Data Connector built for Microsoft Defender XDR Alerts & Incidents

Last updated: Jun. 25, 2025

Overview

Ingest **Alerts Security data** , **Incidents Security data** from Microsoft Defender Graph API for analysis, threat detection, and investigation with the Data Connector built for Microsoft Defender XDR Alerts & Incidents.

> **Tip:** If you need to configure multiple Microsoft connectors, you can use the Microsoft connector reference table to help with set up and configuration. For more info, see Microsoft connectors [/documentation/page/a76b8289/data-connectors#g7ff80b6].

Requirements

Subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB

CrowdStrike clouds: Available in US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.

Additional requirements:

- Global Administrator access to the Microsoft 365 portal
- Your environment must include a functioning deployment of Microsoft Defender XDR
- Global Administrator or Security Administrator access to the Microsoft Azure and Defender portals
- Administrator access to the Falcon console for the respective CID
- Confirm the **Data Connector built for Microsoft Defender XDR Alerts & Incidents** plugin app is available in the Crowdstrike Store

  > **Note:** If the app is not available, contact your sales engineer to have it enabled or provisioned.

Setup

Set up data ingestion for Data Connector built for Microsoft Defender XDR Alerts & Incidents through Microsoft GRAPH API and the data connector in the Falcon console.

> **Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Step 1: Register Microsoft application and generate secret value

Register your Microsoft application in the administration interface of Azure portal and generate a client secret .These steps are performed in the administration interfaces of your Microsoft Azure and Microsoft Graph API instances.

1. Login as Global Administrator.
2. Go to **Microsoft Azure Active Directory > Application > App registrations**.
3. Click **New Registration**.
4. In **Register an application**, enter the following details:
   - **Name:** For example, `CrowdStrike`.
   - **Supported account types:** Select **Accounts in this organizational directory only ("Organization's Name" only - Single tenant)**.
   - Click **Register**.
5. In **Overview**, save the **Application (Client) ID** value and the **Directory (Tenant) ID** value for use in a later step.
6. In **Client credentials**, click **Add a certificate or secret**.
7. Click **Client secrets**.
8. Click **New client secret**.
9. Provide a description (name) and the expiration interval.

   > **Note:** The expiration interval is based on your environment and determines how often the client secret needs to be regenerated.

10. Click **Add**.

    > **Note:** Save the client secret, which appears in the **Value** field. This is the only opportunity to save it as it isn't displayed again. The client secret **Value** poses a security risk if compromised. We recommend deleting it after you enter it in a later step.

Step 2: Add permissions for Microsoft Defender XDR Alerts and Incidents

1. Under **Manage**, Click **API Permissions**.

2. Click **Add a Permission**.
3. Click **Microsoft Graph**.
4. Click **Application permissions**.
5. In the Select Permissions field:
    a. Enter **SecurityAlert**, and enable **SecurityAlert.Read.All** permission.
    b. Enter **SecurityIncident**, and enable **SecurityIncident.Read.All** permission.
6. Click **Add permissions**.
7. In the API permissions window, click **Grant admin consent**.
8. In the **Grant admin consent** confirmation window, click **Yes**.

Step 3: Configure and activate the Data Connector built for Microsoft Defender XDR Alerts & Incidents

Set up your data connector to ingest data from the Data Connector built for Microsoft Defender XDR Alerts & Incidents.

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. Click **+ Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.
4. In the **New connection** dialog, review connector metadata, version, and description. Click **Configure**.

> **Note:** For connectors that are in a **Pre-production** state, a warning dialog appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.
6. Enter the following values:
    - ○ **Client ID**: Enter the **Client ID** value that you saved earlier.
- **Client Secret**: Enter the client secret **Value** that you saved earlier.
- **Configuration name**: Enter a name for your configuration.
- **Base URL**: Enter **graph.microsoft.com**
- **Tenant ID**: Enter the **Tenant ID** value that you saved earlier.

7. Click **Save configuration**.
8. In the **Data connector configuration** field, select the configuration you just created.
9. Enter a name and an optional description to identify the connector.
10. Click the **Terms and Conditions** box, then click **Save**.

Step 4 : Verify successful data ingestion

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. In the **Status** column, verify data connection status is **Active**.
3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.
4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#repo = "3pi_msdefalertandincident"
```

Data reference

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Process:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#p5eme1kf]
- Authentication:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- Configuration:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Iam:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#e3wbhf1h]
- Email:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#f5yqjx4f]

- File:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#y4016g3a]
- Host:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Library:Start:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#s0dfb8yk]
- Network:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx]
- Registry:Creation:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#x6l9dpbt]
- Registry:Change:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#i91q6llu]
- Threat:Indicator:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#s455fd5m]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

Data Conne Data Connector built for Microsoft Defender XDR Events [/documentation/page/j06b4388/data-connector-built-for-microsoft-defender-xdr]