CrowdStrike Falcon
Splunk App v3.x+

User and Configuration Guide

Table of Contents

Overview

This document outlines the deployment and configuration of CrowdStrike App available for Splunk Enterprise and Splunk Cloud.

This app can be downloaded from Splunkbase: https://splunkbase.splunk.com/app/5094/

This app is designed to work with the data that's collected by the officially supported CrowdStrike Technical Add-Ons (TAs):

CrowdStrike Event Streams Technical Add-on: https://splunkbase.splunk.com/app/5082/

CrowdStrike Intel Indicators Technical Add-on: https://splunkbase.splunk.com/app/5083/

Getting Started

Prior to deploying the CrowdStrike App ensure the following:

1. At least one of the supporting OAuth2 based technical add-ons (TAs) has been successfully deployed, configured and is collecting data
2. The associated TAs have been successfully deployed to the system(s) that the App is being deployed to
3. Identify the index(es) that contain the CrowdStrike data
4. An account with proper access to identified Splunk systems is available
5. If any access requirements/modifications will be necessary for the App or accounts accessing it

NOTE:
As of version 3.0.0 – this App requires
at least the CrowdStrike Event Streams Technical Add-on version 3.5.0 or higher

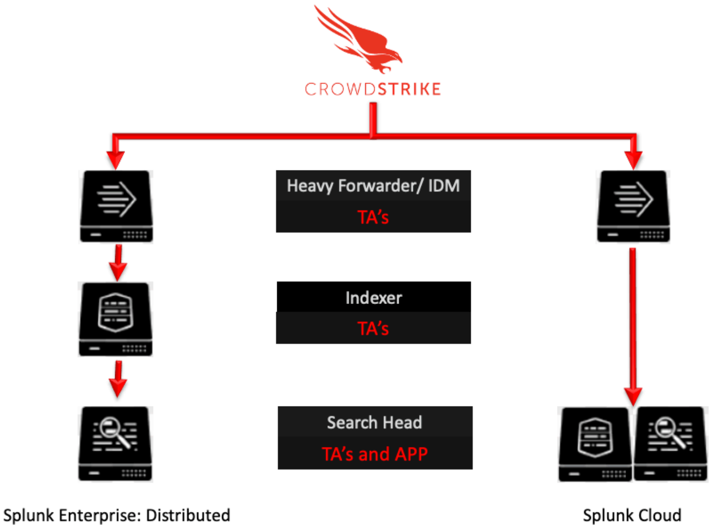
Version Update and Upgrades:

This version of the App introduces the following improvements:

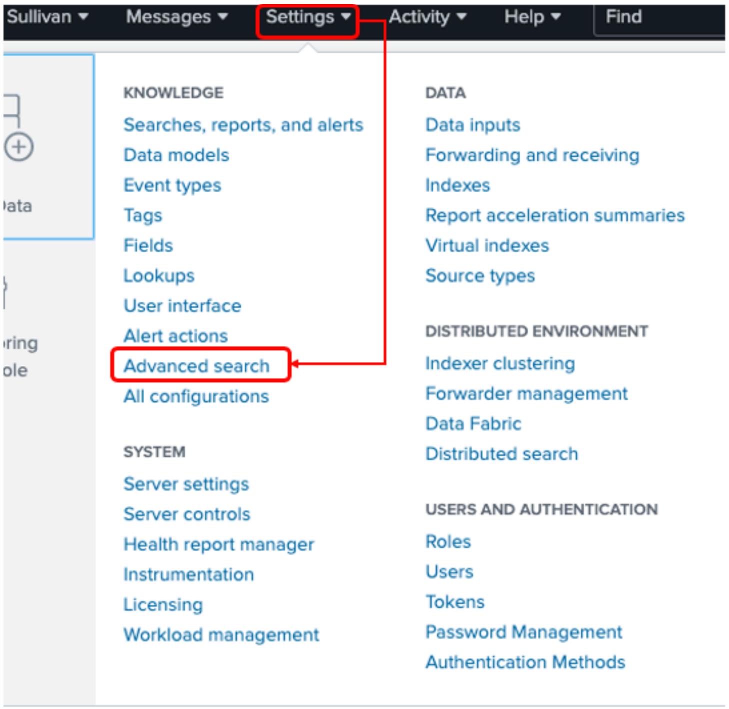
1. New Epp Detection Summary Event centric dashboards and drill downs.
2. Existing Detection and Events centric dashboards have been labeled as legacy.
3. Severity color coding for Epp Detections align with the severity color coding in the Falcon UI.

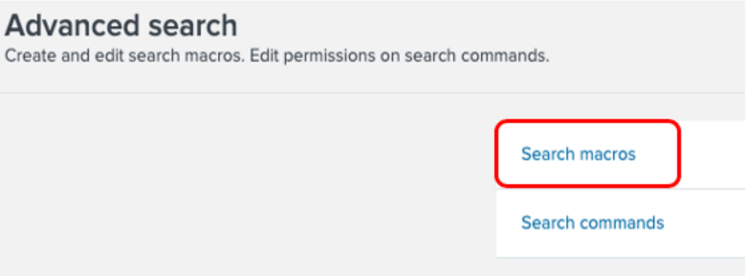
Deployment & Configuration

The CrowdStrike App should be deployed on Search Head systems or Splunk Cloud as it's designed to present the data that's being collected by the CrowdStrike TAs.



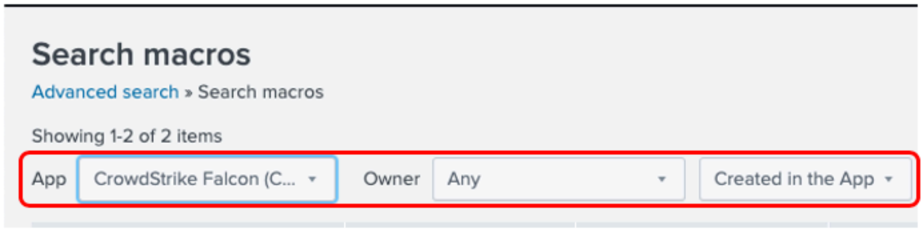
The searches that populate the dashboards leverage search macros to properly point to the indexes that contain the CrowdStrike information. These search macros can be found by navigating to 'Settings' -> 'Advanced Search' -> 'Search Macro' and selecting the CrowdStrike App from the dropdown selector (if necessary, select 'Created in App' as well):





Advanced search

Create and edit search macros. Edit permissions on search commands.



Search macros

Advanced search » Search macros

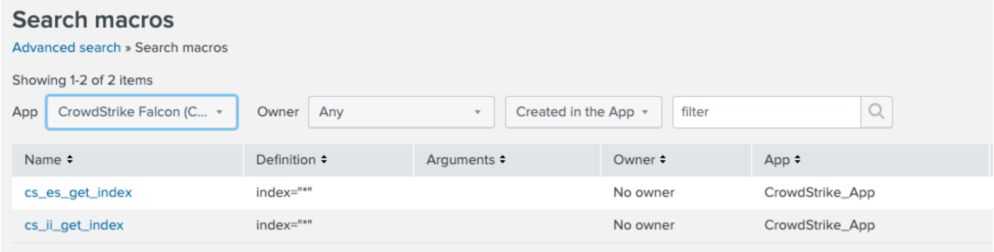
Showing 1-2 of 2 items

App: CrowdStrike Falcon (C...

Owner: Any

Created in the App

There are two search macros currently associated with this App:



Search macros

Advanced search » Search macros

Showing 1-2 of 2 items

App: CrowdStrike Falcon (C...

Owner: Any

Created in the App

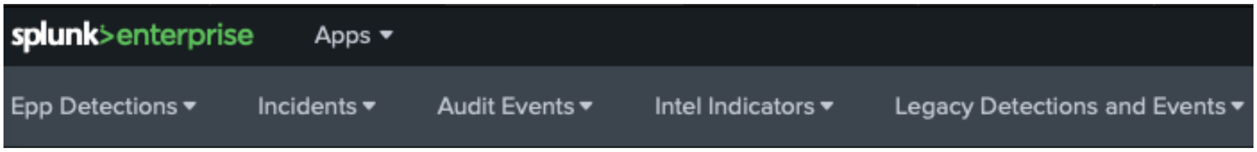
Name	Definition	Arguments	Owner	App
cs_es_get_index	index="*"		No owner	CrowdStrike_App
cs_ii_get_index	index="*"		No owner	CrowdStrike_App

- cs_es_get_index: This search macro is used to point to Event Streams TA data
- cs_ii_get_index: This search macro is used to point to Intel Indicator TA data

The default setting for the search macros are to point to all indexes, this may impact the search time and resources need and should be changed to point to specific index or indexes containing the specific TA data.

General Overview

There are five dashboard sections within the CrowdStrike App. The information that is displayed in these dashboards are dependent on the Technical Add-Ons (TAs) that provide the data:



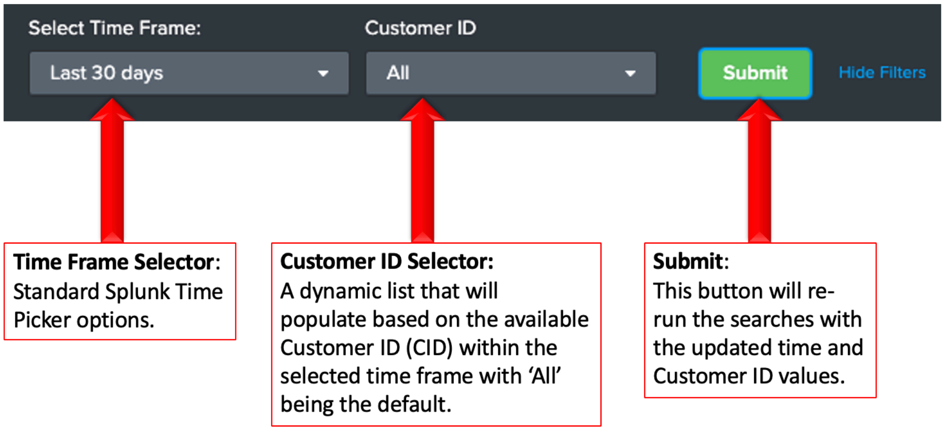
	Event Stream Add-on	Intelligence Add-on
Epp Detections	✓	
Incidents	✓	
Audit Events	✓	
Intel Indicators		✓
Legacy Detections and Events	✓	

The ‘Epp Detections’ section is the default selection and will be displayed when the App is initially open. Each of the dashboard sections represents a pulldown menu that will list the main dashboards that are accessible. It is important to note that not all dashboards are directly accessible, there are some dashboards that are only available as drilldowns.

Input Options

A majority of the dashboards will have input options, which are located at the top of the dashboard. These input options provide the ability to refine or expand the amount of data that's being represented in the dashboards. Input options can vary depending on the type of data that's being displayed but here are some of the more common:

Time Frame and Customer ID



Select Time Frame: Last 30 days

Customer ID: All

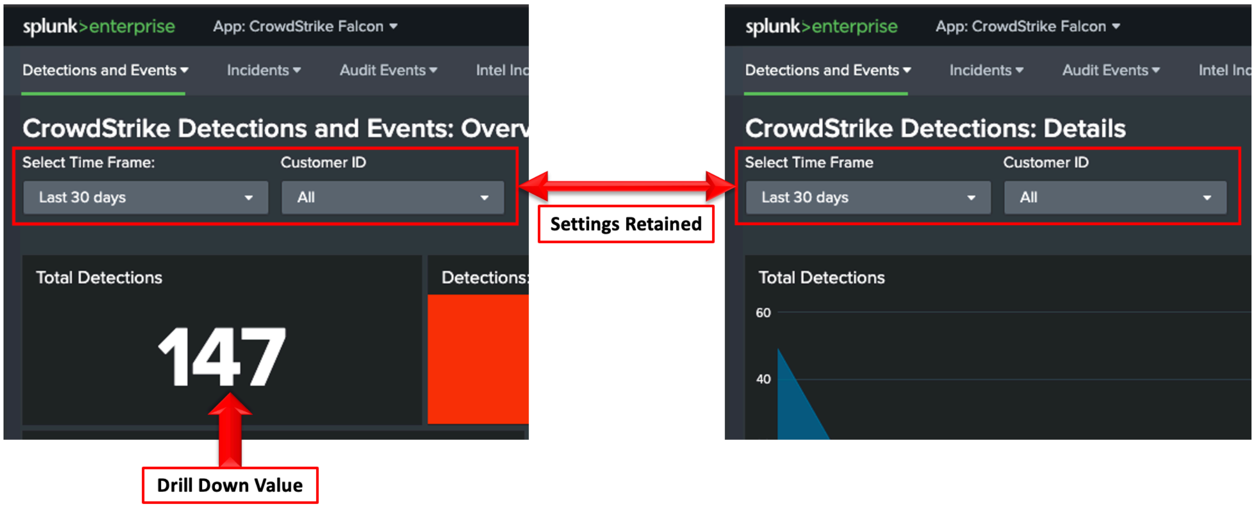
Time Frame Selector: Standard Splunk Time Picker options.

Customer ID Selector: A dynamic list that will populate based on the available Customer ID (CID) within the selected time frame with 'All' being the default.

Submit: This button will re-run the searches with the updated time and Customer ID values.

The Customer ID is populated by a search run within the selected time frame. If a new time frame is selected the Customer ID options will dynamically update. In order to apply a new time frame or select a specific Customer ID the 'Submit' button must be selected.

A majority of the dashboards have selection for the time frame and the Customer IDs available for that time frame. When clicking into a drill down value the select time frame and the Customer ID that have been selected will be retained and applied to the new dashboard:



CrowdStrike Detections and Events: Overv

Select Time Frame: Last 30 days

Customer ID: All

Total Detections

147

Settings Retained

CrowdStrike Detections: Details

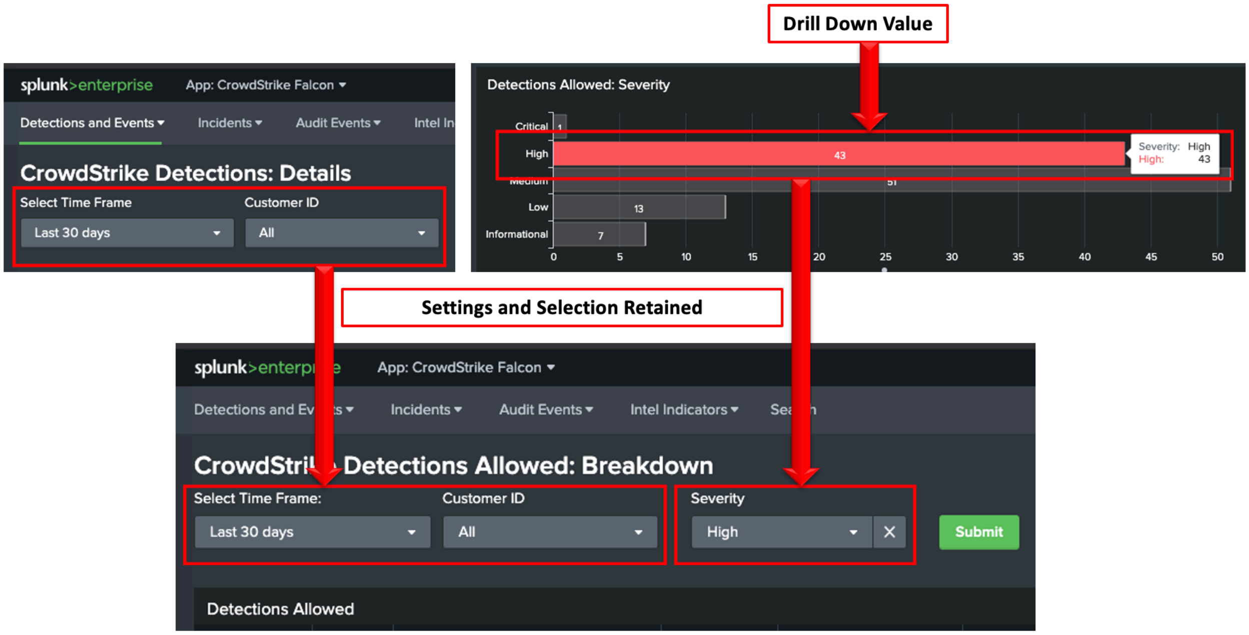
Select Time Frame: Last 30 days

Customer ID: All

Total Detections

Drill Down Value

Some drill downs can be on a certain value, such as severity, which will also be carried forward to the drill down:


Drill Down Value

Settings and Selection Retained

CrowdStrike Detections: Details

Select Time Frame: Last 30 days

Customer ID: All

Detections Allowed: Severity

Severity: High
High: 43

CrowdStrike Detections Allowed: Breakdown

Select Time Frame: Last 30 days

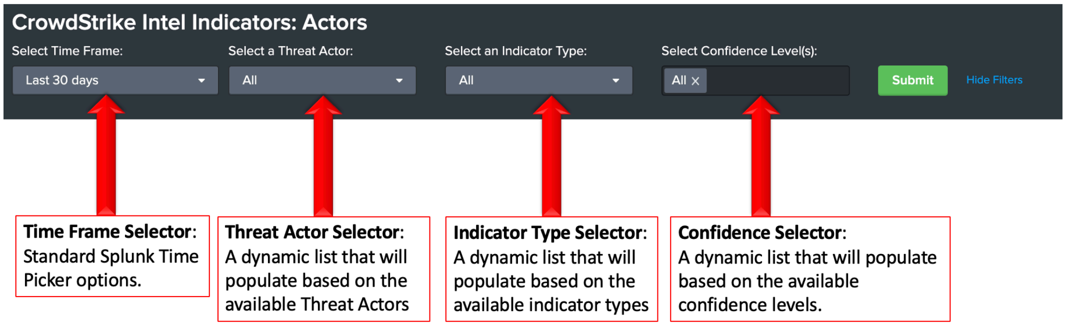
Customer ID: All

Severity: High

Detections Allowed

Intel Indicators Selections

The Intel Indicators dashboard does have different input options based on the different type of data that's available. For example:


CrowdStrike Intel Indicators: Actors

Select Time Frame: Last 30 days

Select a Threat Actor: All

Select an Indicator Type: All

Select Confidence Level(s): All

Time Frame Selector: Standard Splunk Time Picker options.

Threat Actor Selector: A dynamic list that will populate based on the available Threat Actors

Indicator Type Selector: A dynamic list that will populate based on the available indicator types

Confidence Selector: A dynamic list that will populate based on the available confidence levels.

Dashboard Sections

The app is divided into five main sections, each representing distinctly different information:

1. **EPP Detection Summary Events:** The “EPP Detection Summary Events’ section focuses on the detection architecture that was introduced in the Falcon Raptor migration and leverage the ‘EppDetectionSummaryEvent’ event type from the Event Streams API. For the purpose of these dashboards these terms are defines as:
    1) Epp Detection: A detection event that is base on a single EppDetectionSummary event.
    2) Epp Aggregated Detection: A grouping of EppDetectionSummary events based on a shared AggregateId field value.

    NOTE: The severity colors were updated to align with the coloring in the Falcon UI.

2. **Incidents:**
    The ‘Incidents’ section provides high level data on Falcon Incidents. The information provided is also broken down to show the host count, incident count and the event(s) count for the incident.

3. **Audit Events:**
    The ‘Audit’ section provides detailed information about actions taken within the Falcon UI and on/by the Falcon sensor. Authentication attempts to the UI and via API, policy events, group event, Spotlight reports, Real Time Response activity and File Quarantine actions are detailed here.

4. **Intel Indicators:**
    The ‘Intel Indicators’ section provides details on CrowdStrike’s Intelligence Indicators (Intelligence subscription required). The intelligence can be sorted and filter by attributes such as confidence levels, indicator types, threat actors and malware families.

5. **Legacy Detections and Events:**
    The ‘Legacy Detections and Events’ section focuses on Legacy Falcon detections and event, which use the ‘DetectionSummaryEvent’ event type from the Event Streams API. For the purpose of these dashboards these terms are defined as:
    1) Legacy Detections: Detections are identified by using the ‘event.DetectId’ field and counted in a 1:1 ratio, this field will represent a distinct count of the field value. E.g 10 events with the same event.DetectId value are considered 1 detection.
    2) Legacy Events: Events are also identified by using the ‘event.DetectId’ field, however they are counted per occurrence as opposed to a distinct count. E.g. 10 events with the same event.DetectId value are considered 10 events.

Dashboards and Drilldowns

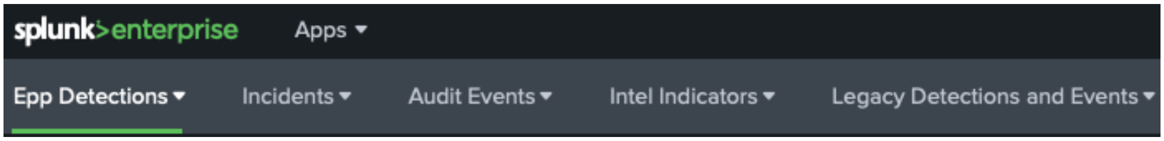
Each section contains a set of main dashboards as well as drilldown dashboards. These designations are defined as the following:

- **Main Dashboard:** A dashboard is directly accessible via the section dropdown
- **Drilldown Dashboard:** A dashboard that is accessible by clicking within another dashboard

In several sections ‘Main Dashboards’ are also considered ‘Drilldown Dashboards’ as they can be accessed by clicking on a value in a main dashboard.

Epp Detections Section

This section represents the new detection architecture that was introduced during the Falcon Raptor migration. It represents a summary of an EPP detection, the full version of which can be found by querying the Alerts API. The dashboard information is collected from the ‘EppDetectionSummary’ event type that’s provided in the Event Streams API. This dashboard requires the CrowdStrike Event Streams Technical Add-on to properly displace data.

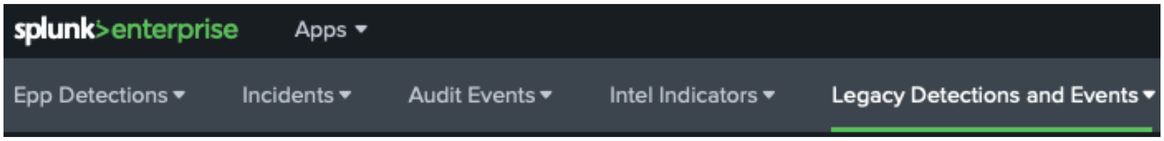


Data Source	Event Streams TA
Search Macro	`cs_es_get_index`
Main Dashboards	3
Drilldown Dashboards	5
Total Dashboards	6

Main Dashboards
CrowdStrike Epp Detection Summary Events: Overview
CrowdStrike Epp Detections: Details
CrowdStrike Epp Aggregated Detections: Details
Drilldown Dashboards
CrowdStrike Epp Detections: Details
CrowdStrike Epp Aggregated Detections: Details
CrowdStrike Epp Aggregated Detections with Allows: Breakdown
CrowdStrike Epp Aggregated Detections with Blocks: Breakdown
CrowdStrike Epp Detections Allowed: Breakdown
CrowdStrike Epp Detections Blocked: Breakdown

Legacy Detections and Events Section

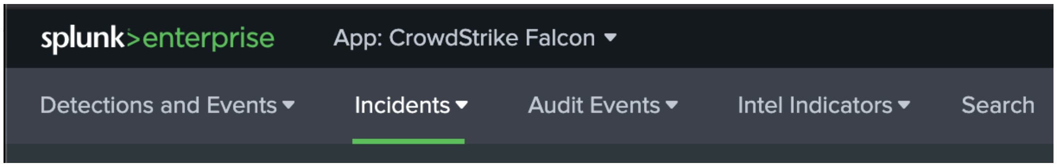
NOTE: This section has been relabeled as ‘Legacy’ and should be considered deprecated. The dashboards will continue to function as long as the ‘DetectionSummaryEvent’ event types are provided in the Event Streams API data or present in the index being queries during the selected time frame. Those events are projected to be removed in April 2025, at which time the dashboards will no longer show new data.
CrowdStrike recommends leveraging the new ‘Epp Detections’ area of this app moving forward.



Data Source	Event Streams TA
Search Macro	`cs_es_get_index`
Main Dashboards	3
Drilldown Dashboards	7
Total Dashboards	8

Main Dashboards
Legacy CrowdStrike Detections and Events: Overview
Legacy CrowdStrike Detection Details
Legacy CrowdStrike Events Details
Drilldown Dashboards
Legacy CrowdStrike Detections Details
Legacy CrowdStrike Detections Allowed Breakdown
Legacy CrowdStrike Detections and Events
Legacy CrowdStrike Detections Blocked Breakdown
Legacy CrowdStrike Detections Partially Blocked Breakdown
Legacy CrowdStrike Events Allowed Breakdown
Legacy CrowdStrike Events Blocked Breakdown
Legacy CrowdStrike Events Details

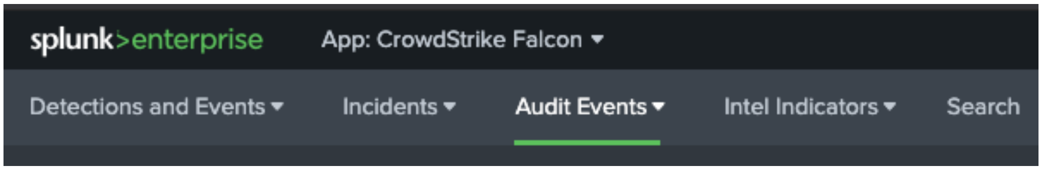
Incidents Section



Data Source	Event Streams TA
Search Macro	\`cs_es_get_index\`
Main Dashboards	2
Drilldown Dashboards	1
Total Dashboards	2

Main Dashboards
Crowdstrike Incidents
Crowdstrike Incidents Details
Drilldown Dashboards
Crowdstrike Incidents Details

Audit Events Section

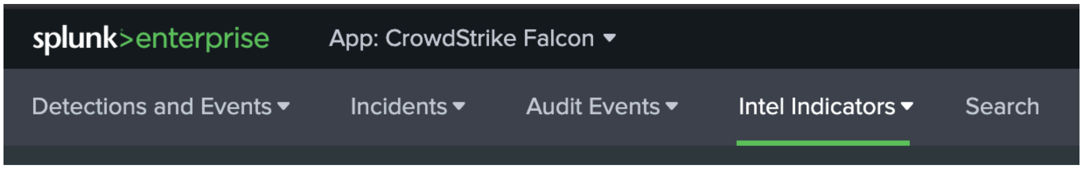


Data Source	Event Streams TA
Search Macro	`cs_es_get_index`
Main Dashboards	6
Drilldown Dashboards	22
Total Dashboards	28

Main Dashboards
CrowdStrike Audit Authentication Events
CrowdStrike Audit Policy Events
CrowdStrike Audit Group Events
CrowdStrike Audit Spotlight
CrowdStrike Audit Real Time Response
CrowdStrike Audit File Quarantine
Drilldown Dashboards
Crowdstrike Audit Authentication Failure
Crowdstrike Audit Authentication Successful
Crowdstrike Audit Policy Creations
Crowdstrike Audit Policy Deletions
Crowdstrike Audit Policy Disabled
Crowdstrike Audit Policy Enabled
Crowdstrike Audit Policy Updates
Crowdstrike Audit Groups Added
Crowdstrike Audit Groups Created
Crowdstrike Audit Groups Deleted
Crowdstrike Audit Groups Removed
Crowdstrike Audit Groups Rules Added
Crowdstrike Audit Groups Rules Removed
Crowdstrike Audit Groups Updated
Crowdstrike Audit Spotlight Report Created
Crowdstrike Audit Spotlight Report Deleted
Crowdstrike Audit File Release Requests
Crowdstrike Audit File Unrelease Requests

Crowdstrike Audit File Unreleased
Crowdstrike Audit Files Deleted
Crowdstrike Audit Files Quarantined
Crowdstrike Audit Files Released

Intel Indicators Section



Data Source	Intel Indicator TA
Search Macro	`cs_ii_get_index`
Main Dashboards	4
Drilldown Dashboards	3
Total Dashboards	4

Main Dashboards
Crowdstrike Intel Actors
Crowdstrike Intel Indicators Malware Families
Crowdstrike Intel Indicators Overview
Crowdstrike Intel Indicators Type Severity Search
Drilldown Dashboards
Crowdstrike Intel Indicators Malware Families
Crowdstrike Intel Indicators Overview
Crowdstrike Intel Indicators Type Severity Search

Troubleshooting and Support

CrowdStrike provides support for the Apps code and functionality.

Potential Issues and Resolutions

1. *No data is present in the dashboards*:
   - Ensure that the proper TA has been successfully deployed, configured and is providing data
   - Ensure that the Search Macro has been properly configured
   - Ensure that the user account(s) have the proper permissions to view the data and the dashboards

2. *Not all dashboards are populated*:
   - Validate that your CrowdStrike subscription provides that data
   - Ensure that the proper TA and version has been successfully deployed, configured and is providing data
   - Increase the time frame and ensure that there is data of that type within that time frame
   - Ensure that the proper TA has been deployed to the Search Head/Splunk cloud and that no inputs have been configured

3. *The Intel Indicators dashboard is not populated*:
   - Ensure that you have a valid CrowdStrike Intelligence subscription
   - Ensure that the Intel Indicator TA has been successfully deployed, configured and is providing data

Getting Support

Prior to contacting CrowdStrike support please review the following:

1. Ensure that the proper TAs have been successfully deployed, configured and are providing data
2. Ensure the account being used is able to access both the data and the dashboards
3. Validate that the App has the proper permissions to access the data
4. Verify that the search macros have been properly configured for the App
5. Record the following information about the Splunk system(s):
    - Splunk environment type
    - Splunk version
    - App version
    - TA version(s)
6. Navigate to https://supportportal.crowdstrike.com/
7. Provide the collected information, as well as any addition relevant information in the support request

Recommended:
If the issue has to do with missing data, it is highly recommended to also provide the information and log data that is called out in the Getting Support section of the Technical Add-on Guide for the TA(s) that provides that data.