NG SIEM - CrowdStrike Integration

CrowdStrike Integration

The CrowdStrike Falcon integration allows you to easily connect your CrowdStrike Falcon platform to Elastic for seamless onboarding of alerts and telemetry from CrowdStrike Falcon and Falcon Data Replicator. Elastic Security can leverage this data for security analytics including correlation, visualization and incident response

Requirements

API - Steps to Get Client ID and Client Secret in CrowdStrike Falcon (Recomended)

1. **Log in to the Falcon Console**
   - Go to: https://falcon.crowdstrike.com
   - Use your admin credentials to log in.
2. **Navigate to API Clients and Keys**
   - Click on the **"Support"** (question mark icon) or your **User avatar** on the top right.
   - Select **"API Clients and Keys"** from the dropdown.
     Alternatively, go to: `https://falcon.crowdstrike.com/support/api-clients-and-keys`
3. **Create a New API Client**
   - Click on **“Add new API client”**.
   - **Name** your client and optionally add a **description**.
   - Under **API Scopes**, select the required **permissions** based on what you need (e.g., read access to Hosts, Alerts, IOCs, etc.).
4. **Click Save**
5. **Copy the Client ID and Client Secret**
   - After saving, the **Client ID** and **Client Secret** will be displayed **once**.
   - Copy them immediately and store them securely (e.g., in a password manager or secrets vault).
6. **Token URL**

Collect CrowdStrike Falcon Data Data Replicator Logs (input: aws-s3)

1. Go to: https://falcon.crowdstrike.com
2. Log in with your CrowdStrike account
3. In the left menu, click **Support & Resources → Falcon Data Replicator** (or directly **FDR Access**)

4. You will immediately see a section called **AWS-S3 (Option 1)** with the three fields already filled in for your customer account:
   - **AWS: Access Key ID** → copy this
   - **AWS: Secret Access Key** → copy this (it's shown only here; you can't retrieve it again)
   - **AWS: Queue URL** → copy this exact SQS URL

> Please provide the following information to CyTech:

Collect CrowdStrike Falcon Data Replicator Logs (input: aws-s3)

- **AWS: Access Key ID**
- **AWS: Secret Access Key**
- **AWS: Queue URL**

API - Steps to Get Client ID and Client Secret in CrowdStrike Falcon

- **Client ID: Client ID for the CrowdStrike.**
- **Client Secret: Client Secret for the CrowdStrike.**
- **URL: Token URL of CrowdStrike.**

Revision #3
Created 23 September 2025 08:15:36 by Richmond Abella
Updated 17 November 2025 07:20:39