

Integrieren Sie Reveal (x) 360 mit Microsoft 365

Veröffentlicht: 2023-09-14

Durch die Konfiguration der Reveal (x) 360-Integration mit Microsoft 365 können Benutzer Microsoft 365-Ereignisse überprüfen, die auf kompromittierte Konten oder Identitäten hinweisen könnten.

Anforderungen an das System

ExtraHop Enthüllung (x)

- Sie müssen Ihr Reveal (x) 360-System mit einem ExtraHop verbunden haben Sensor mit Firmware-Version 8.6 oder höher.
- Der ExtraHop-Sensor muss für den Empfang von Paketen lizenziert und konfiguriert sein.

Microsoft

- Sie müssen über Microsoft 365 und Microsoft Graph API verfügen. Nur der Microsoft Graph Global Service unter <https://graph.microsoft.com/> wird für die Integration unterstützt.



Hinweis Um Microsoft Graph aufzurufen, muss Ihre App ein Zugriffstoken von der Microsoft-Identitätsplattform erwerben. Das Zugriffstoken enthält Informationen über Ihre App und die Berechtigungen, die sie für die über Microsoft Graph verfügbaren Ressourcen und APIs hat. Um ein Zugriffstoken zu erstellen, muss Ihre App bei der Microsoft Identity Platform registriert und entweder von einem Benutzer oder einem Administrator autorisiert sein, auf die Microsoft Graph-Ressourcen zuzugreifen.

- Sie müssen über eine registrierte Anwendung in Azure mit den folgenden Berechtigungen verfügen:

API//Name der Berechtigungen	Typ
AuditLog.Read.All	Bewerbung
AuditLog.Read.All	Delegiert
Verzeichnis.Lesen.Alles	Bewerbung
Verzeichnis.Lesen.Alles	Delegiert
IdentityRiskEvent.Read.All	Bewerbung
IdentityRiskEvent.Read.All	Delegiert
IdentityRiskyUser.Read.All	Bewerbung
IdentityRiskyUser.Read.All	Delegiert
Benutzer.Lesen	Delegiert

- Ihr Azure-Abonnement muss über die folgenden Azure AD-Standardfunktionen verfügen:


- Verzeichnisprüfung für Azure AD
- Azure AD P1- oder P2-Lizenzendpunkte

P1 stellt Ihnen die Liste der Dienstkonto-Anmeldungen aus dem Audit-Log zur Verfügung. P2 beinhaltet P1 und bietet Ihnen zusätzlich Risikoerkennungen und riskante Benutzer.

Konfiguration der Integration

Bevor Sie beginnen

Sie benötigen Ihre Microsoft Azure AD-Mandanten-ID, Anwendungs-ID (Client) und den Wert für den geheimen Anwendungsschlüssel.

1. Melden Sie sich beim Reveal (x) 360-System mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Die gesamte Verwaltung**.
3. klicken **Integrationen**.
4. Klicken Sie auf **Microsoft 365** Kachel.
5. Fügen Sie Ihre Microsoft 365-Anmeldeinformationen hinzu.
 - **Mieter-ID:** Geben Sie Ihre Mandanten-ID ein. Ihre Microsoft 365-Mandanten-ID finden Sie im Azure AD Admin Center.
 - **Zugangsschlüssel:** Geben Sie Ihre Microsoft-Anwendungs-ID (Client) ein. Sie können Ihre Kontozugriffsschlüssel mit dem Azure-Portal, PowerShell oder Azure CLI anzeigen und kopieren.
 - **Geheimer Schlüssel:** Geben Sie den geheimen Client-Wert für die Anwendung ein. Sie können den geheimen Wert des Client auf der Seite Certificates & Secrets im Azure-Portal anzeigen und kopieren.
 - **ExtraHop-Sensor:** Wählen Sie aus der Dropdownliste den Sensor aus, an den Sie Daten weiterleiten möchten.
6. klicken **Verbindung testen** um sicherzustellen, dass das ExtraHop-System mit Microsoft 365 kommunizieren kann.
7. klicken **Verbinde**.

Nächste Schritte

- Sie können jetzt Microsoft 365-Ereignisse auf der integrierten [Dashboards](#), in [Aufzeichnungen](#), und in [Erkennungen](#).

Funktionen für die Integration

Nach Abschluss des Microsoft 365-Integrationsvorgangs umfassen mehrere Funktionen von ExtraHop Reveal (x) Microsoft 365- und Azure Active Directory Directory-Ereignisse, sodass Sie Metriken, Aufzeichnungen und Erkennungen für diese Ereignisse anzeigen können.

Armaturenbretter

Zeigen Sie Metriken für Microsoft 365-Ereignisse auf den folgenden integrierten Geräten an [Dashboards](#) :

- Azure Active Directory, das Ereignismetriken wie Transaktionsversuche, Identitäts- und Passwortverwaltung und Benutzeraktivitäten anzeigt.
- Microsoft 365, das Ereigniskennzahlen wie riskante Benutzeraktivitäten, Anmeldeversuche und Risikoerkennung anzeigt.

Arten von Datensätzen

Microsoft 365-Ereignisse anzeigen in [Aufzeichnungen](#)  indem Sie nach den folgenden Datensatztypen suchen:

- Azure-Aktivitätsprotokoll
- Microsoft 365-Verzeichnisprüfung
- Microsoft 365-Risikoereignis
- Microsoft 365-Riskanter Benutzer

- Microsoft 365-Anmeldungen

Erkennungen

Microsoft 365-Risikoereignisse anzeigen, die über die Microsoft Graph-API abgerufen und in der folgenden Enthüllung angezeigt werden (x) [Erkennungen](#):

- Riskante Benutzeraktivitäten
- Verdächtige Anmeldungen

In den folgenden Beispielen werden einige der riskanten Benutzerereignisse und verdächtigen Aktionen beschrieben, die über den Integrationsdienst erkannt werden.

Unmögliches Reisen

Ein Benutzer meldet sich von zwei geografisch unterschiedlichen Standorten aus an. Die beiden Anmeldeereignisse erfolgten innerhalb einer kürzeren Zeit, als der Benutzer für die Reise zwischen den Standorten benötigen würde. Diese Aktivität könnte darauf hindeuten, dass sich ein Angreifer mit Benutzeranmeldedaten angemeldet hat.

Passwort-Spray

Ein Passwort-Spray-Angriff ist eine Art Brute-Force-Angriff, bei dem zahlreiche Anmeldungen mit mehreren Benutzernamen und gängigen Passwörtern versucht werden, unautorisierten Zugriff auf ein Konto zu erlangen.

Verdächtige Posteingangweiterleitung

Der Microsoft Cloud App Security (MCAS) -Dienst identifiziert verdächtige E-Mail-Weiterleitungsregeln, wie z. B. eine vom Benutzer erstellte Posteingangsregel, die eine Kopie aller E-Mails an eine externe Adresse weiterleitet.

Administrator hat bestätigt, dass Benutzer kompromittiert wurde

Ein Administrator wurde ausgewählt **Bestätigen Sie, dass der Benutzer gefährdet ist** in der Risky Users UI oder RiskyUsers API des Identity Protection-Dienstes.

Sehen Sie sich eine vollständige Liste verdächtiger Aktionen und riskanter Benutzeraktivitätsereignisse an, die von der integrierten [Microsoft Azure AD-Identitätsschutzdienst](#).