Event streams APIs

Last updated: Feb. 16, 2023

Contents:

- About CrowdStrike APIs
- Externalize data with event streams
  - Connect to event streams

About CrowdStrike APIs

This guide provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which includes:

- Details on getting started, such as authentication
- Links to our API specification (Swagger) by cloud
- Domains used in base URLs by cloud

Externalize data with event streams

Events are pieces of information gathered by the Falcon sensors on your hosts. Use our streaming APIs to establish a long-lived HTTP connection to the CrowdStrike cloud and observe a "stream" of events as they occur and are processed.

See the Streaming API Event Dictionary for information on the information included in event streams.

You can use the CrowdStrike API to perform these tasks related to streaming events:

- Find streams
- Connect to a stream
- Refresh an active stream

Note: If your CrowdStrike cloud is US-GOV-1 and your CID doesn't have event streams enabled, or if the status is unknown, contact Support for assistance.

Connect to event streams

You can use event streams for a variety of needs - usually correlating Falcon's event data with your own internal or third-party data. However you use the event data, the general workflow looks like this:

1. Discover all available streams for your environment. This returns a series of connection URLs.

   Note: This request requires that you specify an AppID, which is an alphanumeric string to identify an event stream. AppIDs can have a maximum of 32 characters. AppIDs must be unique to each active event stream. If you use the same AppID for two active streams, you'll receive a 401 error for the second stream.

2. Connect to all the URLs returned by your discover request.
3. Consume the event data returned by the connection requests.
4. Refresh your connection approximately every 29 minutes. The CrowdStrike cloud automatically terminates streaming sessions after 30 minutes, unless you send a keep-alive request.

Relevant API endpoints

- GET/sensors/entities/datafeed/v2
- POST/sensors/entities/datafeed-actions/v1/{partition}

Steps

1. Discover all event streams in your environment with `GET /sensors/entities/datafeed/v2?appId=<app_ID>`. This request returns two necessary URLs for each stream:
   - `dataFeedURL`
   - `refreshActiveSessionURL`
2. Connect to each stream using the `dataFeedURL` provided in the response of your discover request. Because the streaming API does not manage client offset, you must include the `&offset=<offset>` parameter in the query string of your requests to indicate the point where you want the stream to begin.

   > Unlike most other CrowdStrike APIs, the connection requests use a different base URL, and this endpoint is not shown in our CrowdStrike API Specification.

   Each stream connection is valid for 30 minutes. If the connection is not refreshed before that time, the stream will automatically terminate.
3. Refresh each stream regularly using the `refreshActiveSessionURL` value provided in the response of your discover request. We recommend refreshing every 29 minutes to ensure a consistent connection.

   > Remember that the OAuth2 token used to authenticate requests also expires after 30 minutes. Make sure you're using a valid auth token from `GET /oauth2/token`.

Example discover request

```
curl -X GET "https://api.crowdstrike.com:443/sensors/entities/datafeed/v2?appId=my_app_id" \
    -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
    -H 'Accept: application/json'
```

Example discover response

```
{
```

```
    "resources": [
        {
            "dataFeedURL": "http://firehose.crowdstrike.com/sensors/entities/datafeed/v1/0?appId=my_app_id",
            "sessionToken": {
                "token": "ui/Papb4QuiW99Er...6E2jB7OjJAZ9fcuWaimU=",
                "expiration": "2019-07-17T16:40:16.166805518Z"
            },
            "refreshActiveSessionURL": "https://api.crowdstrike.com/sensors/entities/datafeed-actions
/v1/0?appId=my_app_id&action_name=refresh_active_stream_session",
            "refreshActiveSessionInterval": 1800
        }
    ],
    "meta": {
        "query_time": 0.007506181,
        "powered_by": "FalconHose",
        "trace_id": "09d04710-e519-4201-8ac3-8341643437b7"
    }
}
```


Example connection request

```
curl -X GET "https://firehose.crowdstrike.com/sensors/entities/datafeed/v1/0?appId=my_app_id&offset=<offset>" \
  -H 'Accept: application/json' \
  -H 'Authorization: Token ui/Papb4QuiW99Er...6E2jB7OjJAZ9fcuWaimU='
```

Example refresh request

```
curl -X POST "https://api.crowdstrike.com:443/sensors/entities/datafeed-actions
/v1/0?action_name=refresh_active_stream_session&appId=my_app_id" \
    -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
    -H 'Accept: application/json'\
    -H 'Content-Type: application/json'
```