Integrieren Sie RevealX 360 mit Microsoft 365

Veröffentlicht: 2024-08-07

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

Anforderungen an das System

ExtraHop RevealX

- Sie müssen Ihr RevealX 360-System an einen ExtraHop angeschlossen 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 aufrufen zu können, muss Ihre App ein Zugriffstoken von der Microsoft Identity Platform 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 sein und entweder von einem Benutzer oder einem Administrator für den Zugriff auf die Microsoft Graph-Ressourcen autorisiert werden.
- Sie müssen eine registrierte Anwendung in Azure mit den folgenden Berechtigungen haben:

API//Name der Berechtigungen	Typ
AuditLog.Read.All	Bewerbung
AuditLog.Read.All	Delegiert
Verzeichnis.Alles lesen	Bewerbung
Verzeichnis.Alles lesen	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 Standardfunktionen von Microsoft Entra ID verfügen:
  - Verzeichnisaudit für Microsoft Entra ID
  - Microsoft Entra ID 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 Entra ID, Mandanten-ID, Anwendungs-ID (Client) und den Wert des geheimen Anwendungsschlüssels.

1. Melden Sie sich mit einem Konto, das über System- und Zugriffsadministrationsrechte verfügt, beim RevealX 360-System an.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Die gesamte Verwaltung**.
3. Klicken Sie **Integrationen**.
4. Klicken Sie auf **Microsoft 365** Fliese.
5. Fügen Sie Ihre Microsoft 365-Anmeldeinformationen hinzu.

   • **Mieter-ID:** Geben Sie Ihre Mieter-ID ein. Ihre Microsoft 365-Tenant-ID finden Sie im Microsoft Entra ID 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 Client-Wert auf der Seite Zertifikate und Geheimnisse im Azure-Portal anzeigen und kopieren.

   • **ExtraHop-Sensor:** Wählen Sie aus der Dropdownliste den Sensor aus, an den Sie Daten weiterleiten möchten.
6. Klicken Sie **Verbindung testen** um sicherzustellen, dass das ExtraHop-System mit Microsoft 365 kommunizieren kann.
7. Klicken Sie **Verbinden**.

Nächste Schritte

- Sie können jetzt Microsoft 365-Ereignisse auf der integrierten Dashboards, in Aufzeichnungen, und in Erkennungen.

Funktionen zur Integration

Nach Abschluss des Microsoft 365-Integrationsvorgangs umfassen mehrere ExtraHop RevealX-Funktionen Microsoft 365- und Microsoft Entra-ID-Ereignisse, sodass Sie Metriken, Datensätze und Erkennungen für diese Ereignisse anzeigen können.

Dashboards

Zeigen Sie Metriken für Microsoft 365-Ereignisse auf den folgenden integrierten Geräten an Dashboards:

- Microsoft Entra ID, die Ereignismetriken wie Transaktionsversuche, Identitäts- und Kennwortverwaltung sowie Benutzeraktivität anzeigt.
- Microsoft 365, das Ereignismetriken 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-Verzeichnisaudit
- Riskantes Microsoft 365-Ereignis
- Riskanter Microsoft 365-Benutzer

- Microsoft 365-Anmeldungen

Erkennungen

Sehen Sie sich Microsoft 365-Risikoereignisse an, die über die Microsoft Graph-API abgerufen und im Folgenden angezeigt werden: RevealX Erkennungen:

- Riskante Benutzeraktivitäten
- Verdächtige Anmeldungen

Die folgenden Beispiele beschreiben einige der riskanten Benutzerereignisse und verdächtigen Aktionen , die vom Integrationsdienst erkannt werden.

Unmögliches Reisen

Ein Benutzer meldet sich von zwei geografisch unterschiedlichen Orten aus an. Die beiden Anmeldeereignisse ereigneten sich innerhalb einer kürzeren Zeit, als der Benutzer benötigen würde, um zwischen Standorten zu reisen. 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, sich unbefugten Zugriff auf ein Konto zu verschaffen.

Weiterleitung verdächtiger Posteingänge

Der Microsoft Cloud App Security (MCAS) -Service identifiziert verdächtige E-Mail-Weiterleitungsregeln, 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 vom integrierten Microsoft Entra ID-Identitätsschutzdienst.