Intégrer Reveal(x) 360 à Microsoft 365

Publié: 2023-09-19

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

Configuration requise

ExtraHop Reveal(x)

- Votre système Reveal(x) 360 doit être connecté à un capteur ExtraHop doté de la version 8.6 du firmware ou d'une version ultérieure.

Microsoft

- Vous devez disposer de Microsoft 365 et de Microsoft Graph API. Seul le service Microsoft Graph Global Service 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 avoir une application enregistrée dans Azure avec les permissions suivantes :

API / Permissions Nom	Type d'autorisation
AuditLog.Read.All	Application
AuditLog.Read.All	Délégué
Directory.Read.All	Application
Directory.Read.All	Délégué
IdentityRiskEvent.Lire.tout	Application
IdentityRiskEvent.Lire.tout	Délégué
IdentityRiskyUser.Lire.tout	Application
IdentityRiskyUser.Lire.tout	Délégué
User.Read	Délégué

- Votre abonnement Azure doit disposer des fonctionnalités Azure AD standard suivantes :
  - Audit d'annuaire pour Azure AD
  - Azure AD P1 ou P2 License EndpointsP1

    vous fournit la liste des ouvertures de session des comptes de service à partir du journal d'audit. P2 inclut P1 et fournit en plus des détections de risques et des utilisateurs à risque

    .

Configurer l'intégration

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

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

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

   • **Clé d'accès:** Saisissez votre ID d'application Microsoft (client). Vous pouvez afficher et copier les clés d'accès de votre compte à l'aide du portail Azure, de PowerShell ou d'Azure CLI.

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

   • **Capteur ExtraHop:** Dans la liste déroulante, sélectionnez le capteur vers lequel vous souhaitez transférer les données.
6. Cliquez sur **Tester la connexion** pour vous assurer que le système ExtraHop peut communiquer avec Microsoft 365.
7. Cliquez sur **Connecter**.

Prochaines étapes

- Vous pouvez désormais afficher les événements Microsoft 365 sur les tableaux de bord intégrés, dans les enregistrements et dans les détections.

Fonctionnalités d'intégration

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

Tableaux de bord

Les tableaux de bord intégrés suivants permettent d'afficher les mesures des événements Microsoft 365 :

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

Types d'enregistrements

Affichez les événements Microsoft 365 dans les enregistrements en recherchant les types d'enregistrements suivants :

- Journal d'activité Azure
- Audit de l'annuaire Microsoft 365
- Microsoft 365 Risky Event (Événement à risque)
- Utilisateur à risque Microsoft 365

- Connexions Microsoft 365

Détections

Affichez les événements à risque de Microsoft 365 qui sont récupérés via l'API Microsoft Graph et affichés dans les détections Reveal(x) suivantes :

- Activités d'utilisateurs à risque
- Inscriptions suspectes

Les exemples suivants décrivent quelques-uns des événements d'utilisateur à risque et des actions suspectes détectés par le service d'intégration.

Voyage impossible

Un utilisateur se connecte à partir de deux endroits géographiquement différents. Les deux événements de connexion se sont produits dans un laps de temps plus court que celui nécessaire à l'utilisateur pour se rendre d'un endroit à l'autre. Cette activité peut indiquer qu'un pirate s'est connecté avec les informations d'identification de l'utilisateur.

Pulvérisation de mot de passe

Une attaque par pulvérisation de mot de passe est un type d'attaque par force brute, où de nombreuses connexions pour plusieurs noms d'utilisateur et mots de passe communs sont tentées pour obtenir un accès non autorisé à un compte.

Transfert de boîte de réception suspecte

Le service Microsoft Cloud App Security (MCAS) identifie les règles de transfert de courrier électronique suspectes, telles qu'une règle de boîte de réception créée par l'utilisateur qui transfère une copie de tous les courriels vers une adresse externe.

L'administrateur a confirmé la compromission d'un utilisateur

Un administrateur a sélectionné **Confirmer l'utilisateur compromis** dans l'interface utilisateur Risky Users UI ou riskyUsers API du service Identity Protection.

Voir la liste complète des actions suspectes et des événements d'activité d'utilisateur à risque fournis par le service intégré de protection de l'identité Microsoft Azure AD.