

Intégrez RevealX 360 à Microsoft 365

Publié: 2024-07-03

En configurant l'intégration de RevealX 360 à Microsoft 365, les utilisateurs peuvent consulter les événements Microsoft 365 susceptibles d'indiquer des comptes ou des identités compromis.

Exigences du système

Hop Reveal X supplémentaire

- Votre système RevealX 360 doit être connecté à un ExtraHop sonde avec la version 8.6 ou ultérieure du firmware.
- La sonde ExtraHop doit disposer d'une licence et être 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 :

| Nom de l'API/des autorisations | Tapez |
|--------------------------------|---------|
| AuditLog.Read.All | Demande |
| AuditLog.Read.All | Délégué |
| Répertoire.Tout lire | Demande |
| Répertoire.Tout lire | Délégué |
| IdentityRiskEvent.read.all | Demande |
| IdentityRiskEvent.read.all | Délégué |
| IdentityRiskyUser.read.all | Demande |
| IdentityRiskyUser.read.all | Délégué |
| Utilisateur.Read | Délégué |


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

P1 vous fournit la liste des connexions aux comptes de service à partir du journal d'audit d'audit. P2 inclut P1 et vous fournit également des détections de risques et des utilisateurs à risque.

Configuration de l'intégration

Avant de commencer

Vous devez disposer de l'ID de locataire Microsoft Entra ID, de l'ID de l'application (client) et de la valeur de la clé secrète de l'application.

1. Connectez-vous au système RevealX 360 à l'aide d'un compte doté de privilèges d'administration du système et des accès.
2. Cliquez sur l'icône 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.
 - **Identifiant du locataire:** Entrez votre identifiant de locataire. Votre identifiant de locataire Microsoft 365 se trouve dans le centre d'administration Microsoft Entra ID.
 - **Clé d'accès:** Entrez l'ID de votre application Microsoft (client). Vous pouvez consulter et copier les clés d'accès de votre compte à l'aide du portail Azure, de PowerShell ou de l'interface de ligne de commande Azure.
 - **Clé secrète:** Entrez la valeur secrète du client pour l'application. Vous pouvez consulter et copier la valeur du secret client sur la page Certificats et secrets du portail Azure.
 - **Capteur ExtraHop:** Dans la liste déroulante, sélectionnez la sonde à laquelle vous souhaitez transférer les données.
6. Cliquez **Connexion de test** pour s'assurer que le système ExtraHop peut communiquer avec Microsoft 365.
7. Cliquez **Connecter**.

Prochaines étapes

- Vous pouvez désormais consulter les événements Microsoft 365 sur la version intégrée [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 RevealX incluent les événements Microsoft 365 et Microsoft Entra ID afin que vous puissiez consulter les mesures, les enregistrements et les détections de ces événements.

Tableaux de bord

Afficher les statistiques relatives aux événements Microsoft 365 sur les fonctionnalités intégrées suivantes [tableaux de bord](#) :

- Microsoft Entra ID, qui affiche des indicateurs d'événements tels que les tentatives de transaction, la gestion des identités et des mots de passe et l'activité des utilisateurs.
- Microsoft 365, qui affiche des indicateurs d'événements tels que l'activité risquée 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

- Connexions à Microsoft 365

Détections

Afficher les événements de risque liés à Microsoft 365 qui sont récupérés via l'API Microsoft Graph et affichés dans le RevealX suivant [détections](#) :

- Activités risquées des utilisateurs
- Connexions suspectes

Les exemples suivants décrivent certains des événements utilisateur à risque et des actions suspectes détectés via le service d'intégration.

Un voyage impossible

Un utilisateur se connecte depuis deux emplacements géographiques différents. Les deux événements de connexion se sont produits dans un délai plus court que ce qu'il aurait fallu à l'utilisateur pour se déplacer d'un lieu à l'autre. Cette activité peut indiquer qu'un attaquant s'est connecté à l'aide d'informations de localisation de l'utilisateur.

Spray pour mots de

Une attaque par pulvérisation de mots de passe est un type d'attaque par force brute, au cours de laquelle de nombreuses tentatives de connexion utilisant 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 transfère une copie de tous les e-mails vers une adresse externe.

L'administrateur a confirmé que l'utilisateur était compromis

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

Consultez la liste complète des actions suspectes et des activités risquées des utilisateurs fournies par l'interface intégrée [Service de protection d'identité Microsoft Entra ID](#) .