CrowdStrike Falcon
Event Streams Add-on

Transition Guide

Overview

This document outlines the transition process to continue data collection from the last event collected by “CrowdStrike Falcon Endpoint Add-on” (https://splunkbase.splunk.com/app/3944/#/overview) legacy technology add-on for CrowdStrike Falcon Event Streams.

The "CrowdStrike Event Stream" technical add-on for Splunk provides several new capabilities for supporting connections to CrowdStrike's Event Stream APIs. One of these is the ability to support multiple Data Feed URLs within an Event Stream API. In order to properly enable this the "start offset" field in the input configuration was removed. Each Data Feed URL has its own independent offset value which made providing fields and properly ensuring that the data was input and mapped correctly problematic. Instead this information was shifted to JSON files that are maintained in the TA folder and are dedicated to specific inputs.

Contents:

Getting Started

Prior to proceeding with this process the new Event Stream Technical Add-on(TA) should be properly deployed, as detailed in the CrowdStrike Falcon Event Stream Technical Add-on Installation and Configuration Guide, within the Splunk infrastructure without any enabled inputs.

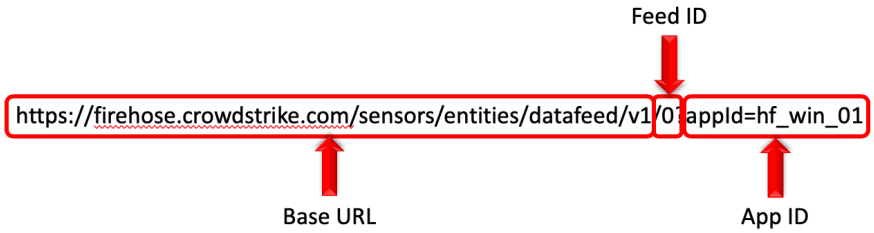
The transitioning and continuation of a connection/communication with the CrowdStrike Event Stream API is centered around two key pieces of information: the Data URL Feed and the Offset value.

The Data URL Feed: This is a URL that is presented by the Event Stream API after authentication and is the endpoint that will be connected to and provide data. It is possible to have multiple Data URL Feeds presented by a single Event Stream API and is essentially used for load balancing of the data. The ability to support multiple Data URL Feeds was a key limitation in the legacy CrowdStrike Endpoint TA.

The Offset Value: This is a numerical value that is present in all Streaming API and Event Stream API events. It is a unique value given to an event per Data URL Feed. This is important because failure to transition the correct Offset Value with the correct Data URL Feed can result in lost and/or duplicated data.

Understanding and Configuring the Data Feed URL

The Data Feed URLs are provided via the Streaming/Event Stream API endpoint and are not visible in the event or log data. The syntax for the URL depends on the cloud environment the Falcon instance is running in, the feed id and the App ID that was provided during the connection process.



- **Base URL** – The cloud environment's base URL for the CrowdStrike Event Stream API gateway
- **Feed ID** – The numerical count of the data feed (count starts a '0')
- **App ID** – The App ID assigned in the TA Input configuration

Customers leveraging the current Splunk Endpoint TA will only have connected to a single feed so the 'Feed ID' should always be '0'.

Collect the Offset Value

The Offset Value is part of every event in the Streaming API and can be located in the metadata section of an event that's been collected by the legacy Endpoint TA:

The legacy Endpoint TA was only designed to support a single Data URL Feed so transitioning from the legacy TA only requires one offset value to collected. This should be done by:

1. Disable the Input for the legacy Endpoint TA
2. Located the last event that was collected and record the offset field value
3. Leave input disabled to ensure that the offset value is the latest

Creating and Implementing the Offset File

Combining the Data Feed URL and the Offset Value

In order to 'pick up' where the legacy TA 'left off' the Data Feed URL and the Offset Value must be paired together correctly.

Step 1:

To construct the Data Feed URL you will need to identify:

1. The CrowdStrike cloud environment that will be contacted
2. The Data Feed URL feed number – which should be '0'
3. The AppID that is being used for the Event Stream TA input

This information will be combined together as shown in the syntax breakdown below to construct the proper Data Feed URL:

For example

1. CrowdStrike cloud environment: US Commercial cloud 1
2. Data Feed URL feed number: 0
3. AppID for the Event Stream TA: hf_win_01

The resulting Data Feed URL would be:
https://firehose.crowdstrike.com/sensors/entities/datafeed/v1/0?appId=hf_win_01

Step 2:

The Offset Value is taken from the last event that the legacy TA received:

Step 3:

The Data Feed URL and the Offset Value are properly combined in JSON format:
"https://firehose.crowdstrike.com/sensors/entities/datafeed/v1/0?appId=hf_win_01":17676670

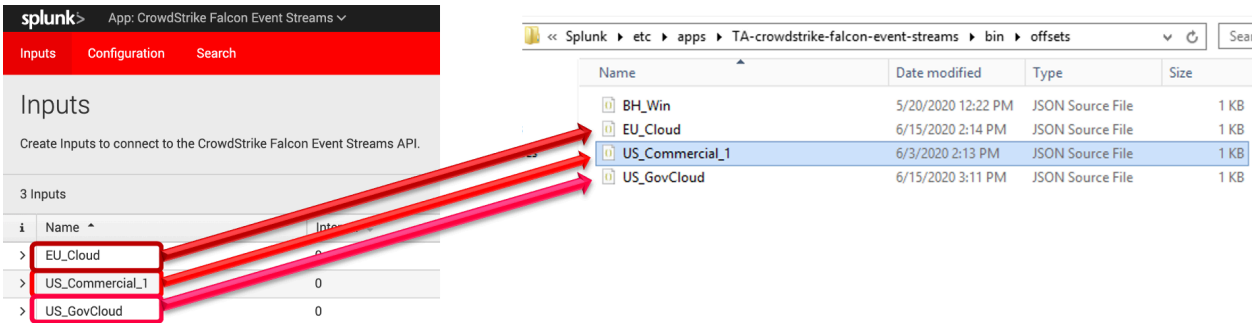
Creating and Populating the Offset JSON file

The Offset JSON files are stored in the $SPLUNK/etc/apps/TA-crowdstrike-falcon-event-streams/bin/offsets folder. The file names are the names of their corresponding inputs (**note that these files are not deleted when the input is removed**). Each JSON file will have the datafeed URLs and offset values that have been associated with that Input.

The Event Streams TA will look for offset values in a JSON file and in the KVStore whenever an input is enabled. If will then use the largest value between the two when calling the Event Stream API. The goal is to create the JSON file so that when the input is enabled the TA will use the value in that file and continue where the legacy TA left off.

Step 1:

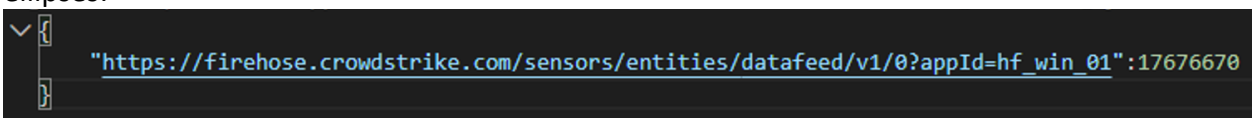
Create a file with a JSON file, named after the input in the Event Stream TA, within the $SPLUNK/etc/apps/TA-crowdstrike-falcon-event-streams/bin/offsets folder*:



***Note: Ensure that the file permissions for the JSON file(s) are correct for the Splunk deployment and that the account running Splunk can access and/or owns the file(s).**

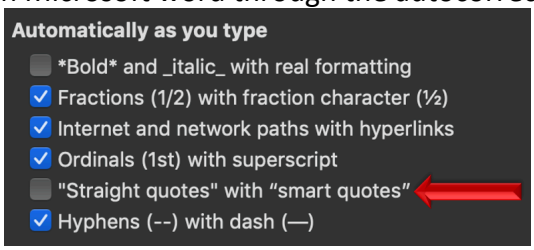
Step 2:

Edit the file to contain the proper Data Feed URL and Offset value combination enclosed in ellipses:



NOTE Ensure that the quotation marks are ‘straight quotes’ and not ‘smart quotes’ such as the ones typically used by default in programs like Microsoft Word.

This setting can be change in Microsoft word through the autocorrect options:



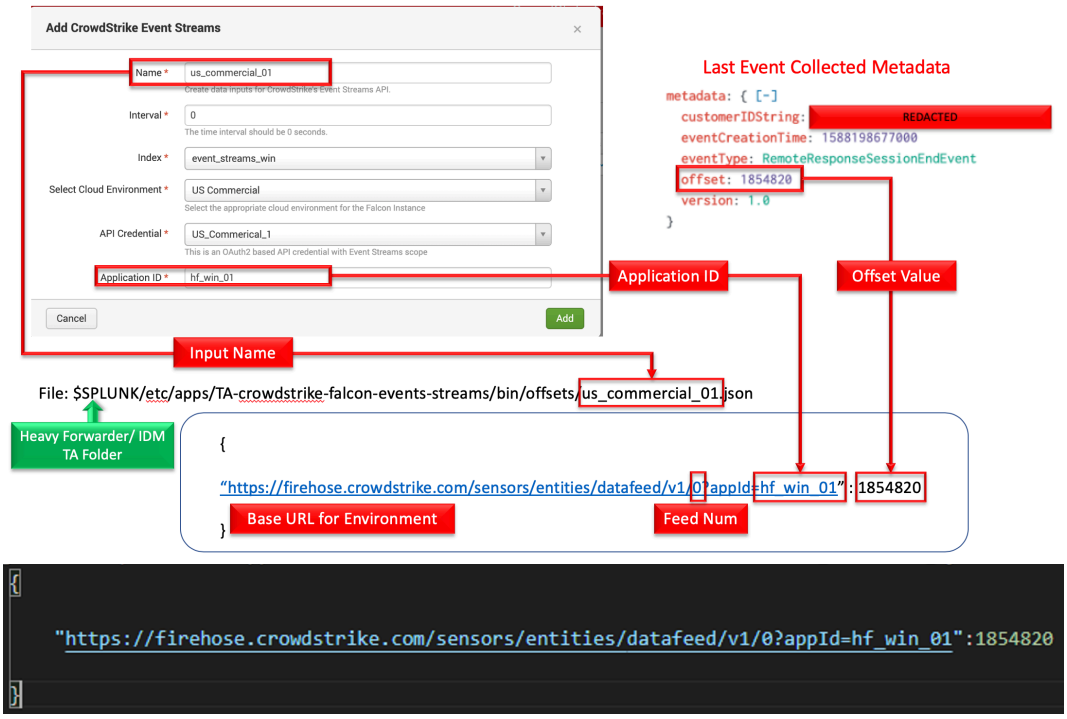
Step 3:

Save the file in the Offsets folder and ensure its recognized as a JSON file.

Recap

The Offset JSON files are stored in the $SPLUNK/etc/apps/TA-crowdstrike-falcon-event-streams/bin/offsets folder. The file names are the names of their corresponding inputs.

The entry in the file tells the TA what offset to use for the specific Data Feed URL for the specific Input:



Search Macro Configuration

The current Splunk Endpoint TA uses a Search Macro named `cs_get_index`. The new Event Stream TA uses a Search Macro named `cs-es-get-index` (which stands for 'CrowdStrike Event Stream Get Index'). The new Search Macro will need to be pointed to the specific index or indexes that contain the Falcon data. Refer to the installation and deployment guide for more details.

Troubleshooting and Support

CrowdStrike provides support for the TA's code, the functionality of that code and authentication to the API endpoint(s). The following topics fall outside of that scope:

1. Network connectivity issues unrelated to authentication response from the CrowdStrike API endpoint
2. Tagging and CIM mapping (these are considered feature requests and will be evaluated by the integrations team)

Checking Configuration

Unable to continue event collection from specific event:

1. Ensure that the JSON format of the file is correct
2. Ensure that the quotation marks in the JSON file are correct
3. Ensure that the Application ID in the input matches the one in the Data Feed URL
4. Ensure that the JSON file is in the correct folder location
5. Ensure that the JSON file has the correct permissions

Getting Support

Prior to contacting CrowdStrike support please review the following:

1. Ensure that the TA logging is set to 'Debug'
2. Toggle the input from disabled to enabled and back for 30-60 seconds to attempt a connection
3. Ensure that the JSON file is formatted correctly
4. Ensure that the JSON file is named after the associated input
5. Ensure that the Application ID in the input matches the one in the Data URL Feed
6. Ensure that the Splunk Event Stream TA has been correctly deployed and configured
7. Download the all log files containing 'ta_crowdstrike_falcon_event_streams' under the $Splunk/var/log/splunk/ directory
8. Record the following information about the Splunk system:
    - Splunk environment type
    - Splunk version
    - TA version
9. Identify the types of networks devices that the connection will traverse and ensure that they have been properly configured
10. Collect API audit logs from the Falcon instance for the time frame when the issue is occurring
11. Navigate to https://supportportal.crowdstrike.com/
12. Provide all information above – to include a copy of the JSON file