Cognito Detect pour Office 365

Détection et neutralisation du principal vecteur d'attaque dans Office 365

Chaque mois, 30 % des entreprises sont victimes d'une prise de contrôle de leurs comptes d'utilisateur. Parfaitement au fait des comportements d'attaque et des privilèges associés aux comptes dans les applications SaaS, Vectra vous permet de mettre un terme aux compromissions.

Déploiement en quelques minutes

Déploiement en mode natif et sans agent dans Office 365. Il vous suffit de lier votre instance et Vectra détecte immédiatement les comportements d'attaque.

Interprétation de la télémétrie de sécurité

Vous êtes dépassé par le volume des journaux de sécurité ? Automatisez le tri et l'enrichissement à grande échelle.

Les violations de données Office 365 sont au centre de toutes les préoccupations. En dépit de l'adoption croissante d'approches de sécurité renforcées telles que l'authentification multifacteur, les cyberpirates continuent de contourner les contrôles d'accès mis en place. En fait, chaque mois, 30 % des entreprises sont victimes d'une prise de contrôle de leurs comptes Office 365.

Non seulement Vectra a lancé la première solution de détection réseau et d'aide à la résolution des incidents pour le cloud du secteur, mais elle est fière d'annoncer l'extension de la plate-forme Vectra Cognito® à Microsoft® Office 365®.

La plate-forme Vectra prévient les violations de données en détectant automatiquement les menaces et en leur attribuant un niveau de risque. Résultat : des investigations plus rapides et une traque proactive des menaces — les cyberpirates n'ont nulle part où se cacher.

Vectra Cognito applique aux applications SaaS la méthodologie éprouvée qui protège actuellement les clouds publics, les centres de données privés et les environnements d'entreprise. La plate-forme allie les recherches en sécurité à l'intelligence artificielle pour vous offrir une visibilité en temps réel sur les attaques et vous permet d'en consulter aisément le détail pour prendre instantanément les mesures requises ou automatiser la résolution des problèmes.

Quelques minutes suffisent pour déployer la solution dans Office 365 en mode natif. Cognito Detect pour Office 365 peut être intégré en toute transparence avec votre installation existante, sans nécessiter la gestion ni l'installation d'agents. Liez simplement votre instance et Vectra détectera immédiatement les comportements d'attaque.

Grâce à Vectra Cognito, vous retrouvez une parfaite visibilité sur l'ensemble de votre infrastructure, du cloud à l'environnement sur site. En mettant au jour les cyberattaques avancées subies par Office 365 grâce à l'analyse des journaux d'activité, la plate-forme permet aux équipes responsables des opérations de sécurité, même en sous-effectif, de garder une longueur d'avance sur les cyberpirates et de contrer rapidement les menaces dissimulées.

Intégrez la solution avec votre écosystème de sécurité existant. Envoyez les données d'activité AWS à votre lac de données ou produit SIEM sous la forme de métadonnées réseau au format Zeek, enrichies par des informations de sécurité. La plate-forme Cognito s'intègre avec vos outils de sécurité cloud existants, comme les solutions EDR ou SOAR, et surveille votre environnement.

PRINCIPAUX AVANTAGES DE COGNITO DETECT POUR OFFICE 365

Détection des comportements malveillants à toutes les phases d'une attaque dans l'ensemble de l'environnement réseau : du LAN aux solutions IaaS et SaaS

Examen et analyse des résultats, avec génération d'alertes priorisées et exploitables

Partenariat avec l'équipe Vectra et engagement de notre part de poursuivre le développement de nos produits afin de satisfaire les besoins croissants de nos clients

Cognito pour Office 365 utilise les journaux d'événements Azure Active Directory, SharePoint et OneDrive pour signaler les détections à chaque phase de la chaîne d'attaque. Parmi les éléments utilisés, citons les événements de connexion, les modifications de la configuration du routage des boîtes aux lettres, la création et la manipulation de fichiers, ainsi que les modifications de configuration de solution DLP.

CHAÎNE D'ATTAQUE SaaS

Infiltration et élévation des privilèges	Les auteurs d'attaque obtiennent un accès illicite à Office 365 et manipulent l'environnement pour mettre la main sur des ressources inappropriées. Lors de ces phases, la solution détecte les activités suivantes : connexions par attaque en force, ajout d'utilisateurs à des groupes, octroi de nouveaux privilèges à des groupes, création de nouveaux rôles.
Reconnaissance	Les auteurs d'attaque cherchent à trouver leurs marques dans des environnements Office 365 qui leur sont peu familiers. Lors de cette phase, la solution détecte les activités suivantes : extraction des listes de tous les partages, de tous les utilisateurs, de tous les rôles et de tous les fichiers, activités inhabituelles, traitement inhabituel, recherches nombreuses, accès à des fichiers rares, accès à un volume anormal de fichiers sensibles.
Persistance et contournement	Les auteurs d'attaque consolident leur présence et évitent la détection. Lors de ces phases, la solution détecte les activités suivantes : installation d'applications, modifications liées à l'authentification, téléchargements inhabituels, modifications de solution DLP, utilisation de récepteurs des e-mails entrants et sortants (*sinks*), modification de paramètres de journal d'audit, modifications de stratégies.
Exfiltration et destruction	Les auteurs d'attaque atteignent leur objectif final : l'extraction ou la destruction d'informations critiques. Lors de ces phases, la solution détecte les activités suivantes : volume important de téléchargements à partir de nouveaux emplacements géographiques et de nouvelles adresses IP, modification du routage des messages, nombre élevé de suppressions, nombre élevé d'accès aux partages.

Traitement des données Office 365

Cognito utilise l'API de gestion Office 365 pour extraire les journaux d'événements Azure Active Directory, SharePoint et OneDrive en demandant les privilèges ActivityFeed.Read et ActivityFeed.ReadDLP.

Le contrôle d'accès basé sur les rôles et l'anonymisation d'objets contribuent à la protection de la confidentialité, et les clients peuvent choisir la législation à laquelle seront soumises leurs données (souveraineté sur les données) aux fins de conformité. De plus, l'environnement de détection met en œuvre une approche sans serveur pour toujours disposer des derniers correctifs publiés.

Pour en savoir plus sur l'API de gestion de Microsoft, consultez la page suivante : https://docs.microsoft.com/fr-fr/office/office-365-management-api/office-365-management-apis-overview

VECTRA
Security that thinks®

E-mail : info_france@vectra.ai / info_dach@vectra.ai **Téléphone :** +33 62 912 4119 / +41 44 551 0143
vectra.ai

DS_CognitoDetectOffice365_020420