Intégrer Reveal (x) 360 à Microsoft 365

Publié: 2024-02-16

En configurant l'intégration de Reveal (x) 360 avec Microsoft 365, les utilisateurs peuvent consulter les événements Microsoft 365 susceptibles d'indiquer des comptes ou des identités compromis.

Exigences du système

ExtraHop Reveal (x)

- Votre système Reveal (x) 360 doit être connecté à un ExtraHop sonde avec la version 8.6 ou ultérieure du firmware.
- La sonde ExtraHop doit être sous licence et configurée pour recevoir des paquets.

Microsoft

- Vous devez disposer de Microsoft 365 et de l'API Microsoft Graph. Seul le Microsoft Graph Global Service disponible à l'adresse https://graph.microsoft.com/ est pris en charge pour l'intégration.

  Note: Pour appeler Microsoft Graph, votre application doit acquérir un jeton d'accès auprès de la plateforme d'identité Microsoft. Le jeton d'accès contient des informations sur votre application et les autorisations dont elle dispose pour les ressources et les API disponibles via Microsoft Graph. Pour créer un jeton d'accès, votre application doit être enregistrée auprès de la plateforme d'identité Microsoft et être autorisée par un utilisateur ou un administrateur à accéder aux ressources Microsoft Graph.
- Vous devez disposer d'une application enregistrée dans Azure avec les autorisations suivantes :

API/Nom des autorisations	Type
AuditLog.Tout lire	Demande
AuditLog.Tout lire	Délégué
Répertoriaire.Tout lire	Demande
Répertoriaire.Tout lire	Délégué
IdentityRiskEvent.Tout lire	Demande
IdentityRiskEvent.Tout lire	Délégué
IdentityRiskyUser.Read.All	Demande
IdentityRiskyUser.Read.All	Délégué
Utilisateur.Read	Délégué

- Votre abonnement Azure doit disposer des fonctionnalités Azure AD standard suivantes :
  - Audit d'annuaire pour Azure AD
  - Points de terminaison de licence Azure AD P1 ou P2

    P1 vous fournit la liste des connexions aux comptes de service à partir du journal dlicensaudit. P2 inclut le P1 et vous fournit en outre des détections de risques et des utilisateurs à risque.

Configuration de l'intégration

Avant de commencer

Vous devez disposer de votre identifiant de locataire Microsoft Azure AD, de votre identifiant d'application (client) et de la valeur de la clé secrète de l'application.

1. Connectez-vous au système Reveal (x) 360 avec un compte doté de privilèges d' administration du système et des accès.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Toute l'administration**.
3. Cliquez **Intégrations**.
4. Cliquez sur **Microsoft 365** tuile.
5. Ajoutez vos informations d'identification Microsoft 365.

   • **ID du locataire:** Entrez votre identifiant de locataire. Votre identifiant de client Microsoft 365 se trouve dans le centre d'administration Azure AD.

   • **Clé d'accès:** Entrez votre ID d'application Microsoft (client). Vous pouvez consulter et copier les clés d'accès à votre compte via le portail Azure, PowerShell ou Azure CLI.

   • **Clé secrète:** Entrez la valeur secrète du client pour l'application. Vous pouvez consulter et copier la valeur secrète du client sur la page Certificats et secrets du portail Azure.

   • **Capteur ExtraHop:** Dans la liste déroulante, sélectionnez la sonde vers laquelle vous souhaitez transférer les données.
6. Cliquez **Tester la connexion** pour garantir que le système ExtraHop peut communiquer avec Microsoft 365.
7. Cliquez **Connectez**.

Prochaines étapes

- Vous pouvez désormais consulter les événements Microsoft 365 sur le système intégré tableaux de bord, dans disques, et dans détections.

Fonctionnalités d'intégration

Une fois la procédure d'intégration de Microsoft 365 terminée, plusieurs fonctionnalités d'ExtraHop Reveal (x) incluent les événements Microsoft 365 et Azure Active Directory afin que vous puissiez consulter les métriques, les enregistrements et les détections relatifs à ces événements.

Tableaux de bord

Consultez les statistiques des événements Microsoft 365 sur les fonctionnalités intégrées suivantes tableaux de bord:

- Azure Active Directory, qui affiche des indicateurs d'événements tels que les tentatives de transaction, la gestion des identités et des mots de passe, ainsi que l'activité des utilisateurs.
- Microsoft 365, qui affiche des indicateurs d'événements tels que les activités risquées des utilisateurs, les tentatives de connexion et la détection des risques.

Types d'enregistrements

Afficher les événements Microsoft 365 dans disques en recherchant les types d'enregistrement suivants :

- Journal d'activité Azure
- Audit de l'annuaire Microsoft 365
- Événement risqué lié à Microsoft 365
- Utilisateur risqué de Microsoft 365
- Inscriptions à Microsoft 365

Détections

Afficher les événements liés aux risques liés à Microsoft 365 qui sont récupérés via l'API Microsoft Graph et affichés dans le Reveal (x) suivant détections :

- Activités risquées des utilisateurs
- Connexions suspectes

Les exemples suivants décrivent certains des événements utilisateur risqués et des actions suspectes détectés par le biais du service d'intégration.

Voyage impossible

Un utilisateur se connecte à partir de deux emplacements géographiques différents. Les deux événements de connexion se sont produits dans un délai plus court que celui qu'il aurait fallu à l'utilisateur pour se déplacer d'un site à l'autre. Cette activité peut indiquer qu'un attaquant s'est connecté avec les informations dac.identification de lac.user.

Spray pour les mots

Une attaque par pulvérisation de mots de passe est un type d'attaque par force brute, dans le cadre de laquelle de nombreuses tentatives de connexion avec plusieurs noms d'utilisateur et mots de passe courants sont tentées pour obtenir un accès non autorisé à un compte.

Transfert de boîte de réception suspect

Le service Microsoft Cloud App Security (MCAS) identifie les règles de transfert d'e-mails suspectes, telles qu'une règle de boîte de réception créée par l'utilisateur qui transmet une copie de tous les e-mails à une adresse externe.

Utilisateur confirmé par l'administrateur compromis

Un administrateur sélectionné **Confirmez que l'utilisateur est compromis** dans l'interface utilisateur Risky Users ou dans l'API RiskyUsers du service Identity Protection .

Consultez la liste complète des actions suspectes et des événements risqués liés à l'activité des utilisateurs fournie par le Service de protection de l'identité Microsoft Azure AD.