Integrate Reveal(x) 360 with Microsoft 365

Published: 2023-07-10

By configuring the Reveal(x) 360 integration with Microsoft 365, users can review Microsoft 365 events that might indicate compromised accounts or identities.

System requirements

ExtraHop Reveal(x)

- You must have your Reveal(x) 360 system connected to an ExtraHop sensor with firmware version 8.6 or later.
- The ExtraHop sensor must be licensed and configured to receive packets.

Microsoft

- You must have Microsoft 365 and Microsoft Graph API. Only the Microsoft Graph Global Service at https://graph.microsoft.com/ is supported for the integration.

  Note: To call Microsoft Graph, your app must acquire an access token from the Microsoft identity platform. The access token contains information about your app and the permissions it has for the resources and APIs available through Microsoft Graph. To create an access token, your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator to access the Microsoft Graph resources.
- You must have a registered application in Azure with the following permissions:

API / Permissions Name	Type
AuditLog.Read.All	Application
AuditLog.Read.All	Delegated
Directory.Read.All	Application
Directory.Read.All	Delegated
IdentityRiskEvent.Read.All	Application
IdentityRiskEvent.Read.All	Delegated
IdentityRiskyUser.Read.All	Application
IdentityRiskyUser.Read.All	Delegated
User.Read	Delegated

- Your Azure subscription must have following Standard Azure AD features:
  - Directory Audit for Azure AD
  - Azure AD P1 or P2 License Endpoints

    P1 provides you with the list of service account sign-ins from the audit log. P2 includes P1 and additionally provides you with risk detections and risky users.

Configure the integration

Before you begin

You must have your Microsoft Azure AD tenant ID, application (client) ID, and application secret key value.

1. Log in to the Reveal(x) 360 system with an account that has System and Access Administration privileges.
2. Click the System Settings icon and then click **All Administration**.
3. Click **Integrations**.
4. Click the **Microsoft 365** tile.
5. Add your Microsoft 365 credentials.

   • **Tenant ID:** Enter your tenant ID. Your Microsoft 365 tenant ID can be found in the Azure AD admin center.

   • **Access Key:** Enter your Microsoft Application (client) ID. You can view and copy your account access keys with the Azure portal, PowerShell, or Azure CLI.

   • **Secret Key:** Enter the client secret value for the application. You can view and copy the client secret value on the Certificates & secrets page in the Azure portal.

   • **ExtraHop Sensor:** From the drop-down list, select the sensor that you want to forward data to.
6. Click **Test Connection** to ensure that the ExtraHop system can communicate with Microsoft 365.
7. Click **Connect**.

Next steps

- You can now view Microsoft 365 events on built-in dashboards, in records, and in detections.

Integration features

After completing the Microsoft 365 integration procedure, several ExtraHop Reveal(x) features include Microsoft 365 and Azure Active Directory events so that you can view metrics, records, and detections for those events.

Dashboards

View metrics for Microsoft 365 events on the following built-in dashboards:

- Azure Active Directory, which displays event metrics such as transaction attempts, identity and password management, and user activity.
- Microsoft 365, which displays event metrics such as risky user activity, sign-in attempts, and risk detection.

Record types

View Microsoft 365 events in records by searching for the following record types:

- Azure Activity Log
- Microsoft 365 Directory Audit
- Microsoft 365 Risky Event
- Microsoft 365 Risky User
- Microsoft 365 Sign-ins

Detections

View Microsoft 365 risk events that are retrieved through the Microsoft Graph API and displayed in the following Reveal(x) detections:

- Risky User Activities
- Suspicious Sign-ins

The following examples describe some of the risky user events and suspicious actions that are detected through the integration service.

Impossible Travel

A user signs in from two geographically different locations. The two sign-in events occurred within a shorter time than it would take for the user to travel between locations. This activity might indicate that an attacker signed in with user credentials.

Password Spray

A password spray attack is a type of brute force attack, where numerous sign-ins for multiple usernames and common passwords are attempted to gain unauthorized access to an account.

Suspicious Inbox Forwarding

The Microsoft Cloud App Security (MCAS) service identifies suspicious email forwarding rules, such as a user-created inbox rule that forwards a copy of all emails to an external address.

Admin Confirmed User Compromised

An administrator selected **Confirm user compromised** in the Risky Users UI or riskyUsers API of the Identity Protection service.

View a complete list of suspicious actions and risky user activity events provided by the integrated Microsoft Azure AD Identity Protection service.