Data Connector built for Microsoft Sentinel

Last updated: Jun. 9, 2025

Overview

Microsoft Sentinel is a cloud-native, scalable Security Information and Event Management (SIEM) platform that incorporates intelligent Security Orchestration, Automation, and Response (SOAR) capabilities. This solution enables comprehensive cyberthreat detection, investigation, response, and hunting functionalities while maintaining enterprise-wide visibility.

Use this connector to ingest Alerts and Incidents logs from Microsoft Sentinel:

- **Alerts:** Security notifications generated by Microsoft Sentinel's detection rules.
- **Incidents:** Correlated collections of alerts representing potential security events requiring investigation.

Requirements

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

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

CrowdStrike access and permissions: Administrator or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements

- You must have an active subscription to Microsoft Event Hubs.
- Global Administrator or Security Administrator role to register an application and validate an event hub.
- Owner or User Access Administrator role to add a role assignment. For more info, see Create a Microsoft Entra app & service principal in the portal [https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal]
.

Setup

> **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.

Set up data ingestion for Microsoft Sentinel through Event Hubs and the data connector in the Falcon console. For more info, see the Microsoft Azure Event Hubs [https://learn.microsoft.com/en-us/azure/event-hubs/] documentation.

> **Important:** Read this information before setup.

- If you are configuring multiple Microsoft data connectors, each data connector should connect to its own dedicated Event Hub.
- You can use a single Event Hub Namespace to host multiple Event Hubs. The number of Event Hubs permitted per namespace depends on your subscription tier. To learn more about how many Event Hubs you can host per namespace, see Basic vs. standard vs. premium vs. dedicated tiers [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-quotas#basic-vs-standard-vs-premium-vs-dedicated-tiers]
.
- Microsoft Entra ID application credentials are required for data connector configuration in Step 8 of this guide. If you already have an Microsoft Entra ID application and Event Hub set up that you wish to configure with this data connector, you can begin at setup at Step 4.

Step 1: Register a Microsoft application and generate a client secret

1. In the Microsoft Azure portal, search and select **Microsoft Entra ID**.
2. In the Microsoft Entra ID **Overview** page, click **+ Add > App registration**.
   The **Register an application** page opens.
3. On the **Register an application** page, enter this info:
   a. **Name:** Enter an application name. Save this name to enter in a later step.
   b. **Supported account types:** Choose the account type based on your organization's requirements. We recommend choosing **Accounts in this organizational directory only** based on least privilege access. For more info, see Identity and account types for single- and multitenant apps [https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types]
   .
   c. Click **Register**. The **Application** page opens with a **Successfully created application** notification.
4. In the **Essentials** section on the **Application** page, copy and save the **Application (client) ID** and the **Directory (tenant) ID** values to use in a later step.
5. In the navigation menu, click **Manage > Certificates & secrets**.
   The **Certificates & secrets** page appears.
6. Click the **Client secrets** tab and click **+ New client secret**.
   The **Add a client secret** dialog opens.

7. Enter a description for the client secret and a client secret expiration time. The expiration interval is based on your environment and determines how often the client secret needs to be regenerated.

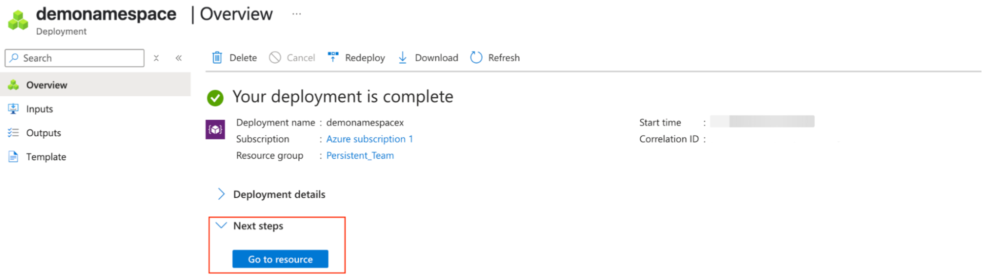
8. Click **Add**. Your new client is now listed in the **Client secrets** tab with a **Successfully updated application credentials** notification.

9. Copy the **Value** field and save it somewhere safe to enter in a later step.

> **Note:** This sensitive info is displayed only once and is required for data connector configuration in a later step.

Step 2: Create an Event Hub

1. In the **Next steps** section, click **Go to resource**.



demonamespace | Overview

Deployment

Your deployment is complete

Deployment name : demonamespacex
Subscription : Azure subscription 1
Resource group : Persistent_Team

Start time : [redacted]
Correlation ID :

The namespace **Overview** page opens.

2. Click **+ Event Hub**.
The **Create Event Hub** page opens.

3. In the **Basics** tab, enter **Event Hub Details** and set **Retention** settings:

- **Name:** Enter a name. Save this event hub name to enter in a later step.

  > **Note:** Avoid using the same name for both the Event Hub and Event Hub Namespace.

- **Partition count:** Select the number of partitions. For more info, see Partitions [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability#partitions].

  > **Note:** As a best practice for processing large volumes of data, we recommended using the highest number of partitions. For more info, see Advantages of using partitions [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability#advantages-of-using-partitions]
  > .

- **Cleanup policy:** Select **Delete** or **Compact** based on your requirements. If you choose **Compact**, complete these tasks.

  - Select **Infinite retention time.**

  - Set a **Tombstone retention time** in hours. For more info, see Configure cleanup policy [https://learn.microsoft.com/en-us/azure/event-hubs/configure-event-hub-properties#configure-cleanup-policy].

- **Retention time (hrs):** As events are sent to the connector for consumption when they are created, we recommend selecting the default 1 hour retention time. You can increase the number as needed. For more info, see Configure retention time [https://learn.microsoft.com/en-us/azure/event-hubs/configure-event-hub-properties#configure-cleanup-policy].

4. In the **Capture** tab, turn Capture **On** or **Off**. For more info, see Capture events through Azure Event Hubs in Azure Blob Storage or Azure Data Lake Storage [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-capture-overview]
.

5. In the **Review + Create** tab, complete these tasks:

   a. Review the instance details.

   b. Confirm the **Validation succeeded** message.

   c. Click **Create**.

   d. The Even Hubs Namespace **Overview** page opens. Confirm successful Event Hub creation with the **Successfully created Event Hub message** notification.

Step 3: Configure Microsoft Sentinel

1. Sign in to the Azure portal.

2. Search for **Microsoft Sentinel**.

3. Select **Create**.

4. Select the workspace you want to use or create a new one. You can run Microsoft Sentinel on more than one workspace, but the data is isolated to a single workspace.

> **Important:** Once deployed on a workspace, Microsoft Sentinel doesn't supportmoving that workspace to another resource group or subscription. The default workspaces created by Microsoft Defender for Cloud aren't shown in the list. You can't install Microsoft Sentinel on these workspaces.

5. Select **Add**.

Step 4: Forward logs from Log Analytics Workspace to Event Hub

Step 4: Forward logs from Log Analytics Workspace to Event Hub

1. In the Azure Portal, search for **Log Analytics Workspace**.
2. Select the workspace you created in step 3. In the **Settings** section, select **Data Export**. At the top of the pane, select **New export rule** and follow these steps:
   - Provide a **Rule Name** for the rule, then click **Next**.
   - Search for **Security**, select **securityalert** and **securityincident**, thenclick Next.
   - For **destination type**, select **Event Hub**. Select your **Subscription**, your **Event Hub Namespace**, and the **Event Hub Name** you created.
   - Click **Review and Create**.

Step 5: Verify successful Event Hubs configuration

Verify data is successfully streaming to your event hub:

1. In the Azure Portal, search for and select **Event Hub**.
2. Click the new Event Hub namespace that you created in Step 2.
3. In the **Overview** page, look at the **Messages** chart and verify incoming messages.

Step 6: Configure and activate the Data Connector built for Microsoft Sentinel

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 dialogue appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.
6. Enter the following information:
   - **Name:** Enter a name for your configuration.
   - **Event Hub Consumer Group:** Enter the name of the Event Hub Consumer Group you created in Step 5.
   - **EventHub Name:** Enter the name of your existing Event Hub or the name that you saved in Step 3.
   - **EventHub Namespace:** Enter the name of your existing Event Hubs Namespace or the Namespace name that you saved in Step 2.
   - **Client ID:** Enter the Application (Client) ID value that you saved in Step 1.
   - **Tenant ID:** Enter the Directory (Tenant) ID value that you saved in Step 1.
   - **Client Secret:** Enter the client secret value that you saved Step 1.
   - **Cloud:** Select **Public**, **Government**, or **China**.
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**.

    > **Note:** Configuring a data source with multiple products creates a new data connector for each product supported by the data source. A confirmation message displays the names of your new connectors.

Step 7: 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:

```
#Vendor = microsoft | #repo = "3pi_microsoft_sentinel" | #event.module = "sentinel"
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **microsoft-sentinel**.

Timestamp

Timestamp Format: `yyyy-MM-ddTHH:mm:ss.nZ`

Example: `2025-03-26T10:28:09.9043782Z`

Structure

Sample Security Alert logs after CrowdStrike parsing:

```
{
    "TimeGenerated": "2025-03-26T10:28:09.9043782Z",
    "DisplayName": "alertincidentrule1",
    "AlertName": "alertincidentrule1",
    "AlertSeverity": "High",
    "ProviderName": "ASI Scheduled Alerts",
    "VendorName": "Microsoft",
    "VendorOriginalId": "1165f40c-XXXX-4a8e-XXXX-d11d4ce7b9ef",
    "SystemAlertId": "dac35fed-XXXX-5956-XXXX-38f85963ce51",
    "AlertType": "d683ffe4-XXXX-4266-XXXX-ac6b47d52b17_b9996647-XXXX-4236-XXXX-17a0c3bef5f7",
    "IsIncident": false,
    "StartTime": "2025-03-26T05:21:27.3964726Z",
    "EndTime": "2025-03-26T10:15:52.8157993Z",
    "ProcessingEndTime": "2025-03-26T10:28:09.8724066Z",
    "ExtendedProperties": "{\"Query Period\":\"05:00:00\",\"Trigger Operator\":\"GreaterThan\",\"Trigger
Threshold\":\"0\",\"Correlation Id\":\"3c60b113-XXXX-XXXX-9d5a-c3d4340ec426\",\"Search Query Results
Overall Count\":\"139\",\"Data Sources\":\"[\\\"azuresentinelpslgrp\\\"]\",\"Query\":\"// The query_now
parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.\
\nset query_now = datetime(2025-03-26T10:17:46.7828250Z);\\nSecurityAlert\",\"Query Start Time UTC\":
\"2025-03-26 05:17:46Z\",\"Query End Time UTC\":\"2025-03-26 10:17:47Z\",\"Analytic Rule Ids\":\"[\\
\"b9996647-19b1-4236-8835-17a0c3bef5f7\\\"]\",\"Event Grouping\":\"SingleAlert\",\"Analytic Rule Name\":
\"alertincidentrule1\",\"ProcessedBySentinel\":\"True\",\"Alert generation status\":\"Full alert
created\"}",
    "SourceSystem": "Detection",
    "WorkspaceSubscriptionId": "d71b54fe-XXXX-4558-XXXX-b86bf500b858",
    "WorkspaceResourceGroup": "persistent_team",
    "ProductName": "Azure Sentinel",
    "ProductComponentName": "Scheduled Alerts",
    "Status": "New",
    "Tactics": "InitialAccess",
    "TenantId": "d683ffe4-8f55-4266-be1b-ac6b47d52b17",
    "_ItemId": "156dd505-0a2d-11f0-b012-000d3a99e479",
    "_Internal_WorkspaceResourceId": "/subscriptions/d71b54fe-XXXX-4558-XXXX-b86bf500b858/resourcegroups/
persistent_team/providers/microsoft.operationalinsights/workspaces/azuresentinelpslgrpXX",
    "Type": "SecurityAlert"
}
```

Sample Security Incident logs after CrowdStrike parsing:

```
{
    "AdditionalData": {
        "alertsCount": 1,
        "bookmarksCount": 0,
        "commentsCount": 0,
        "alertProductNames": [
            "Azure Sentinel"
        ],
        "tactics": [
            "InitialAccess"
        ],
        "techniques": []
    },
    "AlertIds": [
        "25f6edb2-XXXX-071d-XXXX-9331922ed468"
    ],
    "BookmarkIds": [],
    "Comments": [],
    "CreatedTime": "2025-03-26T10:32:32.1166564Z",
    "FirstActivityTime": "2025-03-26T05:26:09.2010487Z",
    "IncidentName": "912e8310-XXXX-41ff-XXXX-af4b6d370618",
    "IncidentNumber": 19898,
    "IncidentUrl": "https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/
subscriptions/d71b54fe-XXXX-4558-XXXX-b86bf500b858/resourceGroups/persistent_team/providers/
Microsoft.OperationalInsights/workspaces/azuresentinelpslgrp/providers/Microsoft.SecurityInsights/
Incidents/912e8310-XXXX-41ff-XXXX-af4b6d370618",
    "Labels": [],
    "LastActivityTime": "2025-03-26T10:20:08.1189853Z",
    "LastModifiedTime": "2025-03-26T10:32:32.1166564Z",
    "ModifiedBy": "Incident created from alert",
    "Owner": {
        "objectId": null,
        "email": null,
        "assignedTo": null,
        "userPrincipalName": null
    },
    "ProviderIncidentId": "19898",
    "ProviderName": "Azure Sentinel",
    "RelatedAnalyticRuleIds": [
        "b9996647-XXXX-4236-XXXX-17a0c3bef5f7"
    ],
    "Severity": "High",
    "SourceSystem": "Azure",
    "Status": "New",
    "Tasks": [],
    "TimeGenerated": "2025-03-26T10:32:32.1166564Z",
    "Title": "alertincidentrule1",
    "Type": "SecurityIncident",
    "_ItemId": "b18083c1-XXXX-11f0-XXXX-000d3a1d6e38",
    "TenantId": "d683ffe4-XXXX-4266-XXXX-ac6b47d52b17",
    "_Internal_WorkspaceResourceId": "/subscriptions/d71b54fe-XXXX-4558-XXXX-b86bf500b858/resourcegroups/
persistent_team/providers/microsoft.operationalinsights/workspaces/azuresentinelpslgrp"
}
```

Next-Gen SIEM events

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

- Web:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#b64y1zpv]
- 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 Connector built for Data Connector built for Microsoft SharePoint › [/documentation/page/sfc3203c/data-connector-built-for-microsoft-sharepoint]