Grundlagen der Untersuchung von Cloud-Bedrohungen: Bedrohungssuche mit MITRE ATT&CK

Sicherheitsteams in Unternehmen verfügen über umfangreiche Erfahrung bei der Untersuchung von Bedrohungen für ihre Endgeräte und Netzwerke. Cloud-native Bedrohungen sind jedoch ein ganz neues Kapitel.

In vielen Fällen wird die Cloud-Umgebung extern von einem Cloud-Dienstanbieter verwaltet, so wie dies bei Microsoft 365 der Fall ist. Es gibt keine Agenten, keine Netzwerk-sicherheitsinfrastruktur oder andere Mittel zur Erkennung von Ereignissen, für die das Sicherheitsteam zuständig ist. Zudem kommt bei Cloud-nativen Angriffen meist nicht einmal Malware zum Einsatz. Stattdessen setzen sie auf kompromittierte Konten und Funktionen des Cloud-Dienstes selbst, um einen Angriff zu starten und auszuweiten.

Die Gefahren von Cloud-Angriffen sind nicht aus der Luft gegriffen, sondern sehr real, da das primäre Ziel in der Exfiltration von Daten besteht. Wie gehen Sicherheitsteams derzeit dagegen vor?

Viele setzen darauf, alle Vorfälle manuell durchzusehen, die von ihrem CASB (Cloud Access Security Broker) gemeldet werden. Die meisten speisen diese Ereignisse zur weiteren Analyse in ein SIEM-System (Sicherheitsinformations- und Ereignis-Management) ein. Da die Anzahl der Ereignisse aber in die Millionen gehen kann, wird die Untersuchung von Cloud-Bedrohungen schnell zu einem arbeitsintensiven Alptraum.

Ein effizienter Weg, sich Einblick in Cloud-Angriffe zu verschaffen und einen nachhaltigen Prozess zur Minimierung von Risiken zu etablieren, existierte bisher noch nicht.

Die Suche im Heuhaufen

Ein korrekt implementierter CASB stellt eine Multimode-Verbindung zu Cloud-Diensten bereit, die sämtliche Ein- und Austrittspunkte für Cloud-native Bedrohungen abdeckt.

- **Anwendungsprogrammierschnittstelle (Application Program Interface, API):** Eine API-Verbindung zu Diensten wie Amazon Web Services (AWS) oder Microsoft 365 ermöglicht einen kompletten Einblick in Daten, Aktivität und Konfiguration der Cloud-Umgebung.
- **Forward Proxy:** Eine Verbindung über einen Forward Proxy (z. B. ein sicheres Web-Gateway der nächsten Generation) gewährleistet Transparenz und Kontrolle über Dienste, die keine öffentliche API für eingehendere Untersuchungen anbieten. Stattdessen wird die Untersuchung inline vom Proxy vorgenommen.
- **Reverse Proxy:** Eine Verbindung über einen Reverse Proxy gibt detaillierte Kontextinformationen über den Benutzer zurück, der auf den Cloud-Dienst zugreift, und kann in Kombination mit IAM-Tools (Identity and Access Management, Identitäts- und Zugriffsverwaltung) verwendet werden, um nicht verwaltete Geräte und ungewöhnliche Zugriffsereignisse zu erkennen.

Zusammen speist dieser Multimode-Ansatz Millionen von Ereignissen in eine Machine Learning-Analysefunktion ein, die daraus dann Tausende von Anomalien und oft nur Dutzende tatsächlicher Bedrohungen herausfiltert. Diese als UEBA (User and Entity Behavior Analytics, Verhaltensanalyse von Benutzern und Entitäten) bezeichnete Funktion nimmt Sicherheitsanalysten die gewaltige Arbeit ab, all die unzähligen Ereignisse zuzuordnen. Dadurch können sie sich auf das konzentrieren, was wirklich wichtig ist: ungewöhnliche Ereignisse und tatsächliche Angriffsmuster.

Übersetzung in eine gemeinsame Sprache mit MITRE ATT&CK

Das ist nur ein Teil des Prozesses. Jedes SOC (Security Operations Center, Sicherheitskontrollzentrum) untersucht Bedrohungen, die aus vielen Umgebungen stammen. Um den vollen Umfang eines Angriffs zu verstehen, ist es unerlässlich, über sämtliche Umgebungen hinweg die gleiche Sprache zu sprechen: MITRE ATT&CK®.

McAfee® MVISION Cloud: CASB ermöglicht das Zuordnen von Cloud-Anomalien und -Bedrohungen in der MITRE ATT&CK Matrix for Cloud. Dadurch kann das SOC Cloud-Bedrohungen mit einer beispiellosen Effizienz untersuchen, was einen Paradigmenwechsel bei der Abwehr von Bedrohungen bedeutet – auf Endgeräten, in Netzwerken und nun auch in der Cloud.

Cloud-Untersuchungen als Teil des Workflows

Um das Risiko in Cloud-Umgebungen wirksam zu senken, müssen Sicherheitsteams über eine Auswahl an Tools verfügen, die nicht nur die MITRE-Sprache sprechen, sondern auch nahtlos in den Workflow vieler Teams passen.

Für SOC-Teams wird nun eine neue, umfangreiche Zusammenstellung von Cloud-Anomalie- und Bedrohungsereignissen – zusammen mit Vorfällen aus DLP, der Konfigurationsprüfung sowie Schwachstellen-Scans – den vertrauten MITRE ATT&CK-Taktiken und -Techniken zugeordnet und gekennzeichnet, die sie derzeit in ihrem Untersuchungsprozess verwenden. Diese Informationen können sie auf verschiedenen Wegen (einschließlich APIs) direkt in ihre SIEM- oder SOAR-Plattform einspeisen, sodass sie einen konstanten Strom vorgefilterter Ereignisse erhalten.

SOC-Analysten können das MITRE ATT&CK-Framework auch direkt in MVISION Cloud einsehen, um Bedrohungen und deren Auswirkungen auf bestimmte Benutzer, Daten und Cloud-Dienste schnell zu analysieren. In MVISION Cloud stehen Analysten mehrere Ansichten zur Verfügung.

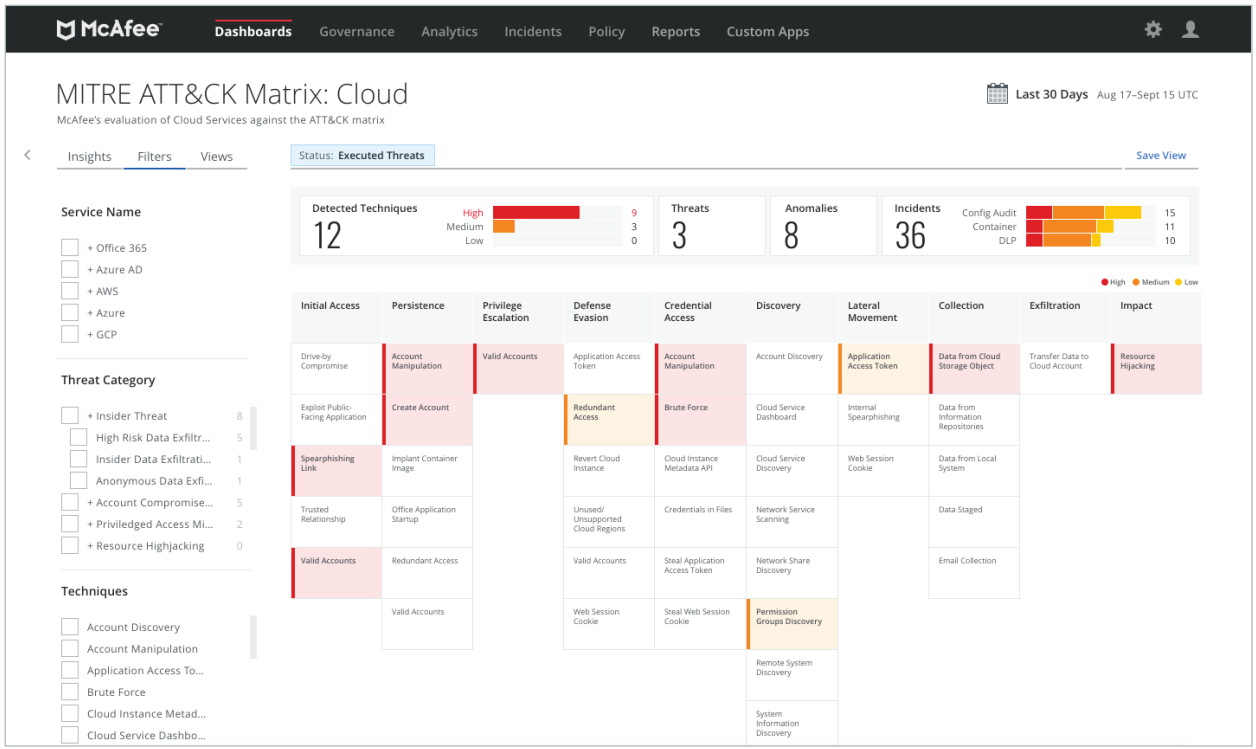

Abbildung 1. Zeigen Sie in MVISION Cloud Bedrohungen an, die in Ihrer Multi-Cloud-Umgebung bereits ausgeführt wurden.

- Eine **rückblickende** Ansicht sämtlicher Cloud-Angriffe, die in der Umgebung vollständig ausgeführt wurden
- Eine **proaktive** Ansicht gerade laufender Angriffe, damit Sie diese stoppen können
- Eine Ansicht der **kompletten „Kill-Chain“** eines Angriffs, die Vorfälle, Anomalien, Bedrohungen und Schwachstellen zu einer ganzheitlichen Folge von Verstößen zusammenfasst

Sicherheitsteams, die für den Schutz wichtiger Ressourcen in Cloud-Umgebungen (z. B. Microsoft 365, Microsoft Teams, AWS oder Azure) verantwortlich sind, können direkt in der MITRE ATT&CK-Ansicht einer laufenden Bedrohung Lücken in ihren Schutzmaßnahmen aufspüren und Änderungen an Richtlinien und Konfigurationen vornehmen.

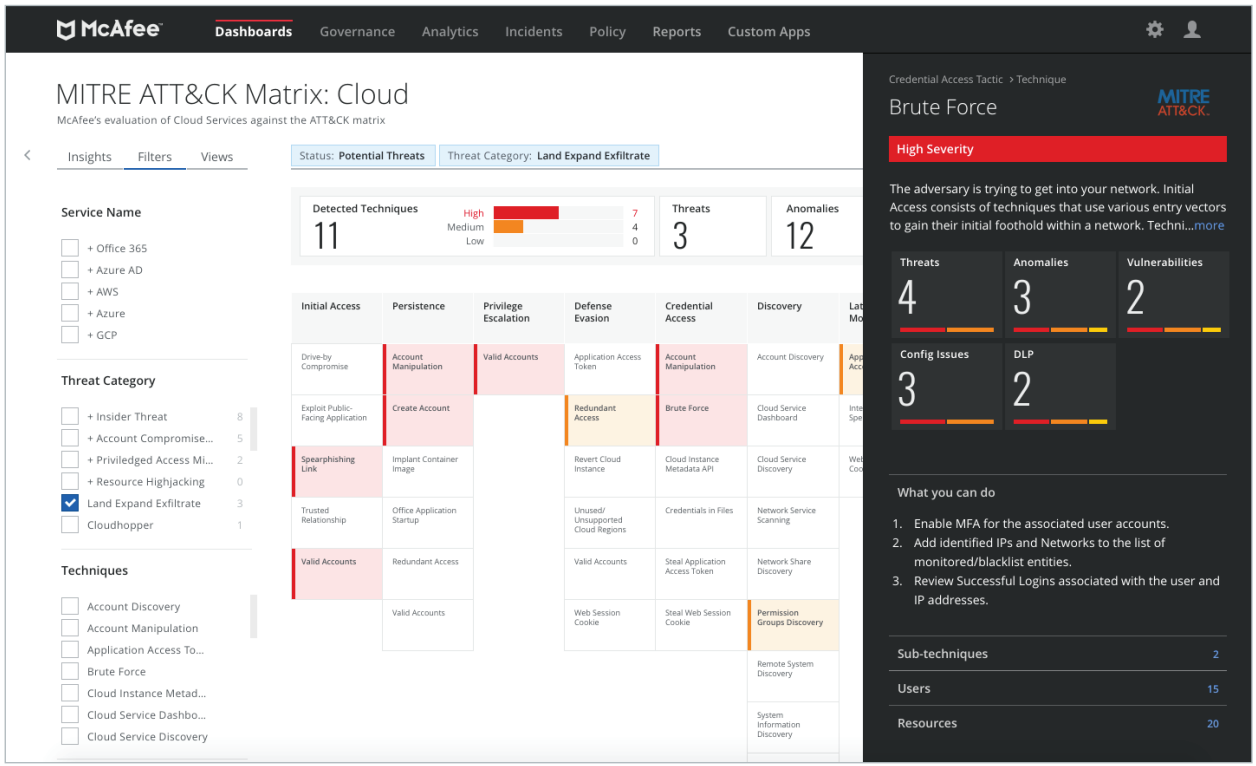

Abbildung 2. Zeigen Sie Angriffe an, die gerade durchgeführt werden. Rechts hervorgehoben sehen Sie einen Brute-Force-Angriff, der genauer aufgeschlüsselt wird.

Dank der Visualisierung von Angriffen in der ATT&CK-Matrix können an geeigneter Stelle effektive Richtlinienentscheidungen getroffen werden, um Angreifer aufzuhalten, bevor sie erfolgreich sind.

MVISION Cloud: Eine zentrale Plattform für Multi-Cloud-Sicherheit

Die weltweit führenden Sicherheitsteams verwenden MITRE ATT&CK. Mit MVISION Cloud bringt McAfee die Cloud-Sicherheitsvorfälle in das Mainstream-SOC. Dies ist ein wichtiger Paradigmenwechsel bei der Untersuchung von Bedrohungen. Nun können sich Unternehmen nicht nur vor Malware-basierten Kompromittierungsversuchen schützen, sondern auch Datenkompromittierungen durch Cloud-Angriffe verhindern.

MVISION Cloud bietet Sicherheitsteams folgende Möglichkeiten:

- Einspeisen vorgefilterter Sicherheitsvorfälle in ihr SOC, einschließlich Zuordnung im MITRE ATT&CK-Framework
- Visualisierung sowohl bereits ausgeführter als auch potentieller Angriffe auf ihre Cloud-Umgebungen über mehrere SaaS-, PaaS- und IaaS-Dienste hinweg
- Unterbindung laufender und zukünftiger Angriffe, indem sie empfohlene Änderungen, die mit MITRE ATT&CK-Techniken direkt verknüpft sind, in Richtlinien- und Cloud-Dienstkonfigurationen implementieren

Mit McAfee beschränken Sie die Bedrohungssuche auf Ihren Analyseplattformen nicht mehr nur auf eine einzige Plattform, sondern weiten sie auf alle Ihre Umgebungen aus – von der Cloud bis zum Endgerät. Mit McAfee MVISION Cloud, MVISION EDR und MVISION Insights erhält Ihr Unternehmen eine XDR-Plattform (Extended Detection and Response) für heterogene Angriffe, die heute Realität sind.

Legen Sie los!

Wenn Sie daran interessiert sind, Ihre Clouds mithilfe von MITRE ATT&CK auf Bedrohungen zu untersuchen, kontaktieren Sie uns. Klicken Sie hier, um eine Demo anzufordern.

McAfee

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de