Splunk® App for SOAR
Use Splunk App for SOAR 1.0.0

Generated: 10/31/2022 11:46 pm

Table of Contents

Get to know Splunk App for SOAR

Learn about Splunk App for SOAR

Use Splunk App for SOAR to bring in data from Splunk SOAR to Splunk Cloud Platform or Enterprise for collecting, searching, monitoring, reporting, and analyzing. Splunk App for SOAR unifies functionality from other apps, such as Splunk Phantom Remote Search and Splunk Add-on for Phantom to create a streamlined process for observing data from Splunk SOAR.

With Splunk App for SOAR, you can ...

- Use SPL commands to refine searches through Splunk SOAR data.
- Report Splunk SOAR data at a glance through dashboards.
- (Optional service.) Monitor the health of your Splunk SOAR (On-premises) environments using dashboards.
- Pull audit logs from any number of Splunk SOAR instances.
- Issue REST API commands to Splunk SOAR environments.

When using the remote-search service in Splunk App for SOAR, the data flows from Splunk SOAR to Splunk Cloud Platform or Enterprise. If you want to set up a flow of data from Splunk Cloud Platform or Enterprise to Splunk SOAR, you must use Splunk App for SOAR Export.

Use remote search in Splunk App for SOAR

Learn about the remote-search service in Splunk App for SOAR

Splunk SOAR can use an external Splunk Cloud Platform or Enterprise instance as the main search engine to search for Splunk SOAR data. To do that, install Splunk App for SOAR (previously known as Splunk Phantom Remote Search) on your Splunk instance to connect your Splunk instance to your Splunk SOAR instance.

After you have configured the remote-search feature on your Splunk SOAR instance, you can use Splunk searches on your Splunk SOAR data. Refer to the **Search reference** manual for more information about search functionality, SPL syntax, and more.

Use the Splunk SOAR System Logs in Splunk App for SOAR

Learn about the Splunk System Logs in SOAR in Splunk App for SOAR

Splunk App for SOAR provides system logs that allow you to monitor the health of your Splunk SOAR instances. The security orchestration, automation, and response (SOAR) platforms are designed to reduce the scale of your security operations. With Splunk SOAR, you can automate tasks, orchestrate workflows, and support a broad range of SOC functions, including event management, case management, collaboration, and reporting.

Find log files

To locate SOAR System Logs, navigate to these locations:

- Server configurations: $SPLUNK_HOME/var/log/splunk/soar_configuration.log.
- Audit checkpoint: $SPLUNK_HOME/var/lib/splunk/modinputs/audit.
- Audit logs: $SPLUNK_HOME/var/log/splunk/soar_audit.log.
- Index creation and setup: $SPLUNK_HOME/var/log/splunk/soar_setup.log.

Use dashboards in Splunk App for SOAR

Understand dashboards in Splunk App for SOAR

Use the dashboards in Splunk App for SOAR to monitor a variety of metrics that help you manage your Splunk SOAR instances:

- Use the dashboards available in the Automation Insights dropdown to see metrics about the actions that run on your Splunk SOAR instances.
- Use the dashboard available from the SOAR Container Overview dropdown to get a summary of all the containers in your Splunk SOAR instances.
- Use the dashboards available in the Container Insights dropdown to see metrics about the containers in your Splunk SOAR instances.

Use the Automation Insights dashboards

Use the dashboards available in the **Automation Insights** dropdown to see metrics about the actions that run on your Splunk SOAR instances. The **Automation Analytics** dashboard helps you understand what actions are running on your Splunk SOAR instances, and the **Action Run Search** dashboard helps you understand specific actions being run on your Splunk SOAR instances. You can also filter what actions you see so that you can find the exact information you need, when you need it.

The Automation Analytics dashboard

Use the **Automation Analytics** dashboard to understand what actions are running on your Splunk SOAR instances.

This dashboard contains many visualizations that are helpful for understanding the actions analysts take in your Splunk SOAR instances:

- **Action Execution Over Time**: This visualization shows the count and average execution time of successful and failed actions that analysts have taken over a period of time. You can specify the period of time from the dropdown menu with the default value, **Last 24 hours**. You can also use the legend items, **count: failed**, **count: success**, **execution_time: failed**, and **execution_time: success**, to filter what information displays in the visualization.
- **Most Active Analysts**: This visualization shows the top ten most active analysts in your Splunk SOAR instances. The visualization displays those users' IDs and the number of actions they've executed in your Splunk SOAR instances. If you have more than Splunk SOAR instance that you're monitoring, you can specify the instance you want to see by selecting the name of that instance from the legend or the name of the instance from the **Index Prefix** dropdown.
- **Most Active Actions**: This visualizations shows the top ten most run actions in your Splunk SOAR instances. You can filter by whether the actions were successes or failures.
- **Action Run by Status**: This visualization shows the number of successful and failed action runs as a percentage. If you hover over the portions of the pie chart, a pop-up displays the **status**, **count**, and **count%**.
- **Actions with Highest Failure by Asset**: This visualization shows the top ten actions that failed by asset. You can filter by asset by selecting the desired asset from the legend.
- **Action Run Count by Status**: This visualization shows the counts of successful and failed actions that have been run by the name of the action.

Filter information in the Automation Analytics dashboard

All of the visualizations are affected by the three dropdowns on the page, the **Last 24 hours**, **Index Prefix**, and **User ID (Username)** dropdowns. Use those dropdowns to filter out unnecessary information and find what you need. Many of the visualizations can be filtered further by selecting or hovering over their index items.

The Action Run Search dashboard

Use the **Action Run Search** dashboard to better understand specific actions being run on your Splunk SOAR instances.

This dashboard contains one visualizations and a table. Both are helpful for understanding the actions analysts take in your Splunk SOAR instances:

- **Automation Timechart**: This visualization shows the count and average execution time of playbooks that analysts have run over a period of time. You can specify the period of time from the dropdown menu with the default value, **Last 24 hours**. You can also use the legend items, **count** and **execution_time_sec**, to filter what information displays in the visualization.
- **Action Run Table**: This table shows specific actions that analysts have taken in your Splunk SOAR instances.

Filter information in the Action Run Search dashboard

All of the visualizations are affected by dropdowns, checkboxes, and fields on the page, the **Last 24 hours**, **Index Prefix**, and **User ID (Username)** dropdowns; the **Status** checkboxes; and **Playbook Run ID** field. Use those to filter out unnecessary information and find what you need. The visualization can be filtered further by selecting or hovering over its index items.

Use the SOAR Container Overview dashboard

Use the dashboard available from the **SOAR Container Overview** dropdown to get a summary of all the containers in your Splunk SOAR instances.

The **SOAR Container Overview** dashboard contains many different visualizations that are helpful for monitoring the containers in your Splunk SOAR isntances:

- **New Containers**: This visualization shows number of available containers.
- **Open Containers**: This visualization shows the number of open containers.
- **Resolved Containers**: This visualization shows the number of resolved containers.
- **Average Container Duration**: This visualization shows the average duration containers have remained open.
- **Average Resolution TIme**: This visualization shows the average duration containers have remained open before being closed.
- **Containers by Status**: This visualization shows the number of containers as a percentage by status.
- **Highest Container Duration Time by Analyst**: This visualization shows which containers have remained open the longest by analyst.
- **Analyst Performance**: This table shows performance metrics for each analyst.
- **Longest Container Duration - Table**: This table shows the containers that have remained open the longest.
- **Longest Container Duration**: This visualization shows the containers that have remained open the longest.

Filter information in the SOAR Container Overview dashboard

Use the dropdowns and fields in the **SOAR Container Overview** dashboard to filter what information you can see.

- **Last 24 hours**: Use this dropdown to specify the time period for information you want to display in the dashboard.
- **Index Prefix**: Use this dropdown to specify the Splunk SOAR instances whose information you want to display in the dashboard.
- **Analyst**: Use this dropdown to specify the analysts whose information you want to display in the dashboard.
- **Container Type**: Use this field to enter the types of containers whose information you want to display in the dashboard.
- **Sensitivity**: Use this field to enter the sensitivity of containers whose information you want to display in the dashboard.
- **Severity**: Use this field to enter the severity of containers whose information you want to display in the dashboard.
- **Label**: Use this dropdown to specify the labels for containers whose information you want to display in the dashboard.
- **Status**: Use this field to enter the status of containers whose information you want to display in the dashboard.

Use the Container Insights dashboards

Use the dashboards available in the **Container Insights** dropdown to see metrics about the containers in your Splunk SOAR instances. The **SOAR Container Insights** dashboard helps you understand what actions are running in particular containers on your Splunk SOAR instances, and the **Container & Notes Search** dashboard provides tables that allow you to find specific cases and notes. You can filter what information you see so that you can find the exact information you need, when you need it.

The SOAR Container Insights dashboard

Use the **SOAR Container Insights** dashboard to understand what actions are running in particular containers on your Splunk SOAR instances.

This dashboard contains many visualizations that are helpful for understanding the actions analysts take in particular containers on your Splunk SOAR instances:

- **Current Status**: This visualization shows the current status of the container.
- **Duration**: This visualization shows how long the container has been open.
- **Last Owner**: This visualization shows the name of the last owner of the container.
- **Action Run**: This table shows the actions run in the container.
- **Container Notes**: This table shows notes associated with the container.
- **Task Notes**: This table shows notes associated with each task.

Filter information in the SOAR Container Insights dashboard

All of the visualizations and tables are affected by the three dropdowns on the page, the **Last 7 days**, **Index Prefix**, and **Container ID (REQUIRED)** dropdowns. Use those dropdowns to filter out unnecessary information and find what you need.

The Container & Notes Search dashboard

Use the **Container & Notes Search** dashboard to understand the cases and notes associated with particular containers on your Splunk SOAR instances.

This dashboard contains several tables that are helpful for understanding the cases and notes in particular containers on your Splunk SOAR instances:

- **Case Search Match**: This table shows summaries of cases associated with particular containers.
- **Notes Search Match**: This table shows summaries of notes associated with particular containers.
- **Case Search Match**: This drilldown shows data for cases associated with particular containers.
- **Notes Search Match**: This drilldown shows data for notes associated with particular containers.

Filter information in the SOAR Container Insights dashboard

All of the visualizations and tables are affected by the three dropdowns and five fields on the page, the **Last 24 hours**, **Index Prefix**, and **Label** dropdowns and the **Search**, **Container Type**, **Sensitivity** and **Status** fields. Use those to filter out unnecessary information and find what you need.

Use auditing in Splunk App for SOAR

Audit logs from Splunk SOAR instances using Splunk App for SOAR

With Splunk App for SOAR, you can audit data pull audit logs from any number Splunk SOAR instances.

Follow these steps to use auditing in Splunk App for SOAR:

1. Make sure the Splunk SOAR server with logs you want to audit is properly configured. During the configuration, when setting up the server, make sure you've entered the information for an automation Splunk SOAR user with an Observer role in the **Authorization Configuration** field. That user is able to set up modular inputs and fetch audit logs.
2. Select the **Configurations** tab to go to the **SOAR Server Configuration** page.
3. For the server you want to audit, select the **Manage** dropdown and then the **Edit Audit Input** option.
4. Enter the name of the input name in the **Audit Input Name** field. The input name is the source.
5. Specify the **Start Date** and **Start Time**.
6. Choose an interval.
7. Select the index from the **Index** dropdown.
8. Select **Save**

Use REST API commands with Splunk App for SOAR

Make REST API calls to Splunk SOAR instances with Splunk App for SOAR

With Splunk App for SOAR, you can now make REST API calls to Splunk SOAR instances. You can make REST API calls to any Splunk SOAR instances listed on the **SOAR Server Configuration** page. To see what servers are available for REST API calls, select the **Configurations** tab.

> When using the REST API calls using Splunk App for SOAR, be careful to optimize any searches so as to ensure high performance.

restsoar

Use the `restsoar` generating command to retrieve information from a Splunk SOAR instance. Because this command is generating you must issue it first when you run an SPL search.

This command requires `endpoint` and `soar_server` parameters:

- `endpoint`: The endpoint of the Splunk SOAR environment (e.g., `/container/`).
- `soar_server`: The name of the Splunk SOAR environment, as configured in Splunk App for SOAR (e.g., "soar-1").

Examples

This command retrieves information about "container 2" from a Splunk SOAR environment named "soar-1":

```
|restsoar endpoint=/container/2 soar_server="soar-1"
```

This command retrieves an audit trail for "container 2" from a Splunk SOAR environment named "soar-1":

```
|restsoar endpoint=/container/2/audit soar_server="soar-1"
```

restsoarstream

Use the `restsoarstream` eventing command to manipulate the data in a Splunk SOAR instance. Because this command is an eventing command, it enriches events with more information, and can be used within a search pipeline. The `endpoint` parameter is a field name instead of string, which allows you to issue multiple requests to a Splunk SOAR API within a single command.

This command requires `endpoint` and `soar_server` parameters:

- `endpoint`: The endpoint of the Splunk SOAR environment (e.g., `/container/`).
- `soar_server`: The name of the Splunk SOAR environment, as configured in Splunk App for SOAR (e.g., "soar-1").

Example

This example demonstrates how to fetch information from containers with IDs 1â 10 from a Splunk SOAR environment named "soar-1":

```
|makeresults count=10
|streamstats count
|rename count as id
|eval endpoint = "/container/".id."/phases"
|restsoarstream endpoint=endpoint soar_server="soar-1"
|mvexpand soar_response
|eval soar_response=replace(soar_response,"'","\"') | spath input=soar_response
```

Troubleshoot Splunk App for SOAR

Find log files

To locate Splunk App for SOAR log files to help you troubleshoot issues, navigate to these locations:

- Server configurations: $SPLUNK_HOME/var/log/splunk/soar_configuration.log.
- Audit checkpoint: $SPLUNK_HOME/var/lib/splunk/modinputs/audit.
- Audit logs: $SPLUNK_HOME/var/log/splunk/soar_audit.log.
- Index creation and setup: $SPLUNK_HOME/var/log/splunk/soar_setup.log.