Splunk® InfoSec App Administration Guide 1.7.0

Generated: 8/02/2021 2:48 pm

Table of Contents

Configure the Splunk InfoSec App

Confirm the health of the InfoSec app for Splunk

Prerequisite

Ensure that you have installed the Splunk InfoSec app in your Splunk platform environment. For information on installing the Splunk InfoSec app, see Install the Splunk InfoSec app in the *Splunk InfoSec App Installation Guide*.

Follow these steps to confirm the health of the InfoSec app:

1. In Splunk Web, navigate to the InfoSec app for Splunk by selecting the app from the **App** menu.
2. In the InfoSec app, select the Health dashboard. The first two rows of visuals within the Health dashboard provide an overview of the data in your Splunk platform environment.
3. Verify the following three metrics using the Health dashboard:

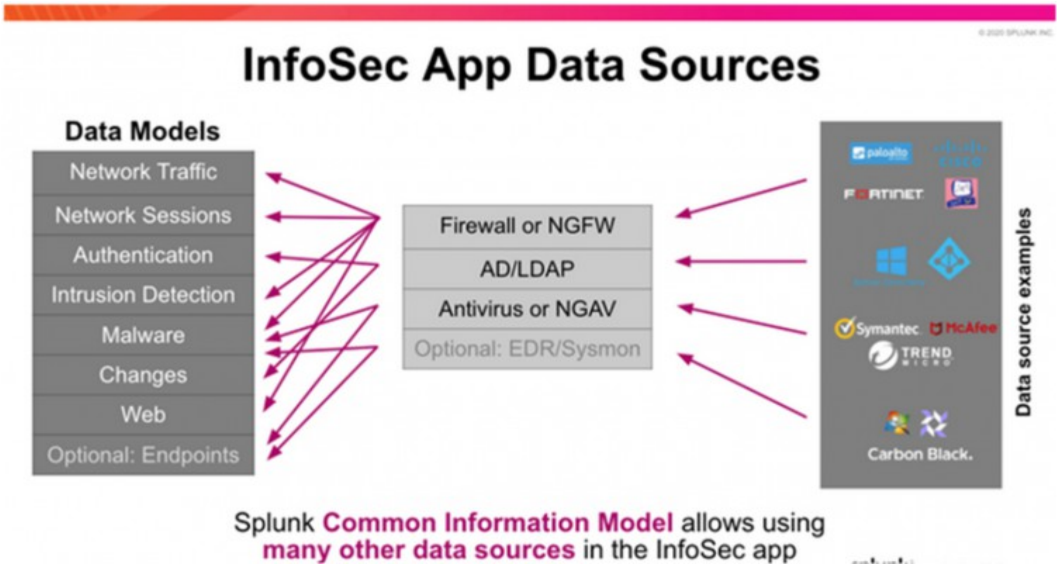
Metrics	Additional information
Count of events that feed each of the data models that are required by the InfoSec app	If the Health dashboard shows that no data feeds into a data model, there may not be an available data source that feeds the data models in your Splunk platform environment. To validate data sources and confirm that your environment is configured correctly for each of the data models, see Validate data sources that feed the data models of the Splunk InfoSec app.
Acceleration status for each of the data models that are required by the InfoSec app	Enable acceleration only for the data models that are fed with data To set acceleration for your data models, see Accelerate data models to build the Splunk InfoSec app dashboards.
Installation status for each of the supporting apps or add-ons that are required by the InfoSec app	If the Health dashboard does not report that the required add-ons are installed, see Install additional apps and add-ons in the Splunk InfoSec app *Installation Guide* to confirm that your environment is configured correctly .

Validate data sources that feed the InfoSec app for Splunk data models

Validate the data sources for each of the data models that are listed on the Health dashboard of the Splunk InfoSec app, even if the Health dashboard reports that data is fed into the data model.

> If only partial data is fed into the data models, you might need to adjust your configuration to ensure full coverage of your Splunk Platform. Additionally, your data sources might feed more than one data model.

The following diagram shows some of the data sources that feed into the data models for the InfoSec app, including firewall, LDAP, and antivirus data:



InfoSec App Data Sources

Data Models

- Network Traffic
- Network Sessions
- Authentication
- Intrusion Detection
- Malware
- Changes
- Web
- Optional: Endpoints

- Firewall or NGFW
- AD/LDAP
- Antivirus or NGAV
- Optional: EDR/Sysmon

Data source examples

Splunk **Common Information Model** allows using **many other data sources** in the InfoSec app

Validate data model configuration

Follow these steps to validate data model configurations and to check that the data sources feed the data models as expected:

1. Use the following search to identify the indexes and source types that feed each of the InfoSec data models:

   ```
   | makeresults | eval datamodels =
   "Authentication:Change:Endpoint:Intrusion_Detection:Network_Sessions:Network
   _Traffic:Malware:Endpoint.Processes:Web" | makemv delim=":" datamodels | mvexpand datamodels | map
   search="| makeresults | eval notfound=\"*** NO DATA FOUND ***\" | append [| tstats count from
   datamodel=$datamodels$ by index, sourcetype] | eventstats count as events |eval
   datamodel=\"$datamodels$\", index=coalesce(index,notfound)| search NOT notfound=* OR events=1 |
   table datamodel, index, sourcetype,count" | sort datamodel, index, sourcetype
   ```

   If the results of the search indicate that each of the required data models for the InfoSec app is populated with data, you can accelerate the data models. See Accelerate data models to build InfoSec app dashboards.

   If the results of the search indicate that all the required data models for the InfoSec app are not populated with data, proceed to the next step.
2. Identify the tagged events to configure the data models that are required by the InfoSec app within your Splunk Platform environment. To identify the tagged events and configure your data models, see Identify tagged events to configure data models.
3. Repeat the process for each data model.

Identify tagged events to configure data models

Follow these steps to identify tagged events and to configure the data models. This example uses the Authentication data model, but you can follow these steps to identify tagged events for any data model.:

1. On the Splunk Platform menu bar, select **Configure** > **Settings** > **Data models**.
2. Select the **Authentication** data model from the list of data models.
3. Use the search bar to identify the events that must feed the Authentication data model.

```
(`cim_Authentication_indexes`) tag=authentication NOT (action=success user=*$)
```

The first part of the search contains a macro called `cim_Authentication_indexes`. This macro constrains the search to certain indexes.

> You must restrict a data model to only the indexes that feed it with data.

The next part of the search `tag=authentication` constrains the search to return events that are tagged as authentication events.

The last part of the search `NOT (action=success user=*$)` excludes any event that contains a field with the label `action` that has the value `success` AND the field `user` that has a value that ends with the `$` character.

4. Identify the data sources in Splunk that might fit your search. For more information on identifying data sources, see Identify data sources that feed data models.

Identify data sources that feed data models

Follow these steps to identify the data sources that feed the data models:

1. Open a new Splunk Platform search window in another tab of your browser.
2. Click **Search & Reporting**.
3. Select **Open Link in New Tab**.
   Before switching to the new browser tab, highlight and copy the search from the tab you are in and paste it into the search bar in the new browser window.
4. Run the search in the new tab.
5. Modify the search to include all the indexes within your Splunk environment.
6. Run the following search to see if any results are returned:

   ```
   index=* tag=authentication NOT (action=success user=*$) | stats count by index, sourcetype
   ```
7. Modify the search macro for the data model if your search results show indexes and data sources. For more information on modifying the search macro, see Modify the search macro for the data model.

Modify the search macro for the data model

Prerequisite

Take note of the name of the indexes returned by the search in Identify the data sources that feed the data models so that you can update the macro.

Follow these steps to modify the search macro for the data model. This example uses the Authentication data model which is fed by the demo_oracle and demo_wineventlog indexes, but you can follow these steps to modify the search macro for any data model.:

1. On the Splunk platform menu bar, select **Configure > Settings**.
2. Open **Advanced Search** under the **Settings** menu.
3. Open **Search Macros**.
4. Search for the `cim_Authentication_indexes` macro. You might need to adjust the filter to find the macro.
5. Set the app context to **All** and type **cim_authentication_indexes** into the search filter.
   If the definition is set to `index=main`, the Authentication data model was not fed data.
6. Click on the macro name to edit the macro.

7. Change the **Indexes Allowlist** to include the indexes that were identified in the previous step.
8. Click **Save**.
9. Rerun the following original data model search to verify that the change to the search macro was successful.

```
(`cim_Authentication_indexes`) tag=authentication NOT (action=success user=*$)
```

10. Repeat this process for all of the following InfoSec data models:
    - Authentication
    - Change (for app version 1.6.x and higher) or Change Analysis (for app version 1.5.3 and lower)
    - Intrusion_Detection
    - Malware
    - Network_Sessions
    - Network_Traffic
    - Endpoint
    - Web

Examples searches for InfoSec app data models

The following table lists the default constraining search and search macro for each of the required data models for the Infosec app. There is no search macro defined for the data models listed. If the search macros is not defined for the data model, the data model relies on the data that resides in the indexes that are searched by default.

Data model	Base search	Search macro
Authentication	(`cim_Authentication_indexes`) tag=authentication NOT (action=success user=*$)`	No search macro defined
Change	(`cim_Change_indexes`) tag=change NOT (object_category=file OR object_category=directory OR object_category=registry)	No search macro defined
Intrusion Detection	(`cim_Intrusion_Detection_indexes`) tag=ids tag=attack	No search macro defined
Malware	(`cim_Malware_indexes`) tag=malware tag=attack	No search macro defined
Network Sessions	(`cim_Network_Sessions_indexes`) tag=network tag=session	No search macro defined
Network Traffic	(`cim_Network_Traffic_indexes`) tag=network tag=communicate	No search macro defined
Endpoint	(`cim_Endpoint_indexes`) tag=listening tag=port | eval transport=if(isnull(transport) OR transport="","unknown",transport),dest_port=if(isnull(dest_port) OR dest_port="",0,dest_port),transport_dest_port=mvzip(transport,dest_port,"/") | mvexpand transport_dest_port	No search macro defined

Data model	Base search	Search macro
Web	``(`cim_Web_indexes`) tag=web``	No search macro defined

Accelerate data models to build InfoSec app for Splunk dashboards

Accelerate data models after you confirm that the correct event data is fed into the data models that are required for the Splunk InfoSec app. You must accelerate each of the data models.

You can only accelerate the data models after you confirm that they are fed with the correct event data because after acceleration, the data models cannot be edited without first disabling the acceleration.

Accelerate a data model

Perform the following steps on all the data models that are fed event data. This example uses the Authentication data model, but you can follow these steps to accelerate any data model.

Don't accelerate a data model that contains no event data.

1. On the Splunk Platform menu bar, select **Configure** > **Settings** > **Data models**.
2. Identify the **Authentication** data model.

   > Do not click on the '''Authentication''' data model because you must work within the current web page.
3. From the **Actions** column, select **Edit** > **Edit Acceleration**.
4. In the **Edit Acceleration** dialog box, perform the following actions:
   1. Check **Accelerate**.
   2. Set the **Summary Range** to a suitable time frame.
   3. Click **Save**.

   When the Splunk platform starts to build the data model accelerations, track the progress of the accelerations from the Health dashboard of the InfoSec app. The InfoSec app is configured to work with your data sources.
5. View each of the InfoSec app dashboards from the menu bar starting with **Security Posture**.
6. Confirm that all the dashboards are populating with data. If you find a dashboard that is not populating, you might not have the required data source within your Splunk platform to feed the dashboard. For more information on troubleshooting, see Troubleshoot the Splunk InfoSec app.

Extend the capabilities of the InfoSec app for Splunk

Extend the monitoring capabilities of the Splunk InfoSec app by building your own dashboard panels and alerts.

Use the following examples to guide you through two scenarios to extend the monitoring capabilities of the InfoSec app:

- Add a new dashboard panel to the Custom Use Cases dashboard within the InfoSec app
- Add a new alert to the InfoSec app

You must create a custom search to add a new dashboard panel or to add a new alert to the InfoSec app.

Build a custom search

Follow these steps to build a custom search:

1. Navigate to the Splunk Security Essentials (SSE) app within your Splunk Platform environment.
   If you need to download and install the SSE app, you can find the Splunk Security Essentials app (SSE) on Splunkbase.
2. Select **Security Content** from the Security Content menu.
3. Select the **Windows Event Log Clearing Events** search.
4. Select **Live Data from the View** when the search opens.
5. Scroll down and locate **SPL Mode**.
6. Enable **SPL Mode**.
7. Select the search and copy it to your clipboard.

   ```
   index=* (source="*WinEventLog:Security" AND (EventCode=1102 OR EventCode=1100)) OR
   ((source="*WinEventLog:System") AND EventCode=104) | stats count by _time EventCode sourcetype host
   ```
8. Navigate back to the InfoSec app to add it as the custom use case or as an alert.

Example 1 : Add a panel to the Custom Use Cases dashboard

Follow these steps to add a panel to the Custom Use Cases dashboard:

1. Navigate to the InfoSec app within your Splunk Platform environment.
2. Select **Search** from the Search menu within the InfoSec app.
3. Paste the custom search that you copied onto your clipboard. Build a custom search into the search bar.
4. Set a suitable time range.
   For this example, set the time range to **Last 24 hours**.
5. Run the search by clicking the magnifying glass icon.
6. Select the **Dashboard** Panel from the **Save As** menu to add the table to the dashboard panel.
7. Type the following details in the dialog box that opens:
8. *Select **Existing Dashboard**.
9. From the drop-down menu, list, locate, and select the **Custom Use Cases** dashboard.
10. Type in a title for the new dashboard panel. For example, Detected Log File Tampering.
    A new panel is added to the dashboard.

Example 2: Add an alert

Follow these steps to add an alert:

1. Navigate to the InfoSec app within your Splunk Platform environment.
2. Select **Search** from the Search menu within the InfoSec app.
3. Paste the custom search that you copied onto your clipboard in Build a custom search into the search bar.
4. Set a suitable time range.
   For this example, set the time range to **Last 60 minutes**.
5. Run the search by clicking the magnifying glass icon.
6. From the **Save As** menu, select **Alert**.
7. Type a title and description for the alert in the dialog box that opens.
8. Set the permissions to be **Shared in App** so that other users have access to the new alert.
9. Set the Alert type as **Scheduled**. For this example, run the search every hour.
10. Check that the settings set off an alert when the number of results is greater than 0.
11. Under **Trigger Actions**, add the action **Add to Triggered Alerts**.

12. Click **Save**.
    You can verify that the alert is saved by navigating to the Alerts dashboard and selecting **Edit Existing Alerts**.

Troubleshoot the InfoSec app for Splunk

Following are some of the common installation and configuration issues for the Splunk Infosec app:

For more information on troubleshooting the InfoSec app, search Splunk Answers using the tag InfoSec App for Splunk.

Dashboards don't display any data

Problem

One or more dashboards aren't displaying any data.

Cause

The search that drives the dashboard is unable to locate the data within your Splunk platform environment.

Solutions

To check if the search that drives the dashboard is able to locate the data within your Splunk platform environment, click on the magnifying glass on the dashboard to examine the associated search string. The first line identifies the data model on which the dashboard is based. Revisit the configuration steps to ensure that the correct data is fed into the identified data model. For more information to validate data sources, see Validate data sources that feed the infoSec app for Splunk data models.

You can also simplify the search to determine which part of the search prevents the data from being displayed. Additionally, you can remove all but the first line of the search to check if any data is returned. You can also re-add the additional lines from the original search, one-by-one, to identify which component of the search prevents data from being returned as expected. Your data might not be fully Common Information Model (CIM) compliant and you might need to revisit the configuration.

Dashboard displays error message about missing visualization

Problem

Dashboard displays the following error message: "No matching visualization found for type: <type>, in app: <app_name>".

Cause

One of the supporting add-ons is not be installed or is disabled.

Solutions

1. On the Splunk Enterprise toolbar, select **Apps > Manage Apps** and confirm that the missing supporting app or add-on is installed.
2. Check that the supporting app or add-on is not disabled and that the permissions for the app or add-on is set to shared.

Dashboards display error message about missing data model

Problem

Dashboard displays the following error message:`Data model was not found`.

Cause

A specific data model is missing from the InfoSec app.

Solution

1. On the Splunk Enterprise menu bar, select **Configure** > **Settings** > **Data models**.
2. Find the data model and confirm that the permissions are set correctly.
3. Confirm that the Common Information Model (CIM) app is correctly installed and that the app is enabled within the **Settings** menu.

InfoSec app is not visible in the Splunk App menu

Problem

The Splunk InfoSec app is installed but is not visible in the Splunk App menu.

Cause

The InfoSec app is disabled.

Solution

1. On the Splunk Enterprise menu bar, go to the **Manage Apps** menu and check the settings for the InfoSec app. .
2. Select the **Edit Properties** menu and enable the app