

Steps to update the drilldown link to open the related dashboard for detailed insights on data.

Dashboard: SIEM-Workflow-SecurityPosture

List of panels having different dashboard as its drilldown for detailed insights on data

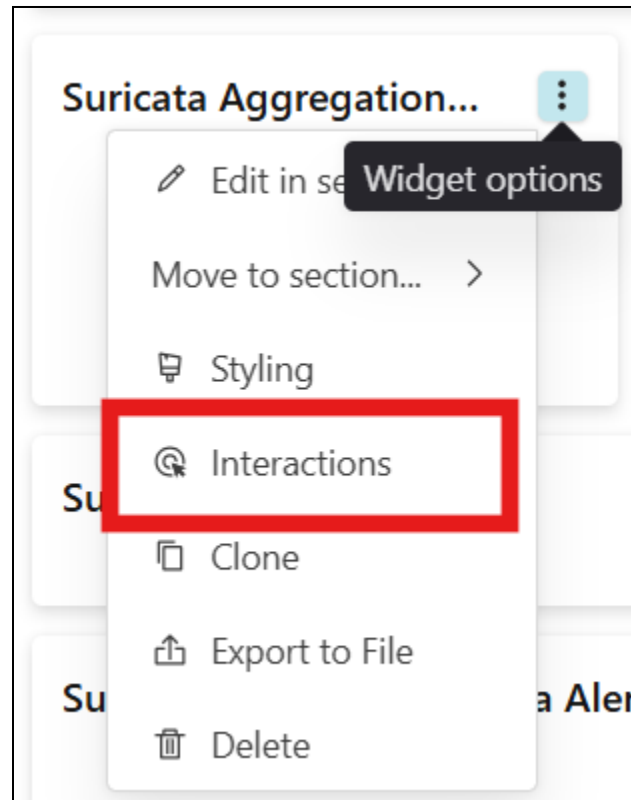
Panel name	Associated drilldown dashboard
Suricata Aggregations (From Suricata Alerts)	Security-CorelightAlertAggregations
Suricata Alerts (All Suricata Alerts)	Security-CorelightSuricata
Notices (Messages excluding Intel)	Security-CorelightNotice
Threat Intel (Intel Indicators)	Security-CorelightIntel

Steps:

1. Open the SIEM-Workflow-SecurityPosture dashboard.
2. Click on three dots on the top right corner of a panel as shown below in the image.



3. Click on the Interactions options from the options menu.



4. Navigate to the **"Behavior"** section within the toggle menu on the right side of the dashboard.

The screenshot shows the configuration interface for an 'Interactions' widget. The main title is 'Interactions'. Below it, there's a 'Widget' section with a blue header 'Details of Suricata Aggregations'. A toggle menu on the right side of the configuration panel has three items: a list icon, a monitor icon, and a circular arrow icon. The 'Behavior' section is highlighted with a red box. Below the 'Behavior' section, there's a 'Type' dropdown menu with 'Dashboard link' selected. Above the 'Behavior' section, there's a 'Display' section with a dropdown arrow. Under 'Display', there's a 'Name' field with the text 'Details of Suricata Aggregations', a 'Title template' field with an information icon and the text 'e.g. https://example.com/?q={{fields.myField}}', and a 'Type' dropdown menu with 'Dashboard link' selected.

Interactions

Widget

Details of Suricata Aggregations

^ v +

Display v

Name

Details of Suricata Aggregations

Title template ⓘ


e.g. https://example.com/?q={{fields.myField}}

Behavior v


Type

Dashboard link v


5. Search for the targeted dashboard in the "Target Dashboard" field using the name you entered while importing the dashboard.

Behavior 


Type

Dashboard link 

Target repository

Current repository (All) 

Target dashboard

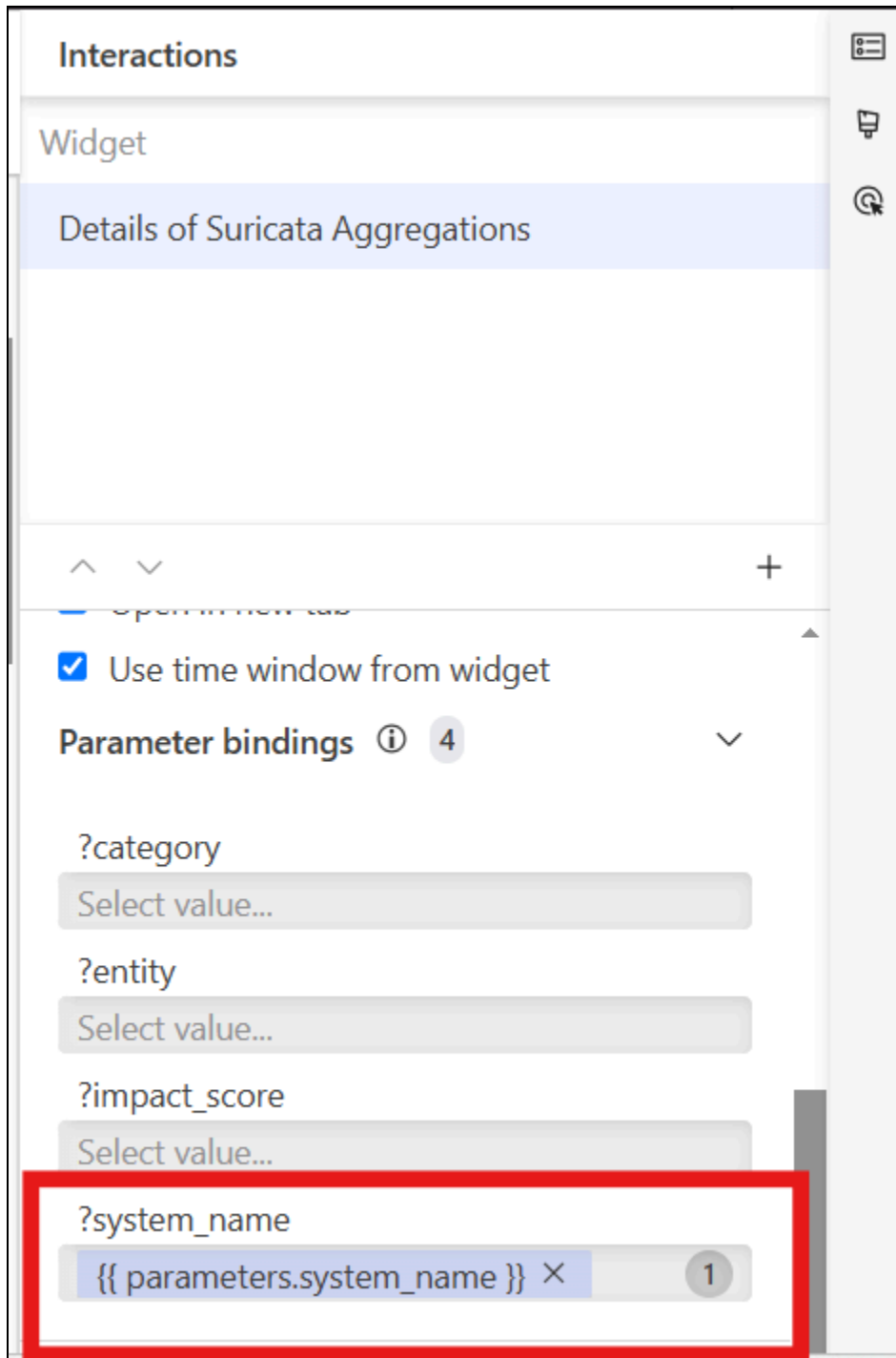
Security - Corelight Alert Aggregations 

General

Alert Aggregations

Corelight Investigator - Alerts

6. Bind the **?system_name** parameter to the **system_name** parameter of the current dashboard, as shown in the image. (Select the **system_name** parameter option from the given list.)



7. Click on Save button to save changes.

The screenshot shows a SIEM dashboard in an editing state. The top navigation bar includes 'Editing dashboard', 'SIEM - Workflow - Security Posture - Sections', and buttons for 'Discard changes' and 'Save'. The 'Save' button is highlighted with a red rectangle. The dashboard contains several widgets: a search bar with '[?system_name]' and an 'Apply' button; a row of five summary cards with values 0, 'Search completed. No results found.', 3, 4, and 3.52K; a 'Suricata Alerts' section with a card showing '36.29K' and a line chart titled 'Suricata Alerts (All Suricata Alerts) - Over Time'; and a bottom row of four cards for 'Unique Source IPs', 'Unique Destination IPs', 'Unique Signatures', and 'Internal Hosts Affect...'. On the right, a sidebar titled 'Interactions' shows a 'Widget' section with 'Details of Suricata Aggregations' and a 'Behavior' section with dropdowns for 'Type', 'Target repository', and 'Target dashboard'. The 'Target dashboard' dropdown is open, showing 'Security - Corelight Alert Aggregations' selected.

8. Repeat this process for every dashboard drilldown link changes.

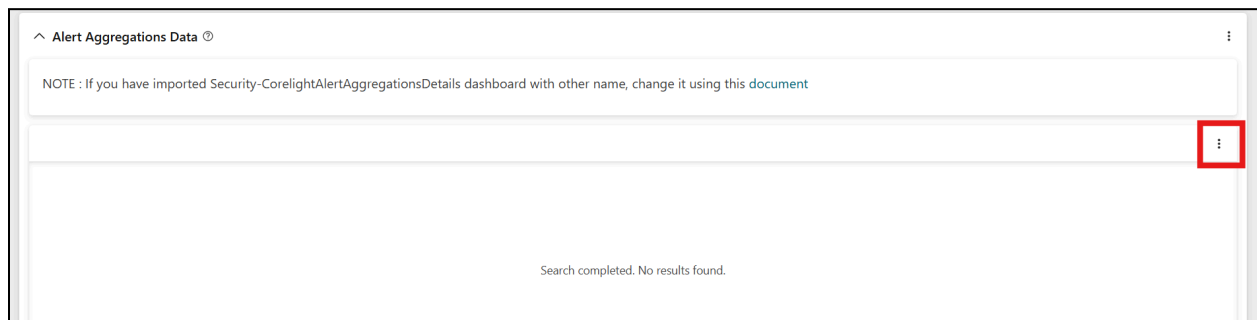
Dashboard: Security-CorelightAlertAggregations

List of panels having different dashboard as its drilldown for detailed insights on data

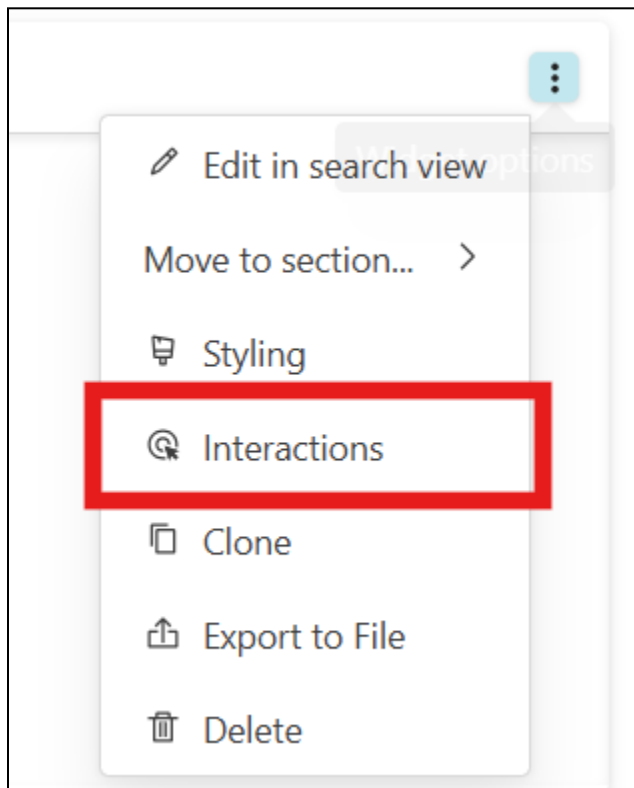
Panel name	Associated drilldown dashboard
Alert Aggregations Data	Security-CorelightAlertAggregationsDetails

Steps:

1. Open the Security-CorelightAlertAggregations dashboard.
2. Click on three dots on the top right corner of a panel as shown below in the image.



3. Click on the Interactions options from the options menu.



4. Navigate to the **"Behavior"** section within the toggle menu on the right side of the dashboard.

The image shows a configuration panel titled "Interactions". It contains a "Widget" section with a toggle menu on the right. The toggle menu has two options: "Details of Alert Aggregations Data" (which is currently selected and highlighted in light blue) and "Behavior" (which is highlighted with a red rectangular box). Below the "Behavior" option, there are configuration fields: "Name" (set to "Details of Alert Aggregations Data"), "Title template" (set to "Details of {{ fields['Aggregated SID(s)] }}"), and "Preview" (showing "Details of <no value>"). Below these, there is a "Type" dropdown menu (set to "Dashboard link") and a "Target repository" field.

Interactions

Widget

Details of Alert Aggregations Data

Display

Name

Details of Alert Aggregations Data

Title template ⓘ

Details of {{ fields["Aggregated SID(s)"] }}

Preview: Details of <no value>

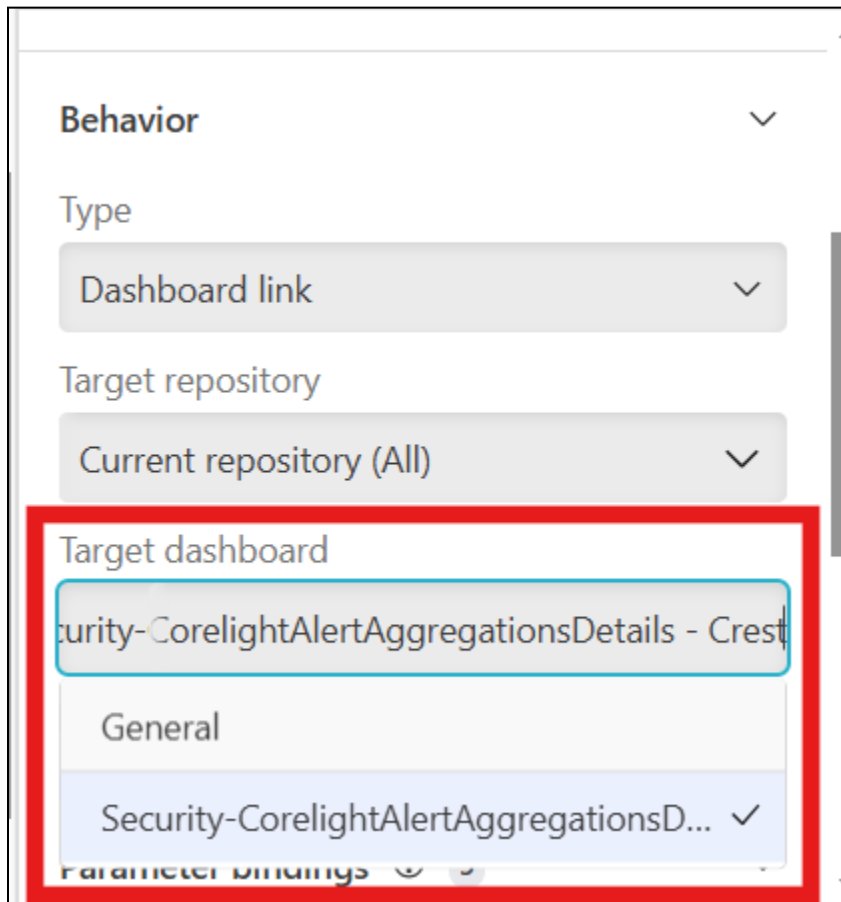
Behavior

Type

Dashboard link

Target repository

5. Search for the targeted dashboard in the "Target Dashboard" field using the name you entered while importing the dashboard.



The screenshot shows a configuration window with a 'Behavior' section. Under 'Type', 'Dashboard link' is selected. Under 'Target repository', 'Current repository (All)' is selected. The 'Target dashboard' dropdown is open, showing a search bar with the text 'Security-CorelightAlertAggregationsDetails - Crest'. Below the search bar, a list of options is shown, including 'General' and 'Security-CorelightAlertAggregationsD...'. The 'Security-CorelightAlertAggregationsD...' option is highlighted with a blue background and a checkmark. A red rectangle highlights the entire 'Target dashboard' section.

6. Bind the **?system_name** parameter to the **system_name** parameter of the current dashboard and the **?agg_id** parameter to the **Aggregated SID(s)** field from the table, as shown in the image. (Select the appropriate parameter option

from the given list.)

Parameter bindings ⓘ 5

?agg_id
{{ fields["Aggregated SID(s")] }}

?log_type
Select values...

?payload_uid
Select value...

?system_name
{{ parameters.system_name }} × 1

?uid
Select value...

7. Click on Save button to save changes.

Editing dashboard Security-CorelightAlertAggregations - [redacted] Discard changes Save

+ Add new ▾ Filters No filter ▾ Parameters Show queries +05:30 Calcutta Shared time < Last 1d ▾ > 🔍 Live

[[?system_name]] × 1 [[?entity]] * [[?impact_score]] * [[?category]] *

Apply ↻

Alert Aggregations Data ⓘ

Click the options menu of a widget to move it here or use the section settings.

[[No Title]] ⋮

[[No Title]] ⋮

Search completed. No results found.

Interactions

Widget

Details of Alert Aggregations Data

Use time window from widget

Parameter bindings ⓘ 5

?agg_id
{{ fields["Aggregated SID(s")] }}

?log_type
Select values...

?payload_uid
Select value...

?system_name
{{ parameters.system_name }} × 1

?uid
Select value...