VECTRA
SECURITY THAT THINKS®

SPOTLIGHT REPORT 2. Quartal 2021

Vision und Transparenz: Die 10 häufigsten Bedrohungserkennungen bei Microsoft Azure AD und Office 365

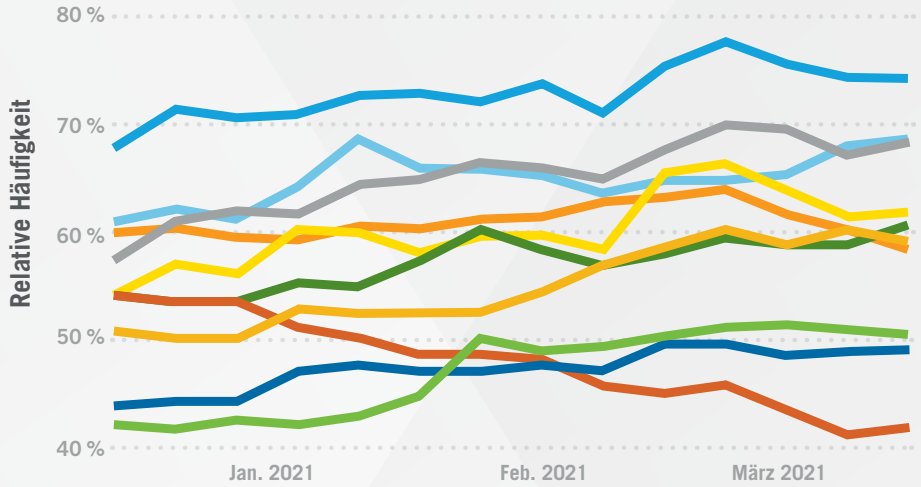
Kurzfassung

Die Cloud ändert nach wie vor alles, was wir über Sicherheit wissen, und selbst Unternehmen, die früher gegen die Cloud-Nutzung waren, suchen nun nach neuen Möglichkeiten, ihre Assets und Mitarbeiter zu schützen. Dies kann wie eine gewaltige Aufgabe scheinen, doch durch die Erfassung der richtigen Daten und den sinnvollen Einsatz von künstlicher Intelligenz (KI) können Security-Teams die erforderliche Vision und Transparenz erzielen, um potenziell gefährliche Aktivitäten bei Cloud-Anwendungen zu erkennen.

In diesem Spotlight Report werden wir uns mit den 10 häufigsten Bedrohungserkennungen befassen, die Kunden von Vectra erleben und dabei helfen, Angriffe in Microsoft Azure AD und Microsoft Office 365 zu bestätigen. Anhand dieser Bedrohungserkennungen können unsere Kunden unterscheiden, ob es sich bei einer Cloud-Aktivität um einen Angreifer oder um einen privilegierten Nutzer handelt. Alle angegebenen Daten stellen echte Beispiele von Bedrohungserkennungen dar, über die Sicherheitsunternehmen durch Vectra informiert werden, wenn etwas Ungewöhnliches passiert. Die Ergebnisse umfassen Folgendes:

- **Die 10 häufigsten Bedrohungserkennungen**: Erkennung von seltenem Verhalten, das ungewöhnlich ist oder die Sicherheit bei Microsoft Azure AD und Office 365 beeinträchtigt. Finden Sie heraus, was diese Bedrohungserkennungen in Ihrer Umgebung bedeuten können.
- **Bedrohungserkennungen basierend auf der Unternehmensgröße**: Erfahren Sie, wie häufig die Top 10 der Bedrohungserkennungen bei Unternehmen verschiedener Größe ausgelöst werden und warum die Erkennung riskanter Exchange-Vorgänge in Office 365 ganz oben auf der Liste steht, was bedeuten könnte, dass ein Angreifer versucht, sich Zugang zu verschaffen.
- **Kompromittierungen erkennen**: Finden Sie heraus, wie die Risiken in Verbindung mit diesen Bedrohungserkennungen dabei helfen können, einen kostspieligen Supply-Chain-Angriff zu verhindern.

Relative Häufigkeit der 10 häufigsten Bedrohungserkennungen



Lesen Sie den Spotlight Report: Die 10 häufigsten Bedrohungserkennungen bei Microsoft Azure AD und Office 365, um zu erfahren, welche Aktivitäten Bedrohungserkennungen bei diesen beliebten Cloud-Anwendungen auslösen.

Holen Sie sich den vollständigen Bericht

Cognito® Detect for Office 365 von Vectra® erkennt automatisch die Verhaltensweisen von Cyber-Angreifern und reagiert entsprechend, beschleunigt die Untersuchung von Vorfällen und ermöglicht proaktives Threat Hunting.

E-Mail: info_dach@vectra.ai vectra.ai/de

© 2021 Vectra AI, Inc. Alle Rechte vorbehalten. Vectra, das Vectra AI Logo, Cognito und Security that thinks sind eingetragene Marken und Cognito Detect, Cognito Recall, Cognito Stream, Vectra Threat Labs und der Threat Certainty Index sind Marken von Vectra AI. Alle weiteren in diesem Dokument verwendeten oder aufgeführten Marken, Produkte und Services sind Marken oder registrierte Marken oder Servicemarken der jeweiligen Eigentümer. Version: **060921**