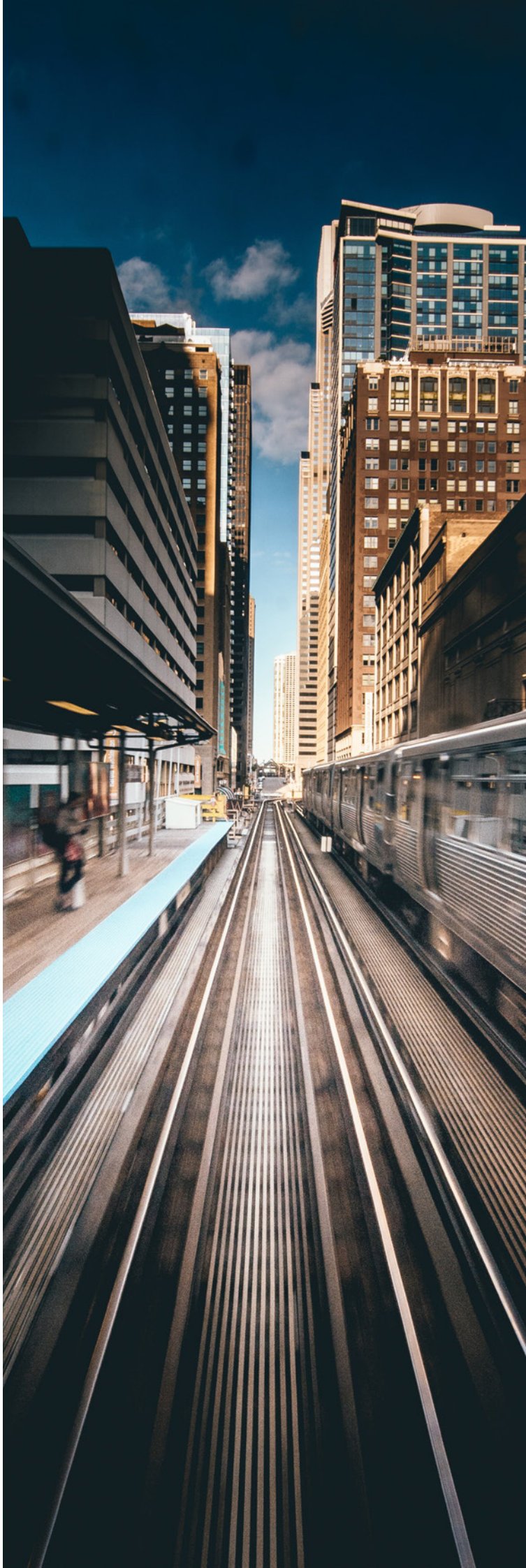
Auf der Basis des globalen Netzwerks aus Echtzeit-Bedrohungsinformationen von Microsoft und historischen Daten Ihres Netzwerks aus den letzten 30 Tagen entwickelt sich Sentinel ständig weiter, kann Risiken vorhersehen und ist somit immer einen Schritt voraus. Durch das integrierte maschinelle Lernen und den Einsatz fortschrittlicher Sicherheitsanalysen sowie mit ihren umfangreichen Erfahrungen können Sicherheitsexperten mit agilen, adaptiven Verteidigungssystemen erfolgreich darauf reagieren.

Darüber hinaus passt sich Azure Sentinel dem Wachstum des digitalen Bestands eines Unternehmens an und ermöglicht durch die Nutzung von GitHub[35] die einfache Zusammenarbeit mit einer großen Community, um Analyseregeln, Suchabfragen, benutzerdefinierte Arbeitsmappen und Playbooks auszutauschen.

Auch wenn Cyberbedrohungen und -angriffe weiterhin die Unternehmen belasten, wird Sentinel dank der leistungsstarken Kombination aus datengesteuerter Maschinenintelligenz und menschlichem Fachwissen zunehmend intelligenter.

---

[35] [LGASIC]



avanade

Abkürzungen und Begriffe

Begriff	Abkürzung	Definition
Security Operations Center	SOC	Das Security Operations Center ist ein Kontrollzentrum, das für den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation verantwortlich ist.
Security Information and Event Management	SIEM	Security Information and Event Management ist ein Ansatz für das Sicherheitsmanagement der SIM(Security Information Management)- und SEM(Security Event Management)-Funktionen, d. h. die Verwaltung von Sicherheitsinformationen und -ereignissen in einem Sicherheitsmanagementsystem kombiniert. Siemens verwendet derzeit das Splunk-SIEM-System.
Security Orchestration, Automation and Response	SOAR	Security Orchestration, Automation and Response (Sicherheitsorchestrierung mit automatisierter Reaktion) ist eine Kombination kompatibler Programme, die es einer Organisation ermöglicht, Daten über Sicherheitsbedrohungen aus einer Vielzahl von Quellen zu sammeln.
Active Directory	AD	Active Directory ist ein Verzeichnisdienst von Microsoft für Windows-Netzwerke. Active Directory ermöglicht es, die Struktur einer Organisation abzubilden und die Nutzung von Netzwerkressourcen oder -objekten zentral zu verwalten.
Künstliche Intelligenz	KI	Künstliche Intelligenz bezieht sich auf die Simulation menschlicher Intelligenz mittels Maschinen, die darauf programmiert sind, wie Menschen zu denken und ihre Handlungen nachzuahmen.
Informationstechnologie	IT	Informationstechnologie ist die Verwendung von Computern, Speicher-, Netzwerk- und anderen physischen Geräten, Infrastrukturen und Prozessen zur Erstellung, Verarbeitung, Speicherung, Sicherung und zum Austausch aller Arten von elektronischen Daten.
Internet of Things	IoT	Das Internet of Things (Internet der Dinge) ist ein System miteinander verbundener Geräte, Objekte, Tiere oder Menschen, die mit eindeutigen IDs (UIDs) und der Fähigkeit ausgestattet sind, Daten über ein Netzwerk zu übertragen, ohne dass eine Interaktion von Mensch zu Mensch oder von Mensch zu Maschine erforderlich ist.
Software-as-a-Service	SaaS	Software-as-a-Service – auch als cloud-basierte Software bekannt – ist eine Methode der Softwarebereitstellung, die es ermöglicht, von jedem Gerät mit Internetanschluss und einem Webbrowser auf Daten zuzugreifen. In diesem webbasierten Modell hosten und warten Softwareanbieter die Server, Datenbanken und den Code, aus denen eine Anwendung besteht.
Infrastructure-as-a-Service	IaaS	Infrastructure-as-a-Service bietet dem Nutzer die typischen Komponenten einer Rechenzentrumsinfrastruktur wie Hardware, Rechenleistung, Speicherplatz oder Netzwerkressourcen aus der Cloud.
Platform-as-a-Service	PaaS	Platform-as-a-Service bezieht sich auf eine Cloud-Umgebung, die eine Plattform zur Entwicklung von Anwendungen im Internet bietet.
Amazon Web Services	AWS	Amazon Web Services ist eine Tochtergesellschaft von Amazon, die Cloud-Computing-Plattformen und APIs nach Bedarf für Einzelpersonen, Unternehmen und Regierungen auf Pay-as-you-go-Basis zur Verfügung stellt.
International Business Machines Corporation	IBM	Die International Business Machines Corporation ist ein multinationales Technologieunternehmen mit Sitz in den Vereinigten Staaten, das Software, Computerhardware, Infrastrukturservices und Beratungsleistungen anbietet.
Kusto Query Language	KQL	Kusto Query Language ist eine einfache, aber mächtige Sprache zur Abfrage von strukturierten, semistrukturierten und unstrukturierten Daten.
Structured Query Language	SQL	Die Abfrage baut auf Entitäten auf, die in einer SQL-ähnlichen Hierarchie organisiert sind: Datenbanken, Tabellen und Spalten. Structured Query Language ist eine Standardsprache für den Zugriff auf und die Manipulation von Datenbanken.
Azure Active Directory	Azure AD/AAD	Azure Active Directory ist Microsofts cloud-basierter Identitäts- und Zugriffsverwaltungsdienst, der Endbenutzer bei der Anmeldung und beim Zugriff auf Ressourcen unterstützt, z. B.: • externe Ressourcen, wie Microsoft Office 365, das Azure-Portal und tausende anderer SaaS-Anwendungen, • interne Ressourcen, wie z. B. Anwendungen in einem Unternehmensnetzwerk oder Intranet, sowie alle Cloud-Anwendungen, die von der eigenen Organisation entwickelt wurden.
Managed Security Service Provider	MSSP	Ein Managed Security Service Provider ist ein externer Anbieter, der einer Organisation Remote-Software/Hardware-basierte Informations- oder Netzwerksicherheitsservices zur Verfügung stellt. Ein MSSP hostet, implementiert und verwaltet die Sicherheitsinfrastruktur und stellt gleichzeitig Informationssicherheitsservices für einen Kunden bereit.
Information Technology Service Management	ITSM	ITSM sind die Aktivitäten, die von Organisationen durchgeführt werden, um IT-Dienstleistungen, die Kunden und Partnern angeboten werden, zu entwerfen, zu planen, bereitzustellen, zu betreiben und zu kontrollieren.

Zitierte Quellen

Abkürzung	Quelle
[LiDefense]	Accenture (2019). IDefense Accenture Security. Abgerufen unter: https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
[LIBM]	IBM (2019). Cost of Data Breach Report. Abgerufen unter: https://databreachcalculator.mybluemix.net/
[LACOC]	Accenture (2019). The Cost of Cybercrime. Abgerufen unter: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cyber-crime-Study-Final.pdf#zoom=50
[LMTIR]	Microsoft Security Intelligence Report, Microsoft Threat Intelligence, www.microsoft.com/en-us/security/business/security-intelligence-report
[LMCJR]	Steve Morgan, Cybersecurity Ventures (2019). 2019/2020 Cybersecurity Jobs Report. Abgerufen unter: https://www.herjavecgroup.com/wp-content/uploads/2019/10/HG-CV-2019-Cybersecurity-Jobs-Report.pdf
[TCSG]	Ofer Shezaf, Microosft Azure Sentinel: The connectors grand (CEF, Syslog, Direct, Agent, Custom and more) (2019), Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-the-connectors-grand-cef-syslog-direct-agent/ba-p/803891
[LGASIC]	GitHub. Azure Sentinel. Abgerufen unter: https://aka.ms/ASICommunity
[LMCDS]	Microsoft (04.11.2019). Connect data sources to Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources
[LMCL]	Microsoft (07.08.2019). Azure Sentinel: Collecting logs from Microsoft Services and Applications. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-collecting-logs-from-microsoft-services-and/ba-p/792669
[LMCS]	Microsoft (19.08.2019). Azure Sentinel: Collecting from Servers and workstations. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-agent-collecting-from-servers-and-workstations-on/ba-p/811760
[LMSC]	Microsoft (13.08.2019). Azure Sentinel: Syslog, CEF, Logstash and other 3rd party connectors grand list. Abgerufen unter: https://techcommunity.microsoft.com/t5/Azure-Sentinel/Azure-Sentinel-Syslog-CEF-and-other-3rd-party-connectors-grand/ba-p/803891
[LMCC]	Microsoft (19.09.2019). Azure Sentinel: Creating Custom Connectors. Abgerufen unter: https://techcommunity.microsoft.com/t5/Azure-Sentinel/Azure-Sentinel-Creating-Custom-Connectors/ba-p/864060
[LMDT]	Microsoft (23.09.2019). Investigate alerts with Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in
[LMCA]	Microsoft (20.02.2020). Create Custom analytic rules to detect suspicious threats with Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom
[LGAS]	GitHub. Azure-Sentinel/SigninAttemptsByIPviaDisabledAccounts.yaml. Abgerufen unter: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SigninLogs/ SigninAttemptsByIPviaDisabledAccounts.yaml
[LMVA]	Microsoft (04.05.2020). Visualize your data using Azure Monitor Workbooks in Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data
[LTHT]	Microsoft (01.11.2019). Hot to use Azure Monitor Workbooks to map Sentinel data. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/how-to-use-azure-monitor-workbooks-to-map-sentinel-data/ba-p/971818
[LMHF]	Microsoft (09.10.2019). Hunting capabilities in Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-gb/azure/sentinel/hunting
[LAMCK]	MITRE. MITRE ATT&CK. Retrieved from https://attack.mitre.org/
[LMB]	Microsoft (24.10.2019). Use hunting bookmarks for data investigations in Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-gb/azure/sentinel/bookmarks
[LMAN]	Microsoft. Microsoft Azure Notebooks. Abgerufen unter: https://notebooks.azure.com/

Abkürzung	Quelle
[LMII]	Microsoft (23.09.2019). Azure Sentinel: Creating Custom Connectors. Abgerufen unter: https://techcommunity.microsoft.com/t5/Azure-Sentinel/Azure-Sentinel-Creating-Custom-Connectors/ba-p/864060
[LMURL]	Microsoft (11.11.2019). Using the new built-in URL detonation in Azure Sentinel. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/using-the-new-built-in-url-detonation-in-azure-sentinel/ba-p/996229
[LMOE]	Microsoft (13.02.2020). Office 365 Email Activity and Data Exfiltration Detection. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/office-365-email-activity-and-data-exfiltration-detection/ba-p/1169652
[LMOLA]	Microsoft (11.03.2020). Automate tasks for enterprise integration – Azure Logic Apps. Abgerufen unter: https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-overview
[LMSAT]	Microsoft (18.02.2019). Tutorial: Run a playbook in Azure Sentinel. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook
[LGASP]	GitHub. Azure/Azure-Sentinel/Playbooks. Abgerufen unter: https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks
[LGPB]	GitHub. Azure/Azure-Sentinel – Potential brute force. Abgerufen unter: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/Syslog/ssh_potentialBruteForce.yaml
[LMMS]	Microsoft (17.06.2019). msticpy – Python Defender Tools. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/msticpy-python-defender-tools/ba-p/648929
[LFUS]	Microsoft. Azure Sentinel Fusion Technology. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/fusion
[LIBAPI]	Sarah Young, Microsoft (07.08.2020). Azure Sentinel API 101. Abgerufen unter: https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-api-101/ba-p/1438928
[LIBSWT]	Microsoft Docs: Extend Azure Sentinel across workspaces and tenants. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants
[LIBMSSP]	Microsoft Docs: Manage multiple tenants in Azure Sentinel as an MSSP. Abgerufen unter: https://docs.microsoft.com/en-us/azure/sentinel/multiple-tenants-service-providers
[LIBAZL]	Microsoft Docs: What is Azure Lighthouse? Abgerufen unter: https://docs.microsoft.com/en-us/azure/lighthouse/overview
[LSAF]	Azure. Reducing Security Alert Fatigue using machine learning in Azure Sentinel. Abgerufen unter: https://azure.microsoft.com/de-de/blog/reducing-security-alert-fatigue-using-machine-learning-in-azure-sentinel/

Über Avanade

Avanade ist ein weltweit führendes Unternehmen im Bereich digitale Services. Auf Basis des Microsoft-Ökosystems entwickeln wir innovative Business- und Cloud-Lösungen sowie designorientierte Anwendungen. Dazu verbinden wir technologische Expertise, profunde Branchenkenntnis sowie wirtschaftliches Denken mit dem Mut zu Neuem und Ungewohntem. Als treibende Kraft hinter der Accenture Microsoft Business Group helfen wir Unternehmen, Arbeitsabläufe zu verbessern, Mitarbeiter_innen neue Möglichkeiten zu eröffnen, Produkte und Services weiterzuentwickeln und mithilfe der Microsoft-Plattform Erlebnisse zu schaffen, die begeistern. Weltweit arbeiten rund 38.000 Menschen in 25 Ländern für Avanade: in einer Kultur der globalen Zusammenarbeit und menschlichen Diversität, von der unsere Kunden_innen profitieren. Avanade wurde im Jahr 2000 von Accenture LLP und der Microsoft Corporation gegründet. Heute gehört das Unternehmen mehrheitlich Accenture. Erfahren Sie mehr unter www.avanade.com

Erfahren Sie mehr auf www.avanade.com

avanade