

Splunk4Rookies - Dashboard Studio

Lab Guide

Overview

The purpose of this workshop is to introduce users to Dashboard Studio.

Prerequisites

To complete these exercises, you need your own Splunk instance. Splunk's hands-on workshops are delivered via the [Splunk Show portal](#), which you need a Splunk.com account to access.

If you don't have a Splunk.com account, create one [here](#) before proceeding with the workshop.

⚠ Troubleshooting Connectivity

If you experience connectivity issues with accessing your workshop environment or the event page, try the following troubleshooting steps. If you still experience issues, reach out to the team running your workshop.

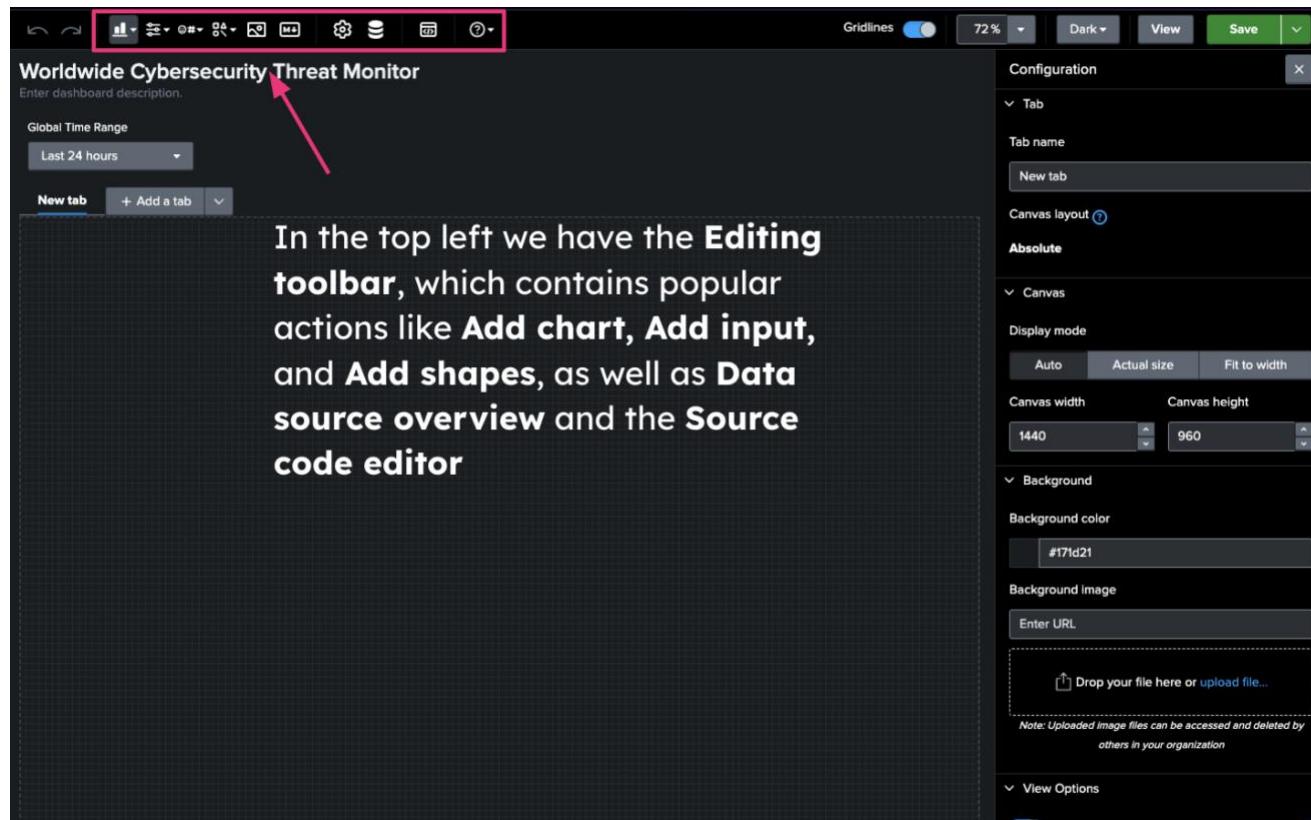
- **Use Google Chrome** (if you're not already).
- If the event page (the link provided by your workshop host) didn't load when you clicked on the link, try **refreshing the page**.
- **Disconnect from VPN** (if you're using one).
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data).
- **Try using private browsing mode** (e.g. incognito in Google Chrome) to rule out any cache issues.
- **Try using another computer** such as your personal computer. All you need is a web browser! Corporate laptops often block cloud platforms like AWS.

Table of Contents

Table of Contents	2
Editor Tour.....	4
Exercise 1 – Create a New Dashboard	6
Exercise 2 – Add a Table.....	8
Add the visualization.....	8
Adjust the Global time range picker	8
Configure the visualization	10
Exercise 3 - Filtering with Tokens.....	12
Add the input.....	12
Use the token.....	13
[OPTIONAL] Add a reset button.....	13
Exercise 4 - Add a New tab.....	16
Set up the canvas.....	16
Add the background	17
Exercise 5 – Create a Single Value Visualization.....	20
Add the visualization.....	20
Configure the visualization	21
Exercise 6 - Add a Timeline	22
Add the visualization.....	22
Configure the visualization	23
Exercise 7 - Add a Sunburst Visualization	25
Add the visualization.....	25
Configure the visualization	26
Exercise 8 - Map + Dynamic Coloring.....	27
Add the visualization.....	27
Configure the visualization	29
Exercise 9 - Interact with Tokens.....	32
Map interactivity.....	32
[OPTIONAL] Token reset	33
[OPTIONAL] Interaction verification	34

Exercise 10 - Conditional Visible Tables.....	35
Add the visualization.....	35
Configure the visualization	36
Exercise 11 - (OPTIONAL) Improve Dashboard Styling	39
Panel transparency.....	39
Completed Dashboard.....	40
Appendix.....	41
Adding a global time range picker.....	41
Searches used.....	43

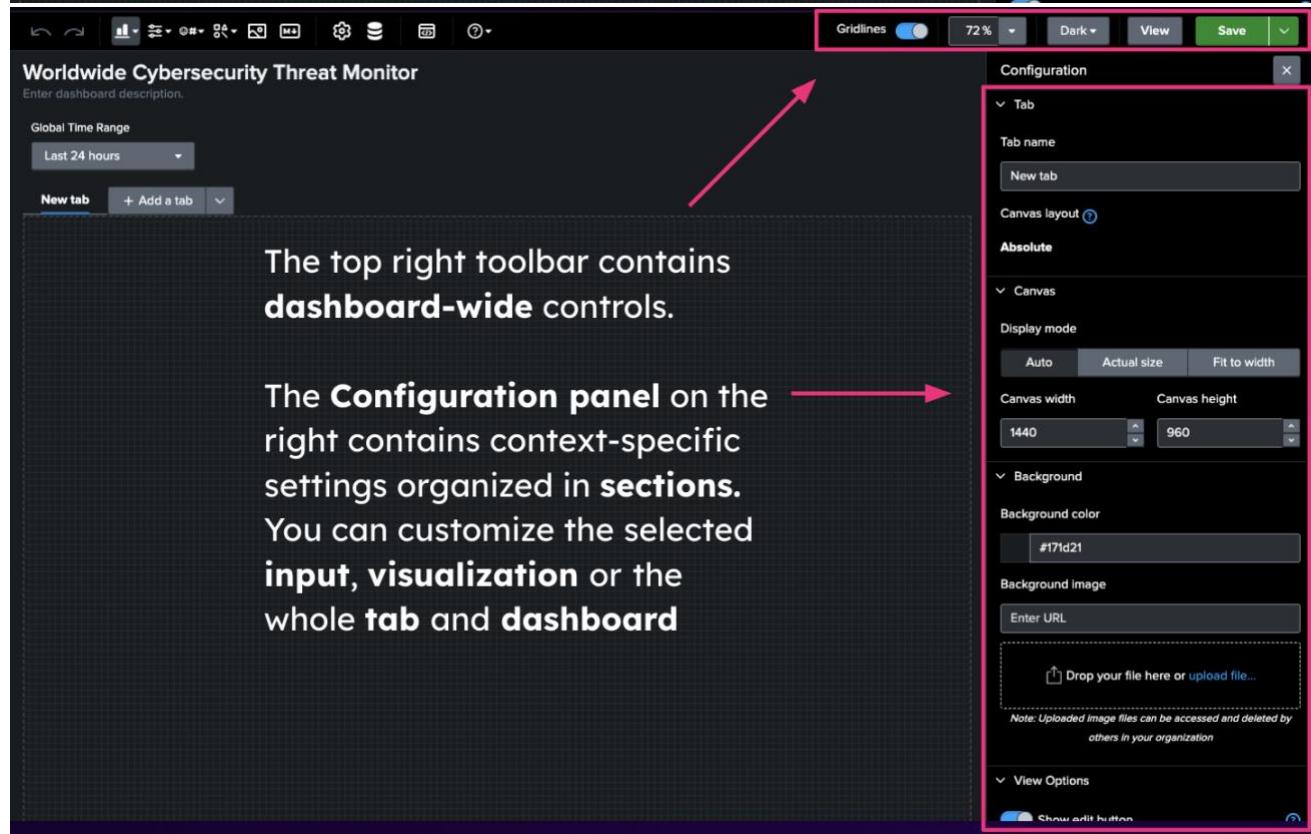
Editor Tour



In the top left we have the **Editing toolbar**, which contains popular actions like **Add chart**, **Add input**, and **Add shapes**, as well as **Data source overview** and the **Source code editor**

Configuration

- Tab**
 - Tab name: New tab
- Canvas**
 - Display mode**: Auto, Actual size, Fit to width
 - Canvas width**: 1440, **Canvas height**: 960
- Background**
 - Background color**: #171d21
 - Background image**: Enter URL, Drop your file here or upload file...
- View Options**

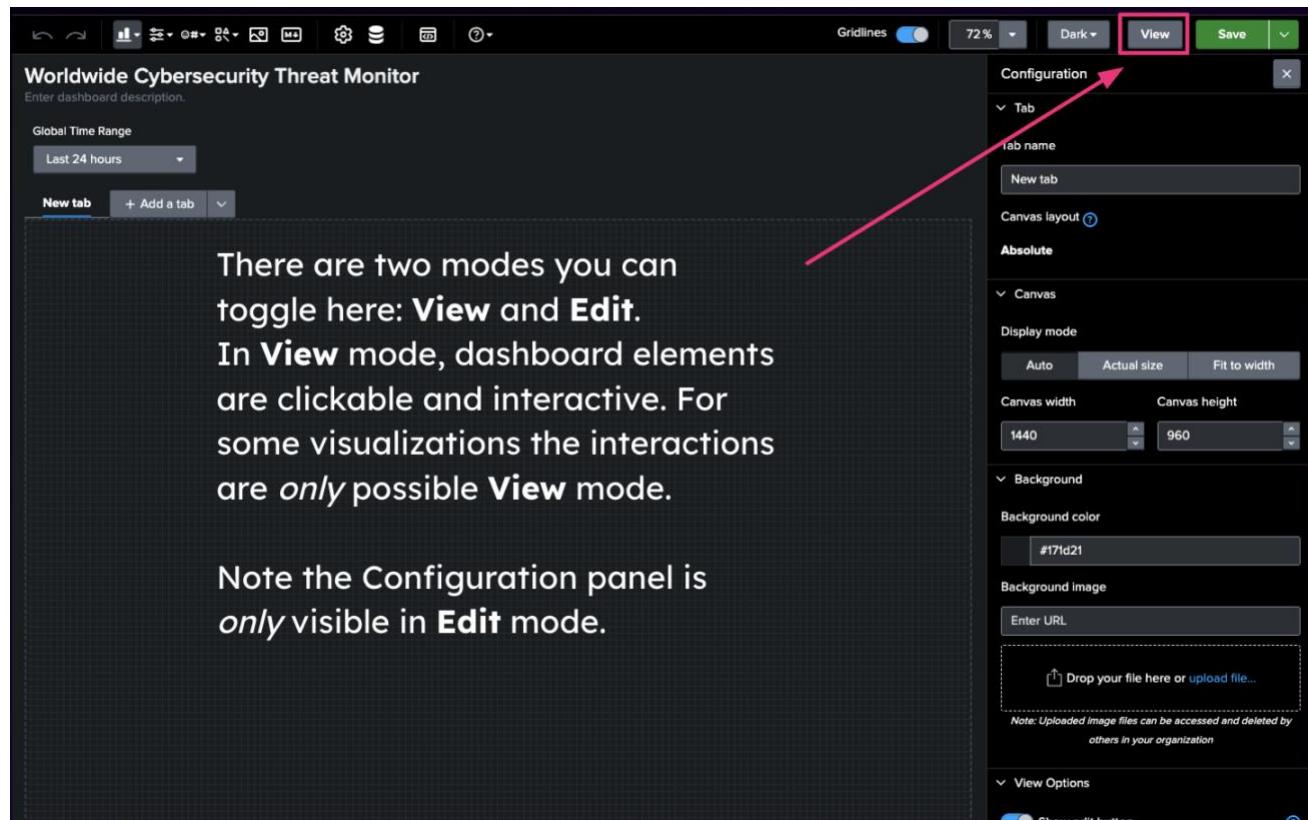


The top right toolbar contains **dashboard-wide controls**.

The **Configuration panel** on the right contains context-specific settings organized in **sections**. You can customize the selected **input**, **visualization** or the whole **tab** and **dashboard**

Configuration

- Tab**
 - Tab name: New tab
- Canvas**
 - Display mode**: Auto, Actual size, Fit to width
 - Canvas width**: 1440, **Canvas height**: 960
- Background**
 - Background color**: #171d21
 - Background image**: Enter URL, Drop your file here or upload file...
- View Options**



Worldwide Cybersecurity Threat Monitor

Enter dashboard description.

Global Time Range

Last 24 hours

New tab + Add a tab

There are two modes you can toggle here: **View** and **Edit**. In **View** mode, dashboard elements are clickable and interactive. For some visualizations the interactions are *only* possible **View** mode.

Note the Configuration panel is *only* visible in **Edit** mode.

Configuration

Tab

Tab name

New tab

Canvas layout

Absolute

Canvas

Display mode

Auto Actual size Fit to width

Canvas width 1440 Canvas height 960

Background

Background color #171d21

Background image Enter URL

Drop your file here or upload file...

Note: Uploaded image files can be accessed and deleted by others in your organization

Show edit button

Exercise 1 – Create a New Dashboard

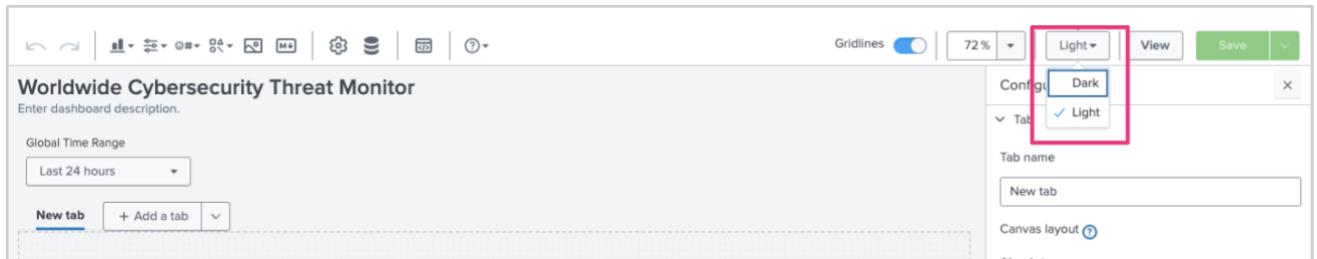
1. Navigate to the **Search & Reporting** app and click on the **Dashboards** tab in the menu bar. Click on the **Create New Dashboard** button.

The screenshot shows the Splunk interface with a dark grey header. In the top right, there's a user icon (Administrator) and several dropdown menus: Apps, Messages, Settings, Activity, Help, and a search bar labeled 'Find'. Below the header, the main navigation bar has tabs: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Dashboards' tab is highlighted with a red box. To the right of the tabs is a green search icon with the text 'Search & Reporting'. Below the navigation bar, a section titled 'Dashboards' is displayed. It contains a brief description: 'Dashboards include searches, visualizations, and input controls that capture and present available data.' and a link to 'Latest Resources'. On the far right of this section is a green button with white text that says 'Create New Dashboard', also highlighted with a red box.

2. Title your dashboard ***Worldwide Cybersecurity Threat Monitor <your name>***
3. Select the **Dashboard Studio** option to build your dashboard.
4. Select the **Absolute** layout.
5. Click on **Create**.

The screenshot shows the 'Create New Dashboard' dialog box. At the top left is the title 'Create New Dashboard' and a close 'X' button at the top right. Below that is a 'Dashboard Title' field containing 'Worldwide Cybersecurity Threat Monitor' with a small 'Edit ID' link next to it. Underneath is a 'Description' field with the placeholder 'Optional'. A 'Permissions' dropdown is set to 'Private'. At the bottom of this section is a 'Dashboard type' label with a question mark icon, followed by two options: 'Classic Dashboards' (described as 'The traditional Splunk dashboard builder') and 'Dashboard Studio' (described as 'A new builder to create visually-rich, customizable dashboards'). The 'Dashboard Studio' option is highlighted with a blue border. Below these is a 'Select layout mode' label. Two options are shown: 'Absolute' (described as 'Full layout control') and 'Grid' (described as 'Quick organization'). The 'Absolute' option is highlighted with a blue border. At the bottom right of the dialog are 'Cancel' and 'Create' buttons, with 'Create' being a green button.

6. Using the dropdown on the right side of the editor toolbar, it should be set to **Light** by default, change the mode to **Dark**.



Exercise 2 – Add a Table

Add the visualization

1. Select Table from the Visualization dropdown in the menu bar.

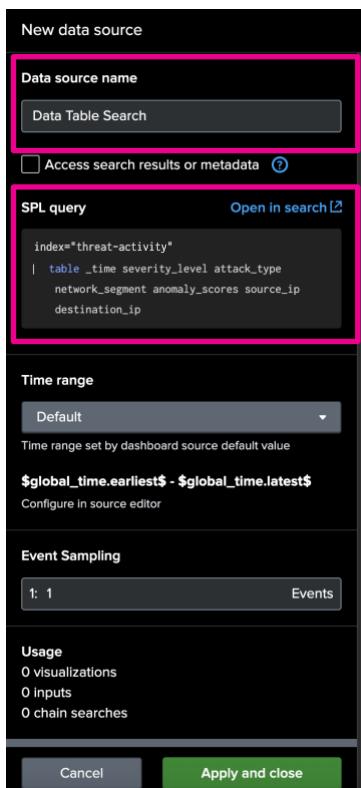


In the **Select data source** panel, select **Search > + Create search**.

2. Set the **Data source name** to “Data Table Search” and input the following search into the **SPL query** input field:

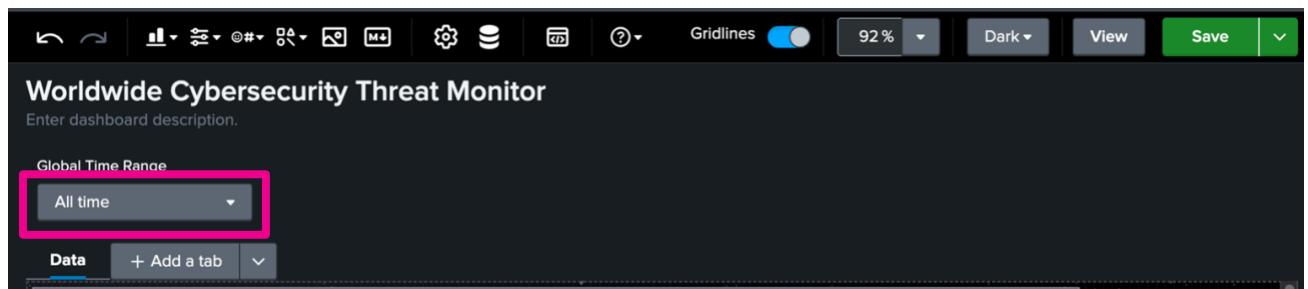
```
index="threat-activity"
| table _time severity_level attack_type network_segment anomaly_scores
source_ip destination_ip
```

3. Click on **Apply and close** at the bottom of the panel.

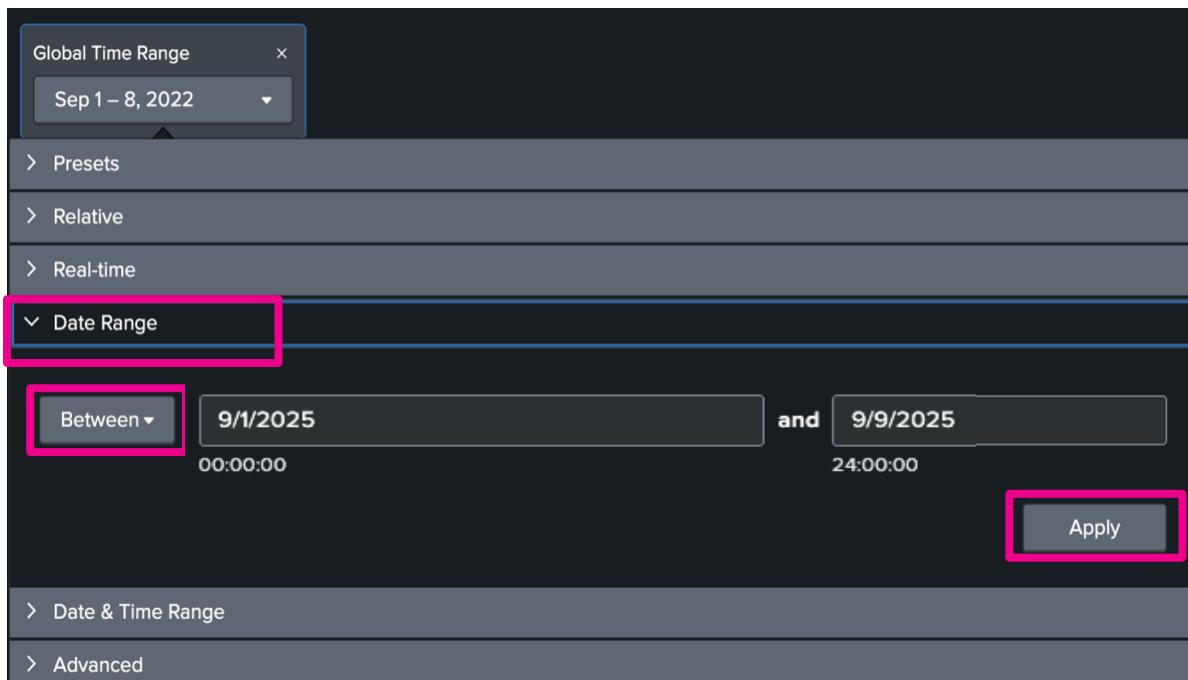


Adjust the Global time range picker

4. Click on the Global Time Range picker dropdown.

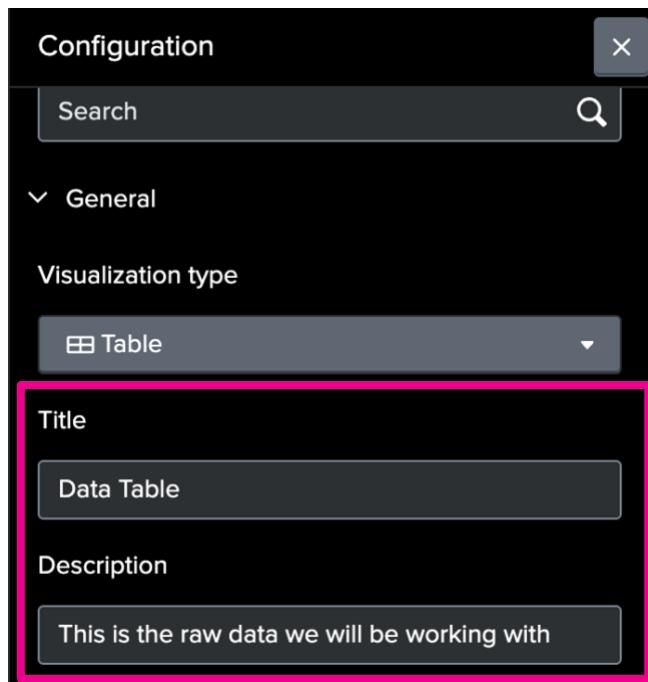


5. In the popup, select **Date Range** and then set the range option to **Between**.
6. Enter **9/1/2025** and **9/9/2025** as our date range.
7. Make sure to click **Apply** to confirm your changes to the **Global Time Range**.



Configure the visualization

8. Click on the table you just added and in the Configuration panel, under **General > Title**, input “Data Table”, and under **General > Description**, input “This is the raw data”



9. Move and resize your table to fill the canvas.

At this point in the workshop, the dashboard looks like this:

Worldwide Cybersecurity Threat Monitor

Enter dashboard description.

Global Time Range

Sep 1 – 8, 2025 ▾

Data + Add a tab ▾

Data Table

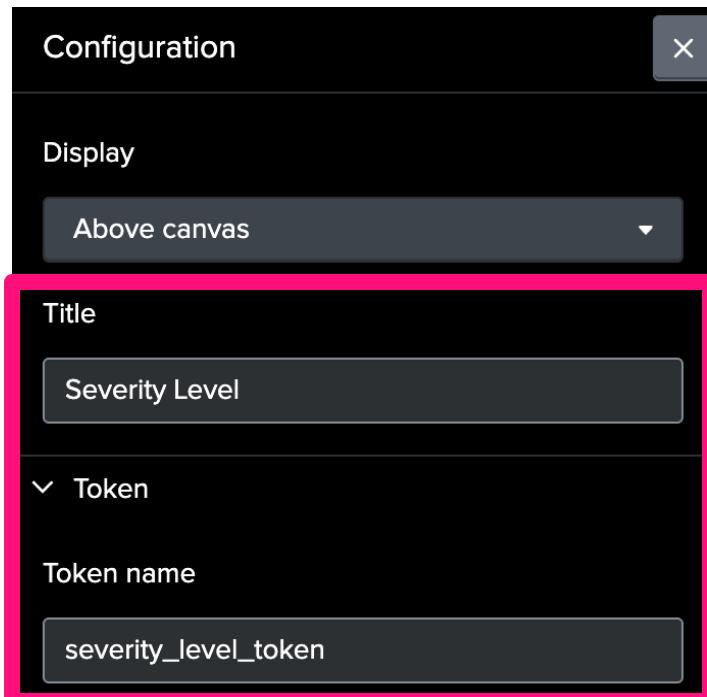
_time	severity_level	attack_type	network_seg...	anomaly_scores	source_ip	destination_ip
2025-09-05T11:37:08.000+00:00	Medium	Malware	Segment B	49.98	74.31.107.127	24.66.36.231
2025-09-05T11:30:46.000+00:00	High	Malware	Segment B	40.34	64.148.222.211	110.98.7.241
2025-09-05T11:06:51.000+00:00	High	Intrusion	Segment B	31.46	218.82.40.187	109.221.80.195
2025-09-05T10:31:29.000+00:00	Low	Malware	Segment A	47.67	201.132.87.40	31.44.56.175
2025-09-05T09:56:34.000+00:00	Medium	Intrusion	Segment B	61.05	195.105.112.38	142.111.30.247
2025-09-05T09:17:50.000+00:00	High	Intrusion	Segment A	40.23	35.9.31.88	220.231.72.143
2025-09-05T09:11:01.000+00:00	High	Intrusion	Segment A	63.22	139.167.106.121	23.117.180.121
2025-09-05T08:57:39.000+00:00	Medium	Malware	Segment A	53.02	85.77.251.155	7.25.121.9
2025-09-05T04:44:19.000+00:00	Medium	DDoS	Segment B	86.81	10.206.35.159	85.100.100.195

< Prev 1 2 3 4 5 ... Next >

Exercise 3 - Filtering with Tokens

Add the input

1. Click on the Inputs icon (⚙️) in the editing toolbar, and then select **Dropdown**.
2. In the **Configuration** panel, set the **Title** to *Severity Level*, and the **Token name** to *severity_level_token*.



3. Go to the **Static menu configuration** section and enter the following options (click on **+ Add new** to add another row):

Static menu configuration

Label	Value
All	*
High	High
Medium	Medium
Low	Low

+ Add new

- In the Default selected values section, select First value.

Default selected values

Choose default First value None

Assigns the first value returned from the data source as the default

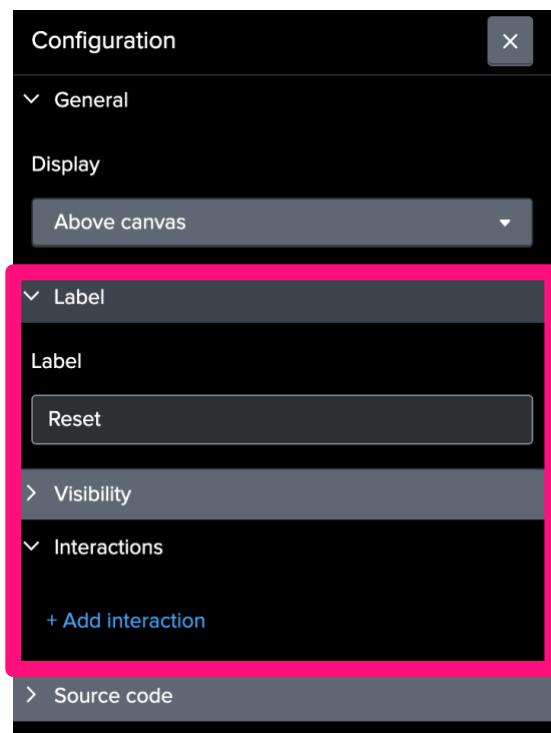
Use the token

- From the editor toolbar, click () to open the Data source overview panel.
- Click the pencil icon (), next to “Data Table”, to open its associated Edit data source panel. Change the SPL query to make sure there are quotes “ ” around \$severity_level_token\$:

```
index="threat-activity" severity_level = "$severity_level_token$"
| table _time severity_level attack_type network_segment anomaly_scores
source_ip destination_ip
```

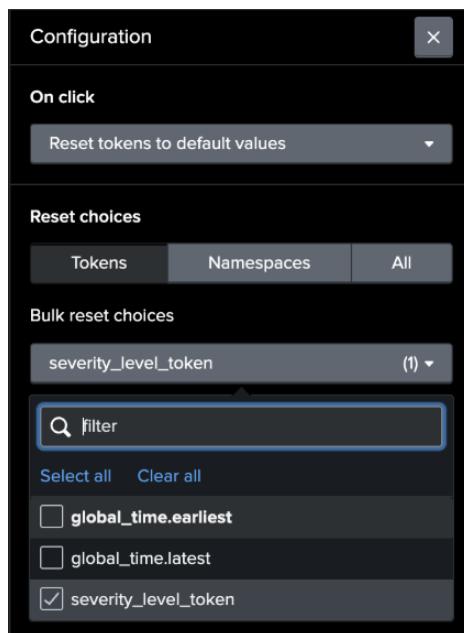
[OPTIONAL] Add a reset button

- In the editor toolbar, select the Inputs dropdown (), then select the Button element.
- In the button's Configuration panel, set the Label to “Reset”.
- Under Interactions, click on + Add interaction.

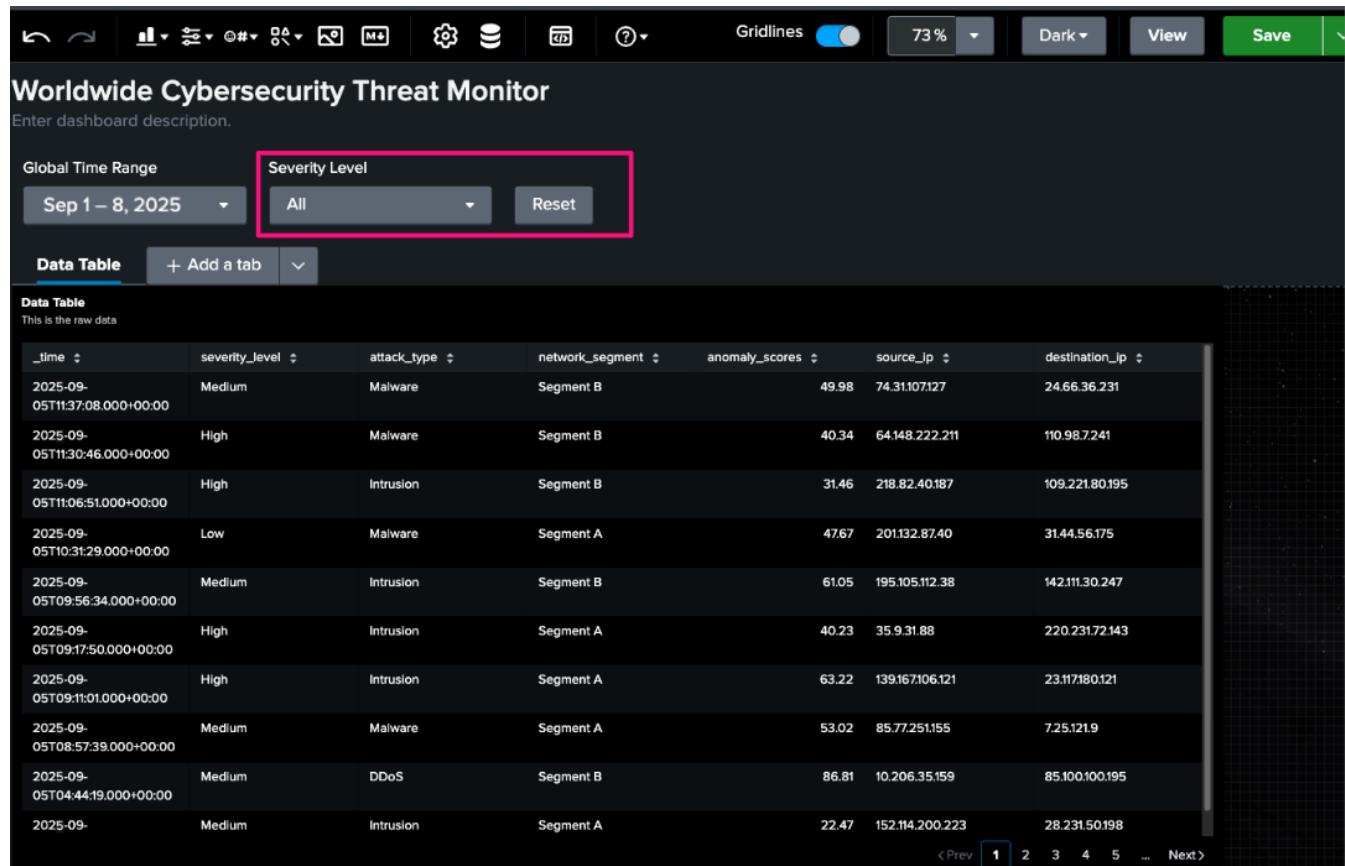


10. In the interaction's Configuration panel, under **On click** select **Reset tokens to default values**.

11. Under **Reset choices**, select **Tokens**, and under **Bulk reset choices**, select **severity_level_token**.



Your dashboard should now have a dropdown to set a filter by severity level and maybe a Reset button.



_time	severity_level	attack_type	network_segment	anomaly_scores	source_ip	destination_ip
2025-09-05T11:37:08.000+00:00	Medium	Malware	Segment B	49.98	74.31.071.27	24.66.36.231
2025-09-05T11:30:46.000+00:00	High	Malware	Segment B	40.34	64.148.222.211	110.98.7.241
2025-09-05T11:06:51.000+00:00	High	Intrusion	Segment B	31.46	218.82.40.187	109.221.80.195
2025-09-05T10:31:29.000+00:00	Low	Malware	Segment A	47.67	201.132.87.40	31.44.56.175
2025-09-05T09:56:34.000+00:00	Medium	Intrusion	Segment B	61.05	195.105.112.38	142.111.30.247
2025-09-05T09:17:50.000+00:00	High	Intrusion	Segment A	40.23	35.9.31.88	220.231.72.143
2025-09-05T09:11:01.000+00:00	High	Intrusion	Segment A	63.22	139.167.106.121	23.117.180.121
2025-09-05T08:57:39.000+00:00	Medium	Malware	Segment A	53.02	85.77.251.155	7.25.121.9
2025-09-05T04:44:19.000+00:00	Medium	DDoS	Segment B	86.81	10.206.35.159	85.100.100.195
2025-09-	Medium	Intrusion	Segment A	22.47	152.114.200.223	28.231.50.198

Exercise 4 - Add a New tab

Set up the canvas

1. In the tab menu, just above the canvas, select **+ Add a tab**.

The screenshot shows the Splunk interface with the title "Worldwide Cybersecurity Threat Monitor". Below the title is a placeholder "Enter dashboard description.". Underneath are two dropdown menus: "Global Time Range" set to "Sep 1 – 8, 2025" and "Severity Level" set to "All". The main area is titled "Data Table" and contains a single row of data:

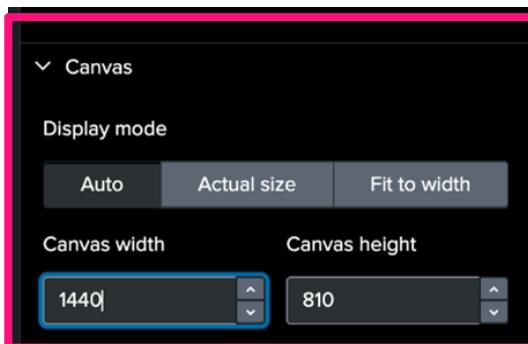
_time	severity_level	attack_type
2022-09-05T11:37:08.000+00:00	Medium	Malware

2. In the **Configuration** panel, set the **Tab name** to “Dashboard”.
3. Under **Canvas layout**, click **Change**. In the pop-up that opens, change the selection to **Absolute** and click **Change** to lock in your changes.

The dialog box has a title "Change tab's canvas layout". It contains a warning message: "⚠ Only Grid layouts can change to a different layout type. After a layout is modified to Absolute or Custom, the layout cannot change type again." Below the message are two radio buttons:
 Absolute - Pixel level control
 Grid - Quick organization

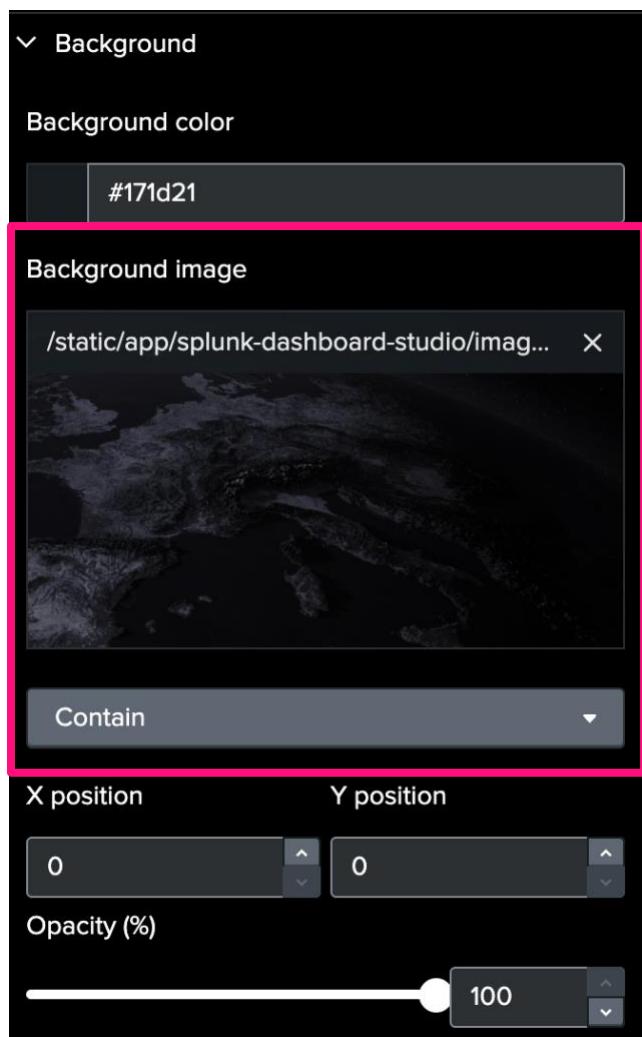
4. With the new tab’s **Configuration** panel still open, if it isn’t click on , make sure the **Display mode** is set to **Auto**.

5. Change **Canvas Width** to “1440” and **Canvas Height** to “810”.



Add the background

6. In the **Configuration** panel, find the **Background Image** section and paste the following image URL into the **Enter URL** input: /static/app/splunk-dashboard-studio/images/examples-hub/europe_network_hub/europe_network_hub_background_image.jpg
7. In the dropdown below the preview image, it will default to **Contain**, select **Cover**.



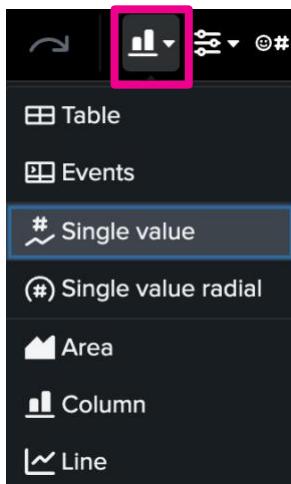
Your dashboard should now have a new tab with the background image.

The screenshot shows the Splunk interface for a "Worldwide Cybersecurity Threat Monitor". The top navigation bar includes standard browser controls (back, forward, search), a gear icon, and a "Save" button. Below the header, there's a search bar with placeholder text "Enter dashboard description." and filter sections for "Global Time Range" (set to "Sep 1 – 8, 2025") and "Severity Level" (set to "All"). A "Reset" button is also present. The main area features a large, dark map of the world with various threat indicators. At the bottom left, there are tabs for "Data" and "Dashboard", with "Dashboard" being the active tab and highlighted by a pink rectangle. A "More" button (three dots) is located next to the dashboard tab. Below the tabs is a button labeled "+ Add a tab".

Exercise 5 – Create a Single Value Visualization

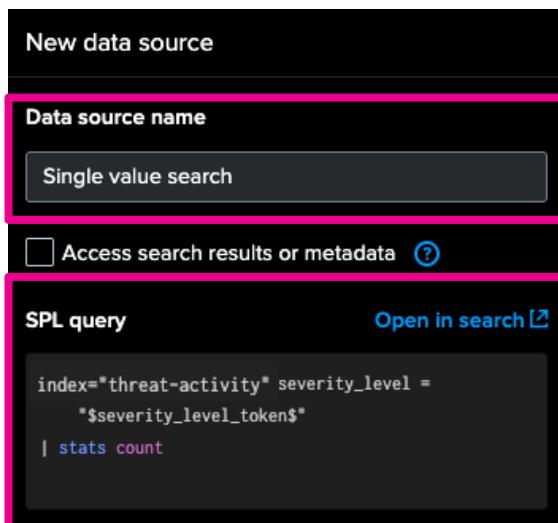
Add the visualization

1. Select **Single value** from the **Visualization** dropdown in the toolbar



2. In the **Select data source** panel, select **Search > + Create search**.
3. Set the **Data source name** to “Single value search” and input the following search into the **SPL query** input field:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| stats count
```

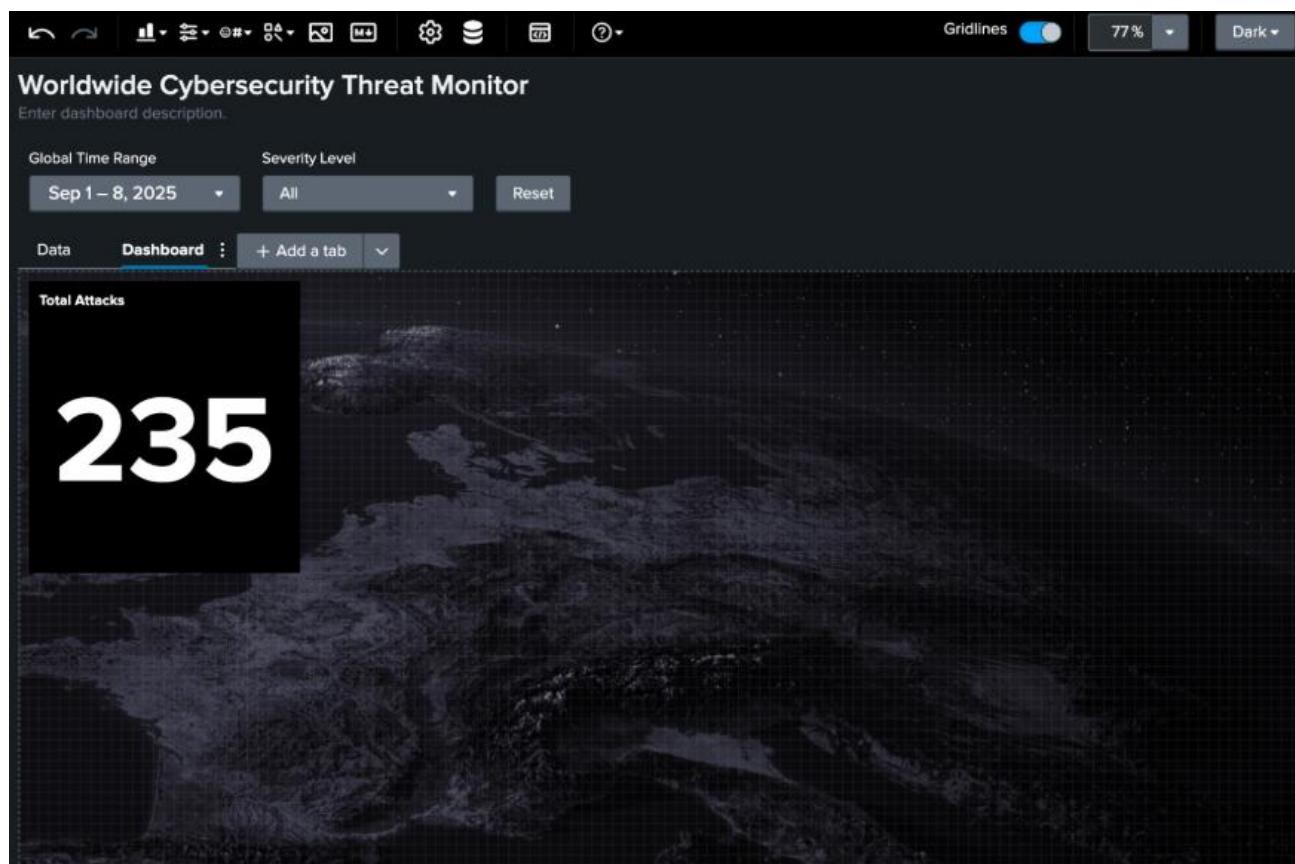


4. Click on **Apply and close** at the bottom of the panel.

Configure the visualization

5. In the single value visualization's **Configuration** panel, input "Total Attacks" as the **Title**.
6. Move and resize the visualization so it is in the top, left corner and covers about $\frac{1}{4}$ of the width of the dashboard.

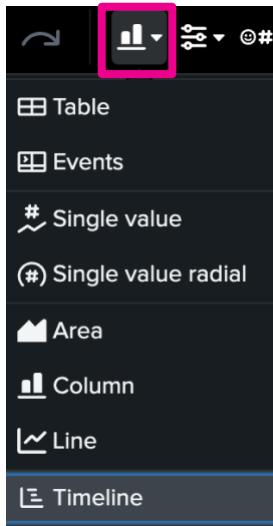
Your dashboard should now have a single value visualization! Make sure you save the dashboard.



Exercise 6 - Add a Timeline

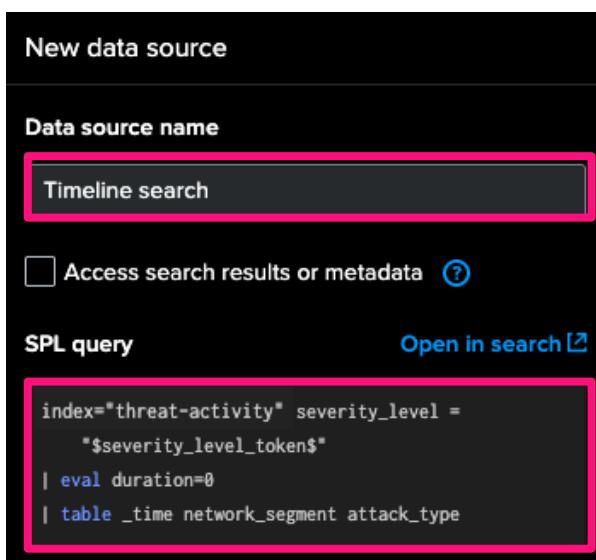
Add the visualization

1. Select **Timeline** from the **Visualization** dropdown in the toolbar.



2. In the **Select data source** panel, select **Search > + Create search**.
3. Set the **Data source name** to “Timeline search” and input the following search into the **SPL query** input field:

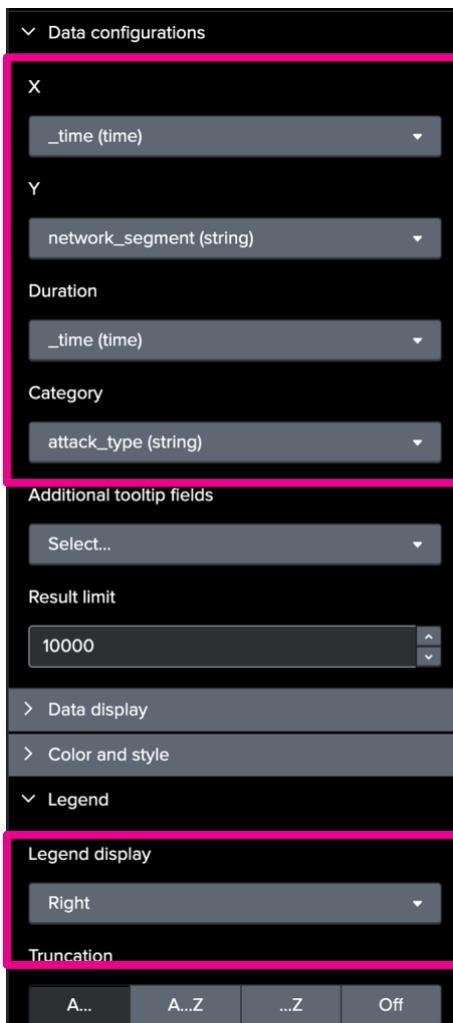
```
index="threat-activity" severity_level = "$severity_level_token$"  
| eval duration=0  
| table _time network_segment attack_type
```



4. Click on **Apply and close** at the bottom of the panel.

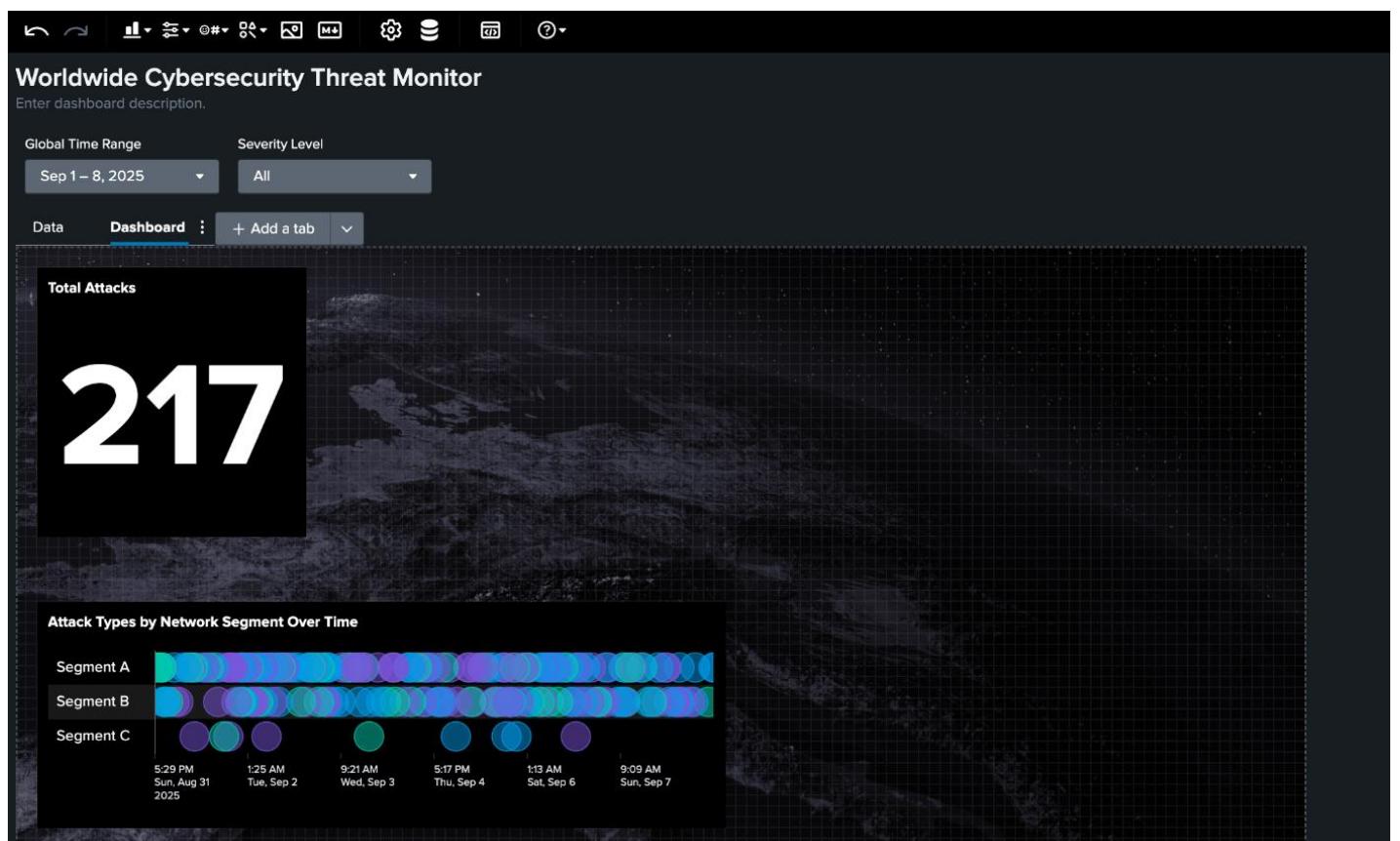
Configure the visualization

5. In the Timeline's Configuration panel, input "Attack Types by Network Segment Over Time" as the **Title**.
6. Under **Data configurations**, set the following settings:
 - a. Under **X** select `_time`.
 - b. Under **Y** select `network_segment`.
 - c. Under **Duration** select `_time`.
 - d. Under **Category** select `attack_type`.
7. Under **Legend display** select **Right**.



8. Move and resize the visualization. It should be below the single value visualization and fill about half of the dashboard.

Your dashboard should now have a timeline visualization! Make sure you save the dashboard.



Exercise 7 - Add a Sunburst Visualization

Add the visualization

1. Select **Sunburst** from the **Visualization** dropdown in the toolbar. It should be at the bottom.
2. In the **Select data source** panel, select **Search > + Create search**.
3. Set the **Data source name** to “Sunburst search” and input the following search into the **SPL query** input field:

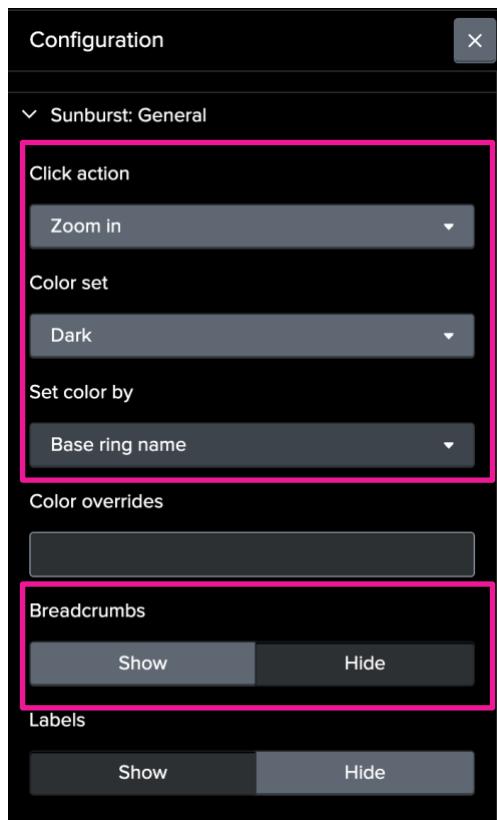
```
index="threat-activity"
severity_level = "$severity_level_token$"
| iplocation source_ip allfields=true
| stats count by attack_type, Continent, Country
```

The screenshot shows the 'Edit data source' interface. At the top, there's a header bar with the title 'Edit data source'. Below it, a section for 'Data source name' has a text input field containing 'Sunburst search'. There's also a checkbox labeled 'Access search results or metadata' with a help icon. The main body of the panel is titled 'SPL query' and contains the SPL search command provided in the text block above. At the bottom, there's a 'Time range' section with a dropdown set to 'Default' and a note about it being the dashboard source default value. A specific time range '\$global_time.earliest\$ - \$global_time.latest\$' is also listed, along with a link to 'Configure in source editor'.

4. Click on **Apply and close** at the bottom of the panel.

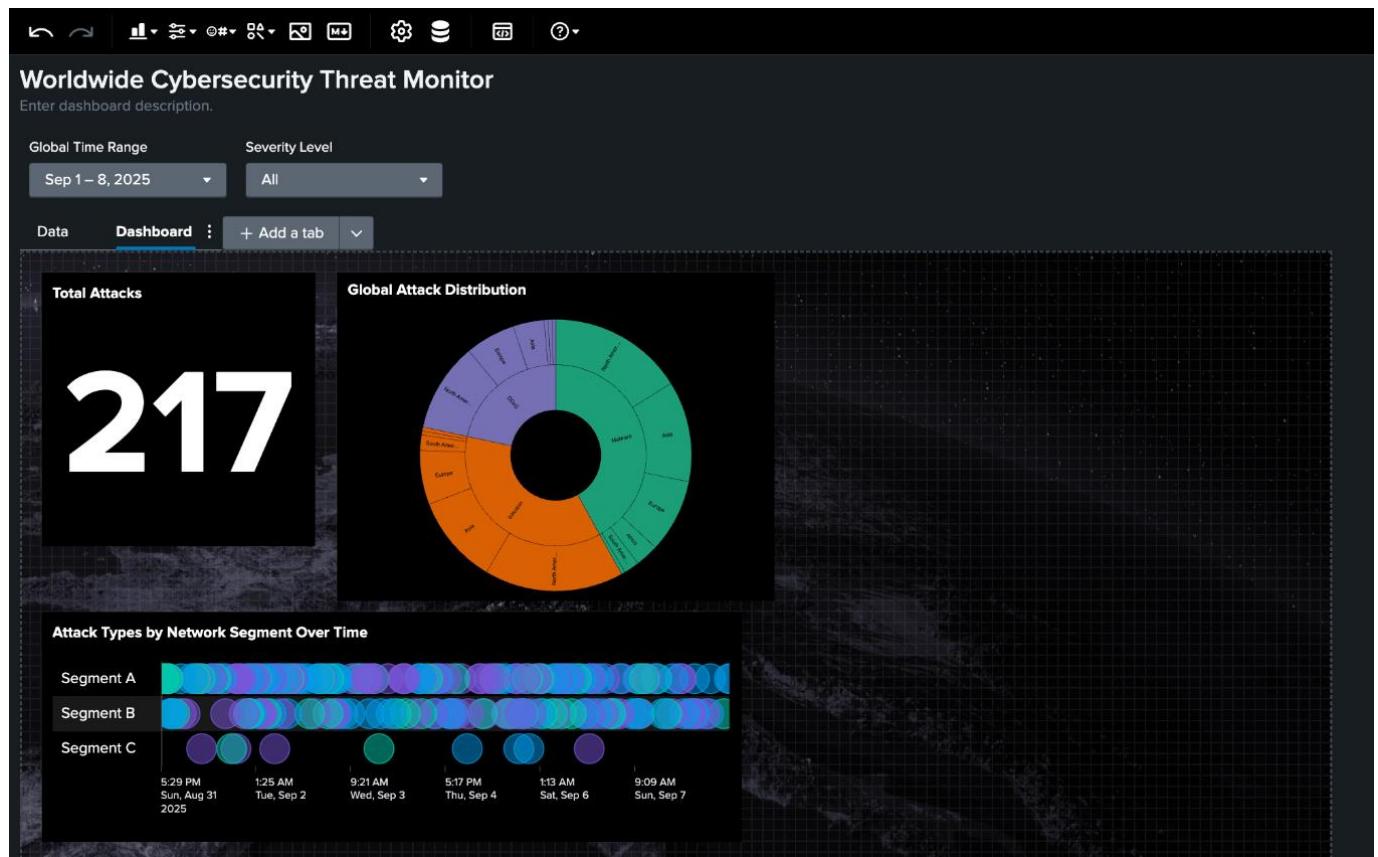
Configure the visualization

5. In the Sunburst's Configuration panel, input "Global Attack Distribution" as the **Title**.
6. Still in the **Configuration** panel, find the **Sunburst: General** section. In that section, set the following settings:
 - a. Under **Click action** select **Zoom in**.
 - b. Under **Color set** select **Dark**.
 - c. Under **Set color by** select **Base ring name**.
 - d. Under **Breadcrumbs** select **Hide**.



7. Move and resize the visualization. It should be next to the single value visualization and leave about half of the dashboard on its right side.

Your dashboard now has an interactive sunburst chart!



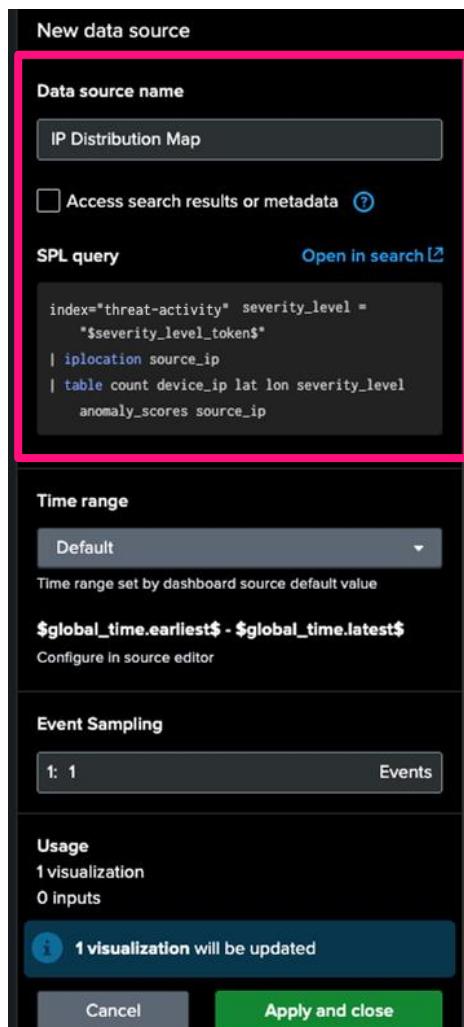
Exercise 8 - Map + Dynamic Coloring

Add the visualization

1. Select **Map** from the **Visualization** dropdown in the toolbar.
2. In the **Select data source** panel, select **Search > + Create search**.

3. Set the **Data source name** to “Map search” and input the following search into the **SPL query** input field:

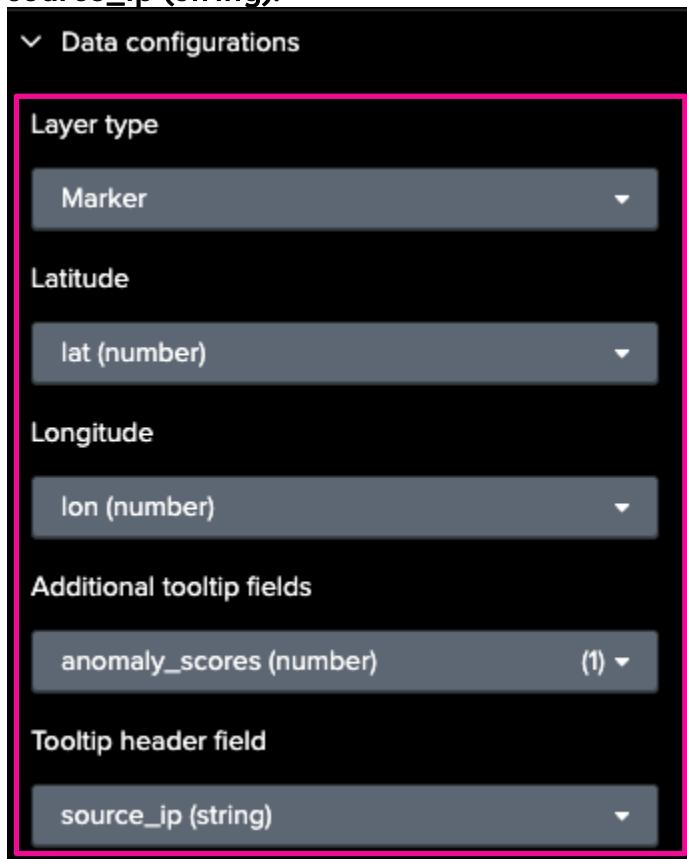
```
index="threat-activity" severity_level = "$severity_level_token$"  
| iplocation source_ip  
| table count device_ip lat lon severity_level anomaly_scores source_ip
```



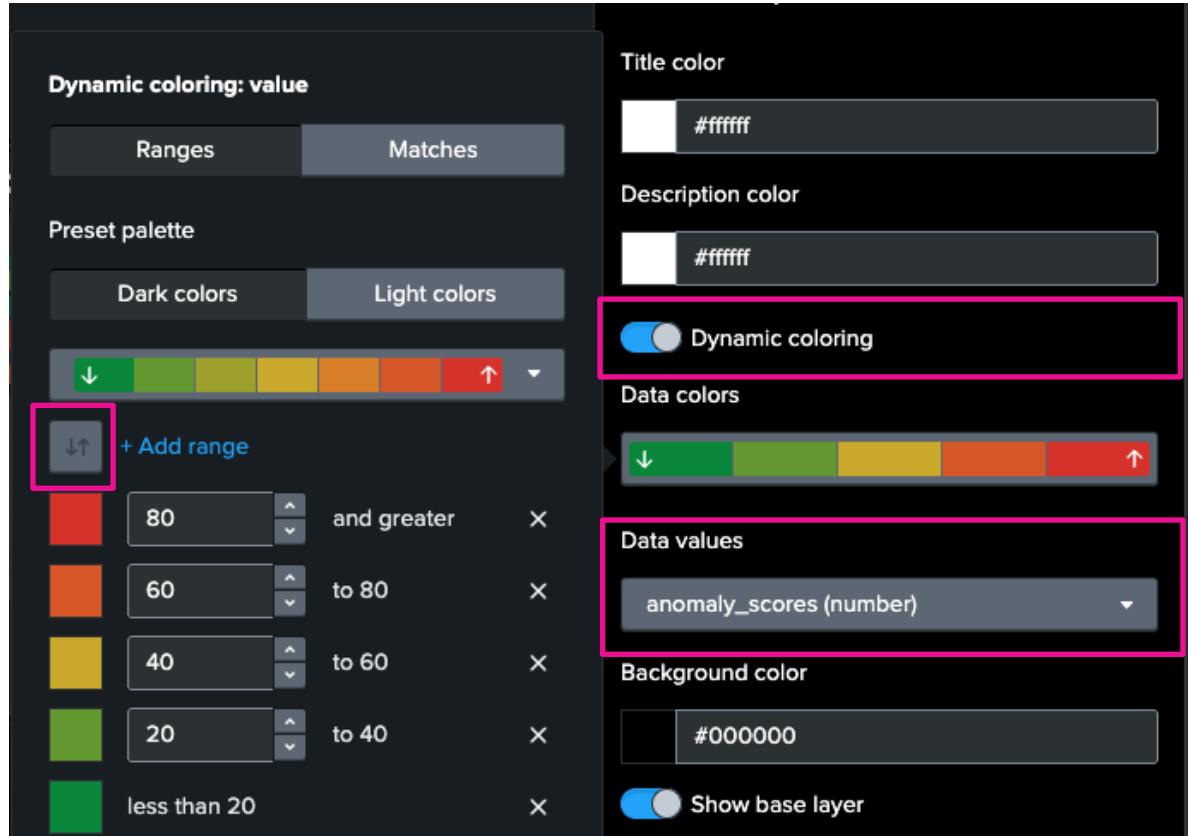
4. Click on **Apply and close** at the bottom of the panel.

Configure the visualization

5. In the Map's Configuration panel, find the **Data configurations** section and set the following:
 - a. For **Layer type** select **Marker**.
 - b. For **Latitude** select **lat (number)**.
 - c. For **Longitude** select **lon (number)**.
 - d. For **Additional tooltip fields** select **anomaly_scores (number)**.
 - e. For **Tooltip header field** select **source_ip (string)**.

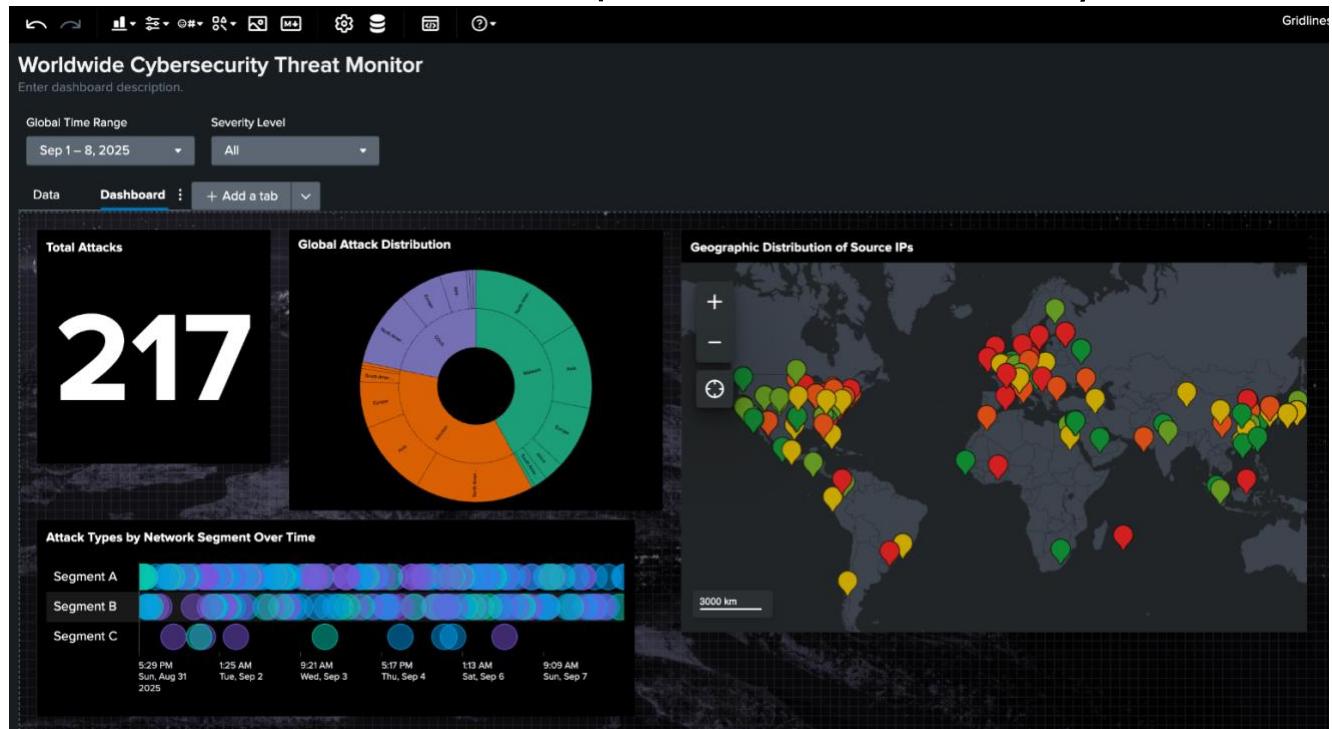


6. Still in the Map's Configuration panel, find the **Color and style** section and set the following:
 - a. Toggle on **Dynamic coloring**.
 - b. Click on **Data colors**, and switch the direction of the color palette by clicking on this icon (↓↑).
 - c. Under **Data values**, select **anomaly_scores (number)**.



7. In the **General** section, set the **Title** to “Geographic Distribution of Source IPs”.
8. Move and resize the visualization. It should be in the top right of the dashboard and cover about half of the width of the dashboard.

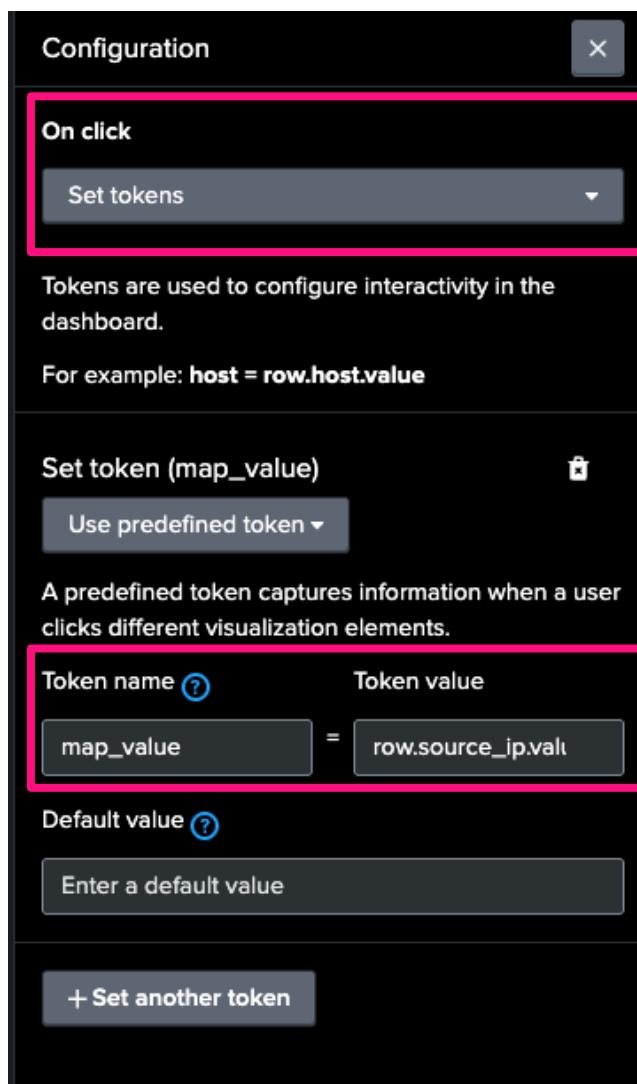
Your dashboard should now have a map visualization with a marker layer.



Exercise 9 - Interact with Tokens

Map interactivity

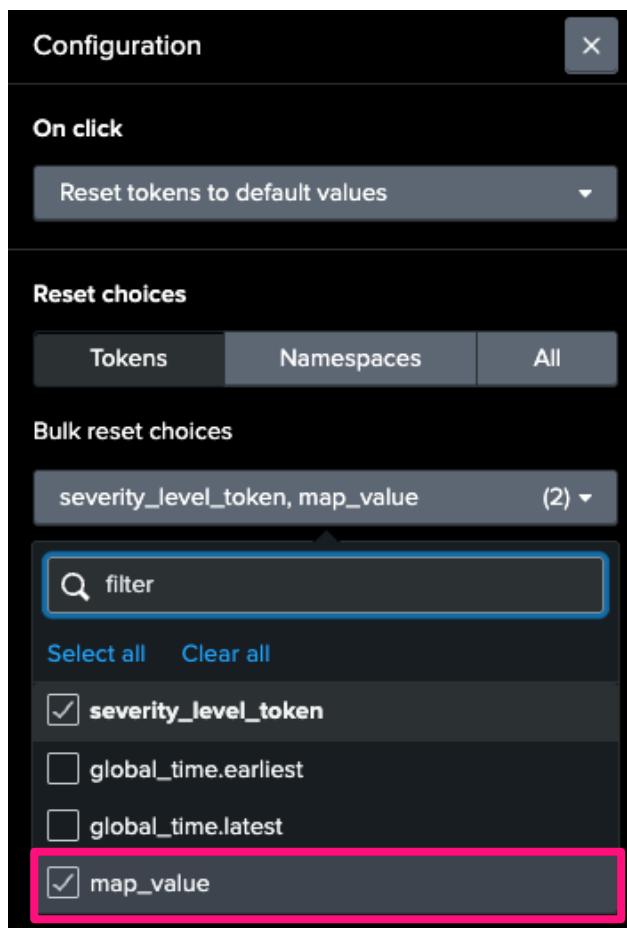
1. Click the Map visualization to open its **Configuration** panel.
2. Find the **Interactions** section and click **+ Add interaction**.
3. Under **On click**, select **Set tokens**.
4. Select **+ Set another token**, then ensure that under **Set token**, **Use predefined token** is selected.
5. For **Token name**, enter “map_value” and for **Token source**, input “row.source_ip.value”



6. Click **Apply** at the bottom of the panel.

[OPTIONAL] Token reset

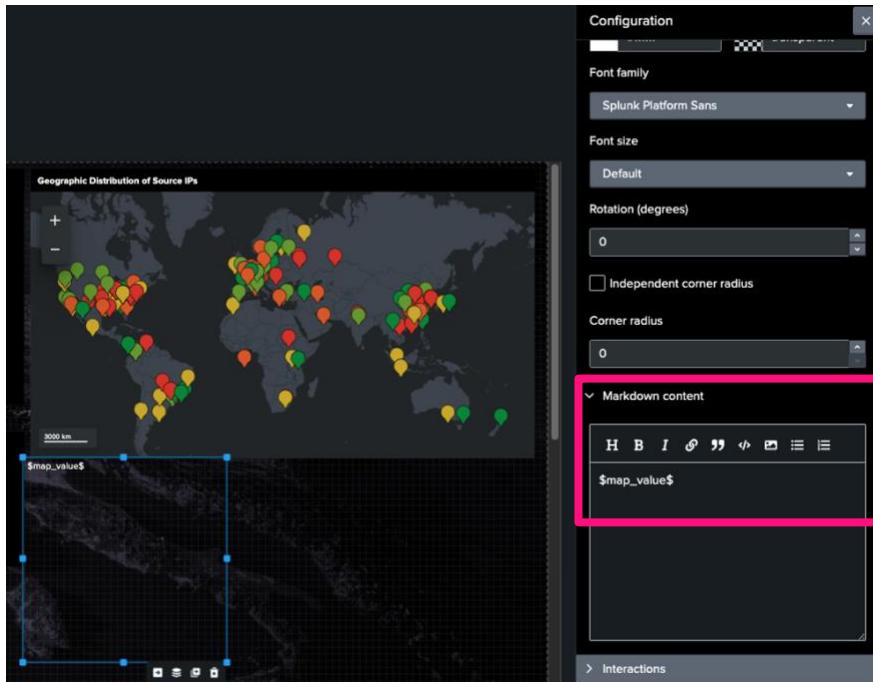
1. Click the **Reset** button to open its **Configuration** panel.
2. In the **Interactions** section, click the pencil icon (>Edit) to edit the existing **Reset tokens to default values** interaction.
3. Under **Bulk reset choices**, click to add **map_value** to the selections.



4. Click **Apply** at the bottom of the panel.

[OPTIONAL] Interaction verification

1. From the editor toolbar, add a **Markdown component** by clicking on this button (MD).
2. In the component's **Configuration** panel, find the **Markdown content** section and enter “\$map_value\$”.



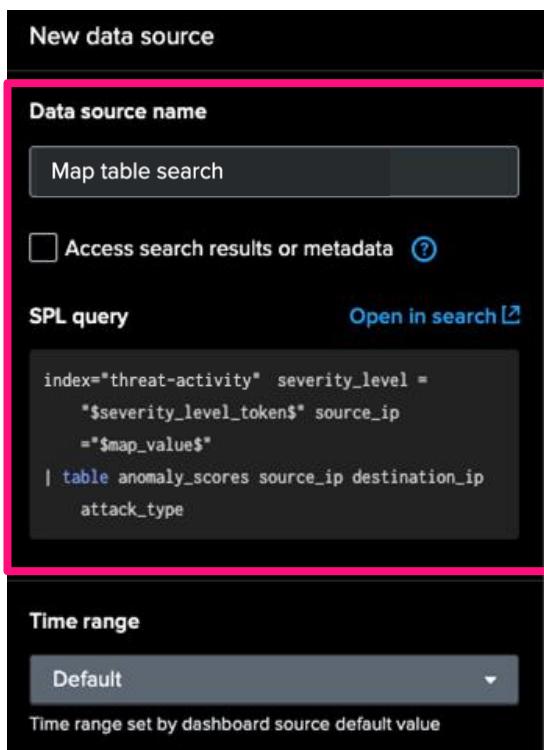
3. In the top right of the page, click the **View** button to switch to view mode.
4. Click any marker on the map. The value in the Markdown component changes to display the selected marker's IP address.
5. Click the reset button (if implemented) and the Markdown component goes back to displaying “\$map_value\$”.
6. You can delete the Markdown component by clicking it and then the trash can icon (X) in the bottom right corner.

Exercise 10 - Conditional Visible Tables

Add the visualization

1. Select **Table** from the **Visualization** dropdown, in the editor toolbar.
2. In the **Select data source** panel, select **Search > + Create search**.
3. Set the **Data source name** to “Map Table Search” and input the following search into the **SPL query** input field:

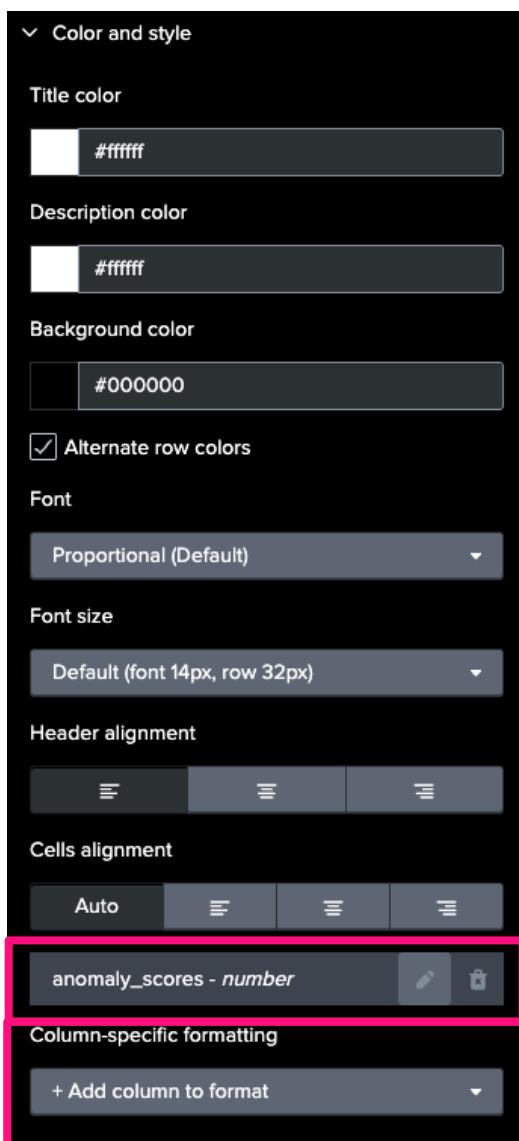
```
index="threat-activity" severity_level = "$severity_level_token$"  
source_ip ="$map_value$"  
| table anomaly_scores source_ip destination_ip attack_type
```



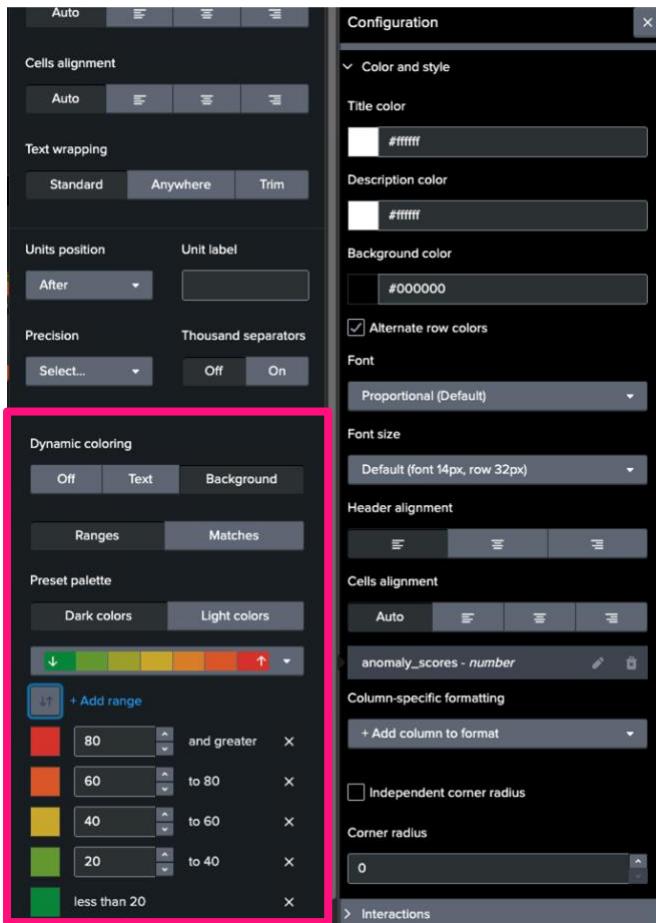
4. Click on **Apply and close** at the bottom of the panel.

Configure the visualization

1. In the new table's Configuration panel, find the **Color and style** section. Under **Column-specific formatting** click on **+ Add column to format**, and then, from the dropdown, select **anomaly_scores - number**.
 - a. You may not be able to select **Column-specific formatting** without a token set. To do so, switch to **View mode** and click on any map marker, then switch back to **Edit mode**.
2. You will see a new element, just above the **+ Add column to format** dropdown, which displays **anomaly_scores - number**. Select the pencil icon to the right of that element, to open the **Column formatting** pop-up.



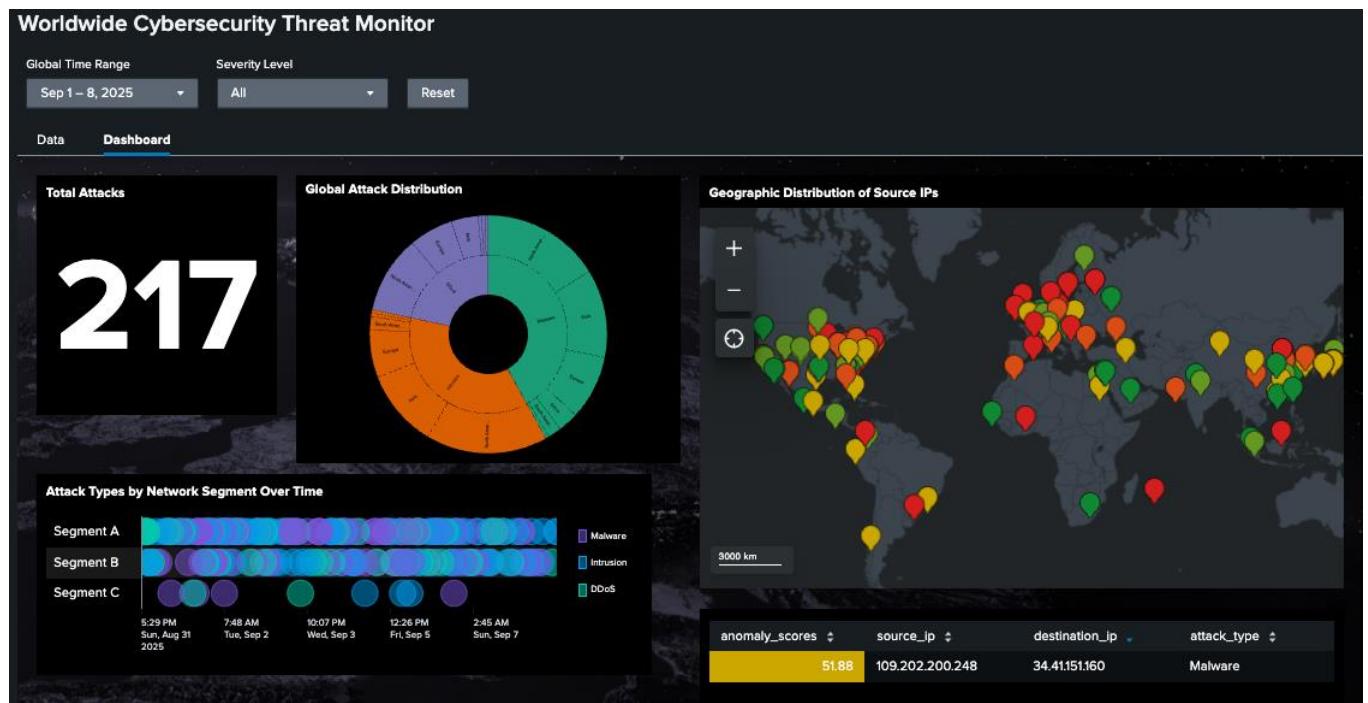
- In the Column formatting pop-up, find the **Dynamic coloring** option and set it to **Background**.



- Under the **Preset palette**, switch the direction of the colors by clicking on this icon (↗️).
- Click on the table to open its **Configuration** panel and find the **Visibility** section. Check the box beside **When data is unavailable, hide element**.
- Move and resize the visualization. It should be in the bottom right of the dashboard and about the same width as the map visualization.

Your dashboard should now look like this.

You can try going to View mode and interacting with the Severity Level, Map markers, and the Reset button, if you implemented it.

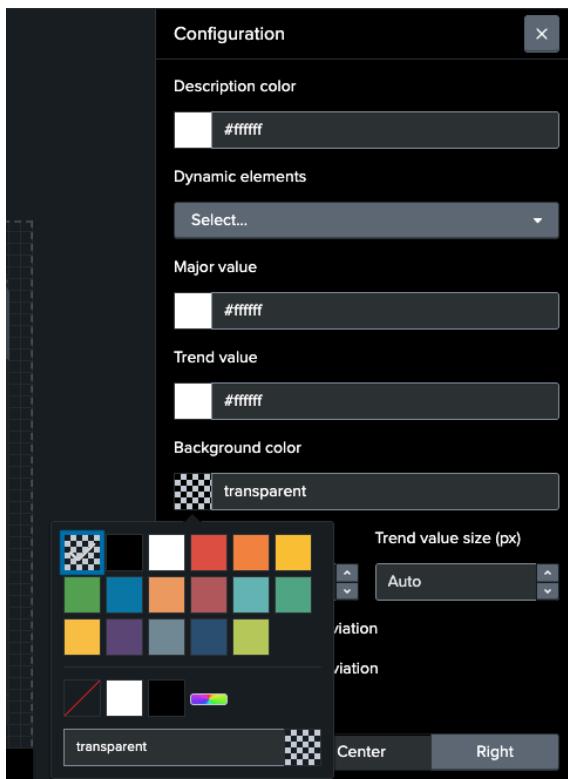


Exercise 11 - (OPTIONAL) Improve Dashboard Styling

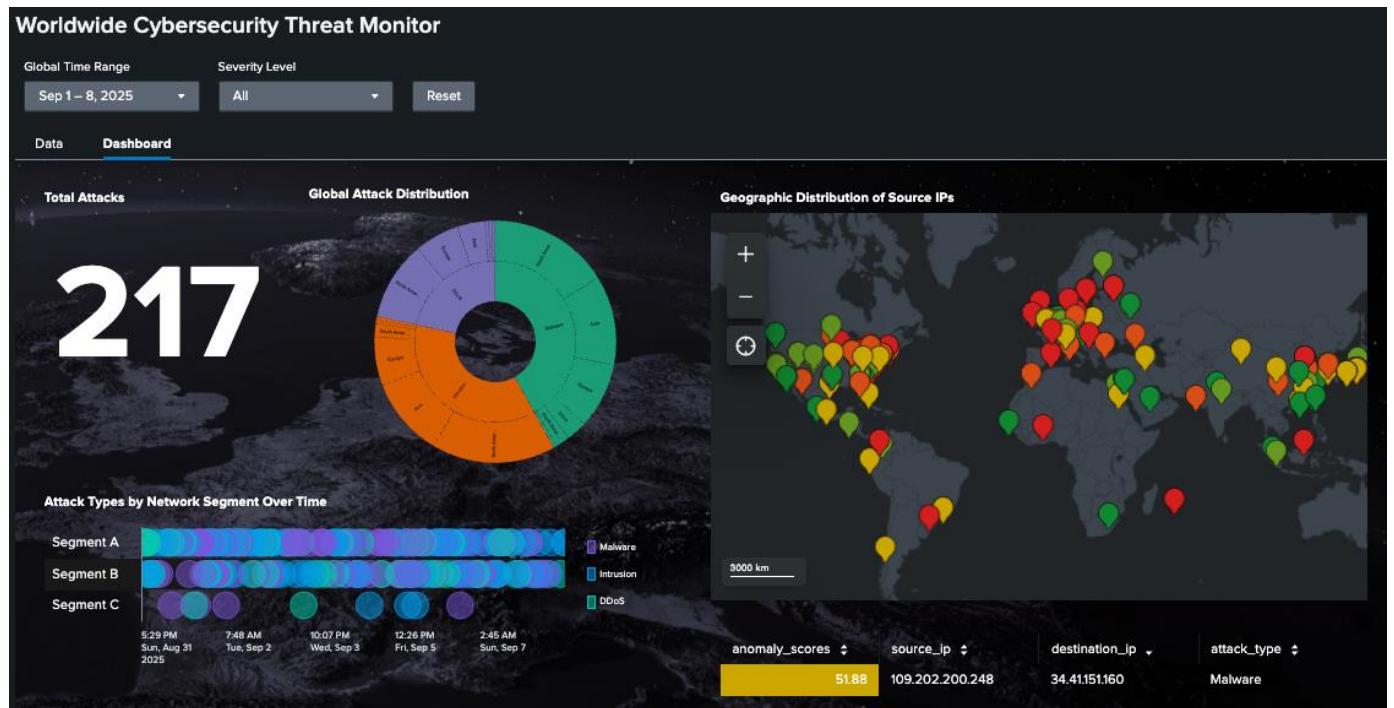
Panel transparency

For each visualization:

1. Select the visualization to open its **Configuration** panel.
2. Find the **Color and style** section.
3. Under **Background color**, select or enter transparent. You can do this by selecting the checkerboard icon, from the color palette, or by typing “transparent” into the color input field.



Completed Dashboard



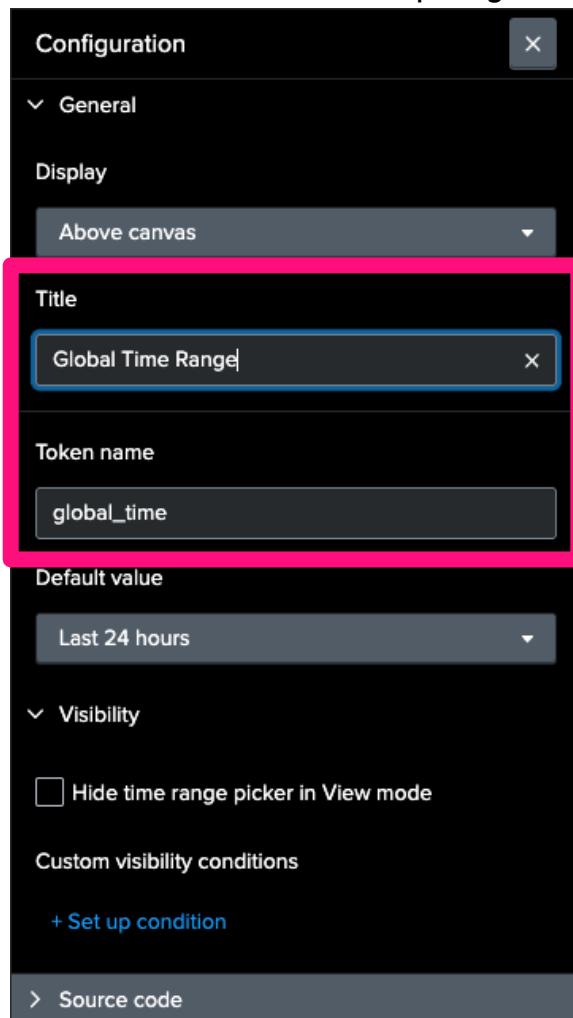
Note: Check out our resources on [Dashboard Design Best Practices](#) and [Visualization Choices and Configurations](#).

Appendix

Adding a global time range picker

The entire dashboard uses the global time range picker by default! For more granular customization, you can set up additional time range pickers, which any number of data sources can use.

1. [OPTIONAL] If you already have a global time range picker, select it and click the x in the top right corner to remove it.
2. From the **Inputs** dropdown (⚙️), select **Time range**.
3. In the input's **Configuration** panel:
 - a. Under **General > Title** put “Global Time Range”.
 - b. Under **Token > Token name** put “global_time”. This is the key to make it global!



4. Press enter or click outside the **Configuration** panel to update.

Searches used

Data table:

Initial iteration:

```
index="threat-activity"
| table _time severity_level attack_type network_segment anomaly_scores source_ip
destination_ip
```

Final iteration:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| table _time severity_level attack_type network_segment anomaly_scores source_ip
destination_ip
```

Single value visualization:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| stats count
```

Timeline:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| eval duration=0
| table _time network_segment attack_type
```

Sunburst:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| iplocation source_ip allfields=true
| stats count by attack_type, Continent, Country
```

Map:

```
index="threat-activity"
severity_level = "$severity_level_token$"
| iplocation source_ip
| table count device_ip lat lon severity_level anomaly_scores source_ip
```

Conditionally visible table:

```
index="threat-activity"
severity_level = "$severity_level_token$"
source_ip = "$map_value$"
| table anomaly_scores source_ip destination_ip attack_type
```