Mandiant

# VIEWING INDEX DATA FOR SPLUNK EVENTS

If you are tuning Splunk and want to verify events are going into the expected index, you can get this information from the Validation Platform using the Director or the API.

## Configure Splunk

To capture the index information for events coming from Splunk, you must add **index** to the list of fields in your Splunk queries. Otherwise it won't be present in the events the Validation Platform receives.

## Viewing the Index Information in the Director

***TO VIEW INDEX DATA FOR SPLUNK EVENTS***

1. Open the Job that has Splunk Events you want to review.
2. Click the Events cell to bring up the detected event for the Action.
3. Click **View Event Details**. This displays the a table listing all the Events.
4. Expand one or expand all Events by clicking **Show All**. The index will be listed in the untranslated field in the table.

## Viewing the Index Information using the API

To view the integration event data for one Action in a Job, use the following call:

```
GET /integration_events?filter[job_action_id]=1&filter[integration_id]=2
```

To view the integration event data for multiple Actions in a Job, use the following call:

```
GET /integration_events?filter[job_action_id]=1,2,3,4,5&limit=500
```

From those results, you could use the following python request to parse out the index information.

```
# Get events for JobActions 1-5 from Integration 2:
params = {'filter[job_action_id]': '1,2,3,4,5',
'filter[integration_id]': 2,
}
resp = requests.get('https://<director>/integration_events.json',
auth=(<username>, <password>),
verify=False,
params=params)
for event in resp.json():
print("index:", event['untranslated']['index'], "\tevent:", event['description'])
```

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.