VECTRA

Cognito Detect für Office 365

Erkennung und Schließung des größten Angriffsvektors in Office 365

30 % aller Unternehmen verzeichnen jeden Monat Kontoübernahmen. Vectra versteht das Verhalten der Angreifer und kennt sich mit Kontenberechtigungen in SaaS-Anwendungen aus, sodass Sie Kompromittierungen ein Ende setzen können.

Bereitstellung innerhalb von Minuten

Die Bereitstellung in Office 365 erfolgt nativ ohne Agenten. Verlinken Sie einfach Ihre Instanz, anschließend kann Vectra sofort Verhaltensweisen von Angreifern entdecken.

Verständnis von Sicherheitstelemetrie

Kämpfen Sie mit riesigen Sicherheitsprotokollen? Automatisieren Sie Triage und Anreicherung in großem Maßstab.

Datenkompromittierungen in Office 365 nehmen rasant zu. Trotz der zunehmenden Implementierung inkrementeller Sicherheitsansätze wie Mehrfaktor-Authentifizierung werden Zugriffskontrollen weiterhin umgangen. Tatsächlich verzeichnen 30 % aller Unternehmen Office 365-Kontoübernahmen – Monat für Monat.

Als Anbieter der branchenweit ersten Lösung für Netzwerk-Erkennung und Response für die Cloud dehnen wir die Vectra Cognito®-Plattform auf Microsoft® Office 365® aus.

Durch die automatische Erkennung und Priorisierung von Bedrohungen in der Cloud verhindert die Vectra-Plattform Datenkompromittierungen und ermöglicht proaktives Threat Hunting. Dadurch haben die Angreifer keine Chance, sich zu verbergen.

Vectra nutzt eine bewährte Methode, die derzeit Public Clouds, private Rechenzentren und Unternehmensumgebungen mit SaaS-Anwendungen schützt. Vectra Cognito verbindet Sicherheitsforschung und künstliche Intelligenz, um Angriffe schnell aufzudecken und entsprechende Details zu liefern, damit Sie sofort Gegenmaßnahmen ergreifen oder die Response automatisieren können.

Die native Bereitstellung in Office 365 ist unkompliziert und erfolgt innerhalb von Minuten. Cognito Detect für Office 365 kann nahtlos in Ihre vorhandene Installation integriert werden, ohne dass Sie dazu Agenten installieren und pflegen müssen. Verlinken Sie einfach Ihre Instanz, anschließend kann Vectra Verhaltensweisen von Angreifern entdecken.

Die Vectra Cognito-Plattform liefert Einblicke in Ihre gesamte Infrastruktur – von der Cloud bis zur lokalen Umgebung. Security-Operations-Teams kämpfen heute mit Fachkräftemangel und einer Flut an Meldungen. Durch die Aufdeckung raffinierter Cyber-Angriffe in Office 365 mithilfe von Aktivitätsprotokollen bleiben die Teams auch solchen Angriffen einen Schritt voraus und können schneller auf verborgene Bedrohungen reagieren.

Sie können Vectra Cognito in Ihr bestehendes Sicherheitsökosystem für den Data Lake integrieren oder als SIEM in Form von Zeek-formatierten Netzwerk-Metadaten mit angereicherten Sicherheitsinformationen einbinden. Überwachen und integrieren Sie die Plattform in Ihre vorhandenen Cloud-Sicherheitstools wie EDR- oder SOAR-Lösungen.

VORTEILE VON COGNITO DETECT FÜR OFFICE 365

Erkennung von böswilligem Verhalten in allen Angriffsstadien in Ihrem gesamten Netzwerk – einschließlich LAN, IaaS und SaaS

Überprüfung und Analyse Ihrer Erkenntnisse mit priorisierten und umsetzbaren Warnungen

Zusammenarbeit mit dem Vectra-Team und unser Engagement bei der Verbesserung unserer Produkte, um Ihre wachsenden Anforderungen zu erfüllen

Cognito für Office 365 verarbeitet Ereignisprotokolle aus Azure Active Directory, SharePoint und OneDrive (z. B. Anmeldeereignisse, Änderungen an der Mailbox-Routing-Konfiguration, Erstellung und Veränderung von Dateien sowie DLP-Konfigurationsänderungen), um Attacken in allen Phasen der Handlungskette (Kill Chain) zu erkennen.

SaaS KILL CHAIN

Infiltration und Eskalation	Angreifer erlangen unberechtigten Zugriff auf Office 365 und manipulieren die Umgebung, um an vertrauliche Ressourcen zu gelangen. Folgende Angriffsmethoden werden in diesen Phasen erkannt: Anmeldung per Brute-Force-Angriff, Hinzufügen von Anwendern zu Gruppen, Erweitern der Berechtigungen von Gruppen, Erstellung neuer Rollen
Reconnaissance	Angreifer orientieren sich in unbekannten Office 365-Umgebungen. Folgende Angriffsmethoden werden in dieser Phase erkannt: Auflisten aller Freigaben, Auflisten aller Anwender, Auflisten aller Rollen, ungewöhnliche Aktivitäten, ungewöhnliche Prozesse, höhere Anzahl von Suchvorgängen, Zugriff auf selten genutzte Dateien, Zugriff auf ungewöhnlich viele vertrauliche Dateien
Persistenz und Umgehung	Angreifer etablieren ihren Zugriff und vermeiden ihre Aufdeckung. Folgende Angriffsmethoden werden in diesen Phasen erkannt: App-Installationen, Veränderungen der Authentifizierungen, ungewöhnliche Uploads, Veränderungen der DLP-Einstellungen, Sammelpostfächer, Veränderungen der Audit-Log-Einstellungen, Richtlinienänderungen
Exfiltration und Zerstörung	Das Endziel: Exfiltration oder Zerstörung kritischer Informationen. Folgende Angriffsmethoden werden in diesen Phasen erkannt: Höhere Anzahl von Downloads aus neuen IP-Adressen und Regionen, Veränderungen der E-Mail-Übertragung, höhere Anzahl von Löschvorgängen, höhere Anzahl von Dateifreigabe-Zugriffen

Datenverarbeitung in Office 365

Cognito nutzt die Office 365-Management-API zum Abrufen von Ereignisprotokollen in Azure Active Directory, SharePoint und OneDrive. Dazu fordert die Lösung die Berechtigungen ActivityFeed.Read und ActivityFeed.ReadDLP an.

RBAC (Role-Based Access Control) und Objektanonymisierung verbessern den Datenschutz. Kunden können aus mehreren Datensouveränitätsregionen wählen, um Compliance-Vorgaben einzuhalten. Hinzu kommt, dass die Erkennungsumgebung auf einen serverlosen Ansatz setzt, um auch bei den neuesten verfügbaren Patches auf dem aktuellen Stand zu bleiben.

Informationen zur Microsoft-Management-API sind hier abrufbar:
https://docs.microsoft.com/de-de/office/office-365-management-api/office-365-management-apis-overview

VECTRA
Security that thinks®

E-Mail: info_dach@vectra.ai **Telefon:** +1 408 326 2020
vectra.ai

DS_CognitoDetectOffice365_020420

© 2019 Vectra AI, Inc. Alle Rechte vorbehalten. Vectra, das Vectra AI Logo, Security that thinks und Cognito sind eingetragene Marken und Cognito Detect, Cognito Recall, 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.