

splunk®> 4rookies

Dashboard Studio



splunk®>
a CISCO company

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as "expects," "anticipates," "targets," "goals," "projects," "intends," "plans," "believes," "momentum," "seeks," "estimates," "continues," "endeavors," "strives," "may," variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the "Risk Factors" section of Cisco's most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the "Risk Factors" section of Splunk's most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk's website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

Please Introduce Yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



By the end of this workshop, you will know:

The fundamentals
for building a
dashboard in
Dashboard Studio

How to incorporate
interactivity into
your dashboard

Best practices for
performance and
sharing



REGISTRATION 5 MINS

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://splunk.show/<uniqueID>>
3. Download the hands-on lab guide:
<https://splk.it/DS4R-Lab-Guide>



Contains step-by-step instructions
for all of today's exercises!

1. Download a copy of today's slide deck.
<https://splk.it/DS4R-Attendee>

Goal



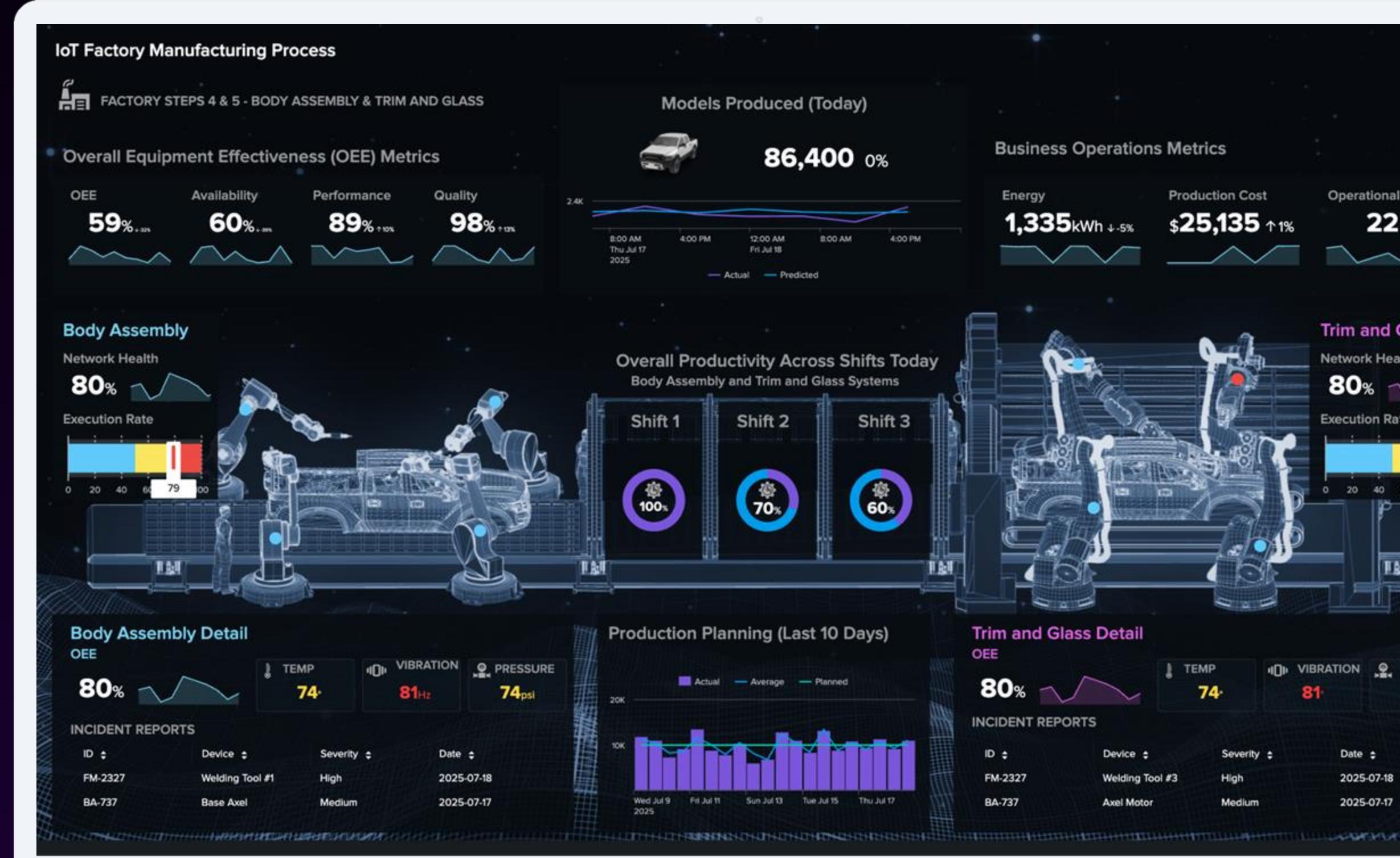
PLATFORM

Splunk4Rookies -
Dashboard Studio
⌚ 28/11 15:53 - 28/11 22:53
💻 Enterprise
🔗 Splunk4Rookies - Dashboard ...
🕒 STARTING SOON Actions ▾

+ Enroll event

Enroll in today's event

About Dashboard Studio



The Evolution of Dashboard Studio



Splunk® Enterprise 9.0
and 9.1

Interactivity improvements

- Set and pass tokens through dashboard drilldowns
- Set tokens from search results
- Show/hide panels



Splunk® Enterprise 9.2 and 9.3

Usability + sharing improvements

- Scheduled email export
- UI for all axes chart configuration options
- Bigger code editor
- Classic to Studio conversion



Splunk® Enterprise 9.4, 10.0,
and upcoming 10.2

Customization and data display

- Publish dashboards to allow viewing without logging in
- Custom Visualization framework
- Advanced conditional visibility
- Optimized rendering and loading

Guidelines for When to Use Dashboard Studio or Classic Dashboards

Dashboard Studio

- Executive- or customer-facing dashboards
- Visualizations that make use of additional physical objects or spacing
- New or less technical users
- Use cases that don't require advanced interactivity

Classic Dashboards

- Dashboards require advanced interactivity or advanced token manipulation
- You need to incorporate complex interactions with custom JS or CSS elements

Today's Scenario

Your Company

- Buttercup Enterprises is a large national online retailer operating in the U.S., which sells a variety of books, clothing and other gifts through its online webstore.
- Buttercup Enterprises invested in Splunk for security.

Your Role

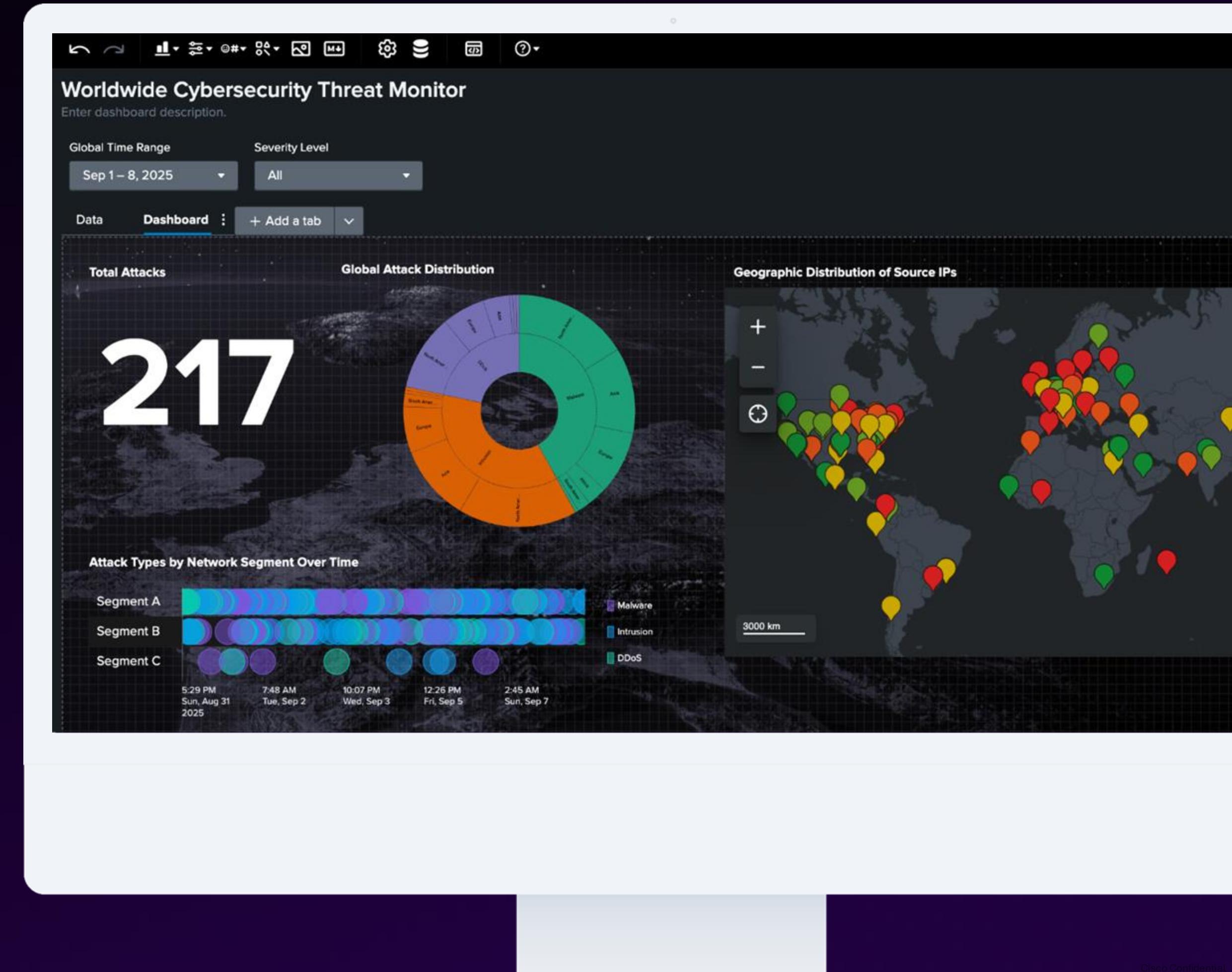
- Your responsibility is to provide dashboards to users throughout the company around cybersecurity analytics.
- You've been asked to gather data and statistics, and provide a view of the following data over the last week:
 - Total Attacks
 - Global Attack Distribution
 - Geographic Distribution of Source IPs
 - Attack Types by Network Segment Over Time



BUTTERCUP
ENTERPRISES

What We're Building Today

Your finished dashboard will look something like this!



Build Time!

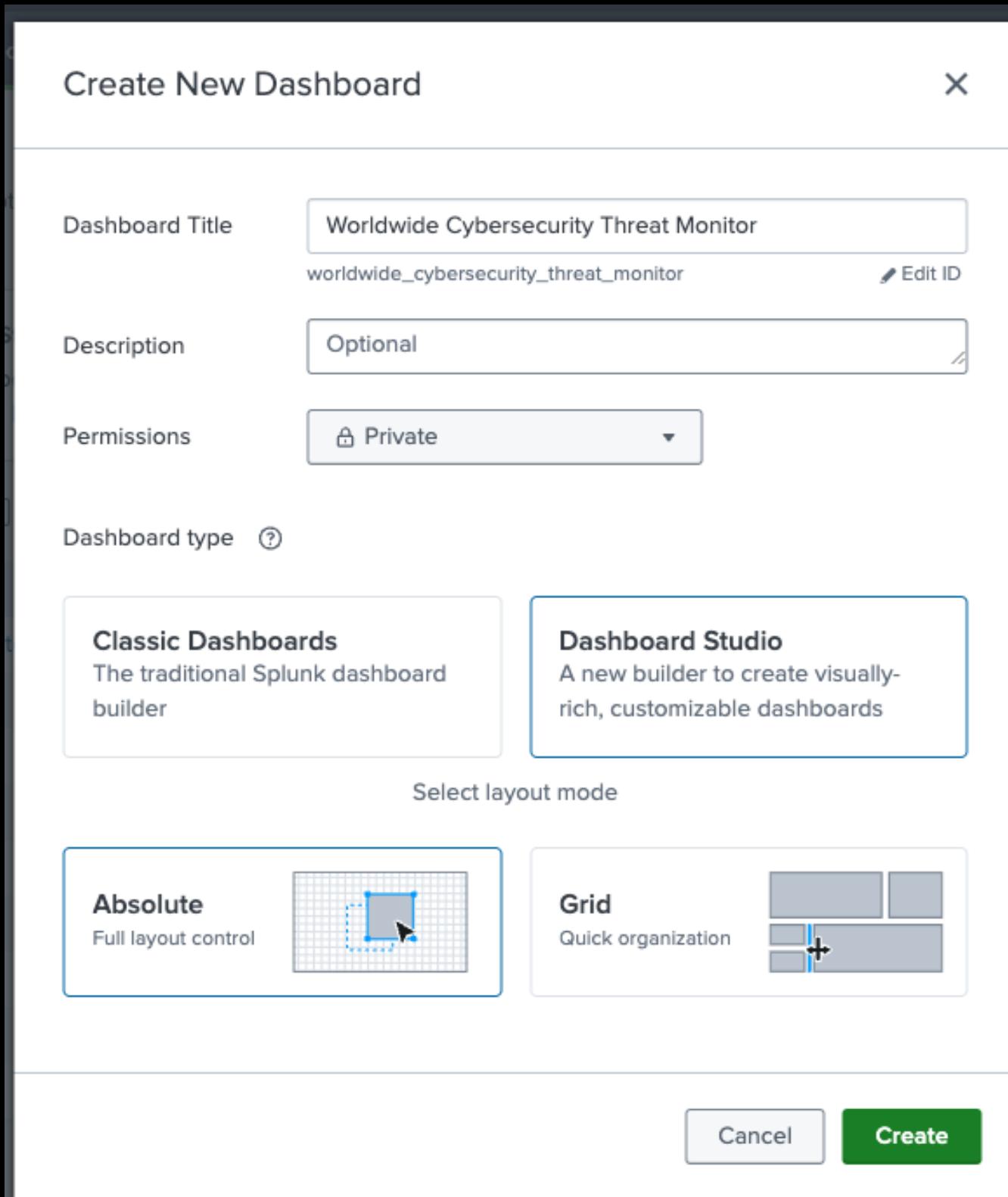
Create a
New
Dashboard



Let's start by creating a new empty dashboard using
Splunk Dashboard Studio

A screenshot of the Splunk Dashboard Studio interface. At the top, there is a toolbar with various icons. To the right of the toolbar, a 'Gridlines' toggle switch is turned on, and a resolution indicator shows '729'. Below the toolbar, the title 'Worldwide Cybersecurity Threat Monitor' is displayed, followed by a placeholder 'Enter dashboard description.' Underneath the title, a 'Global Time Range' dropdown is set to 'Last 24 hours'. A tab bar below the time range shows 'New tab' (which is underlined in blue) and '+ Add a tab'. The main area of the dashboard is currently empty, indicated by a dashed gray border.

Create a New Dashboard

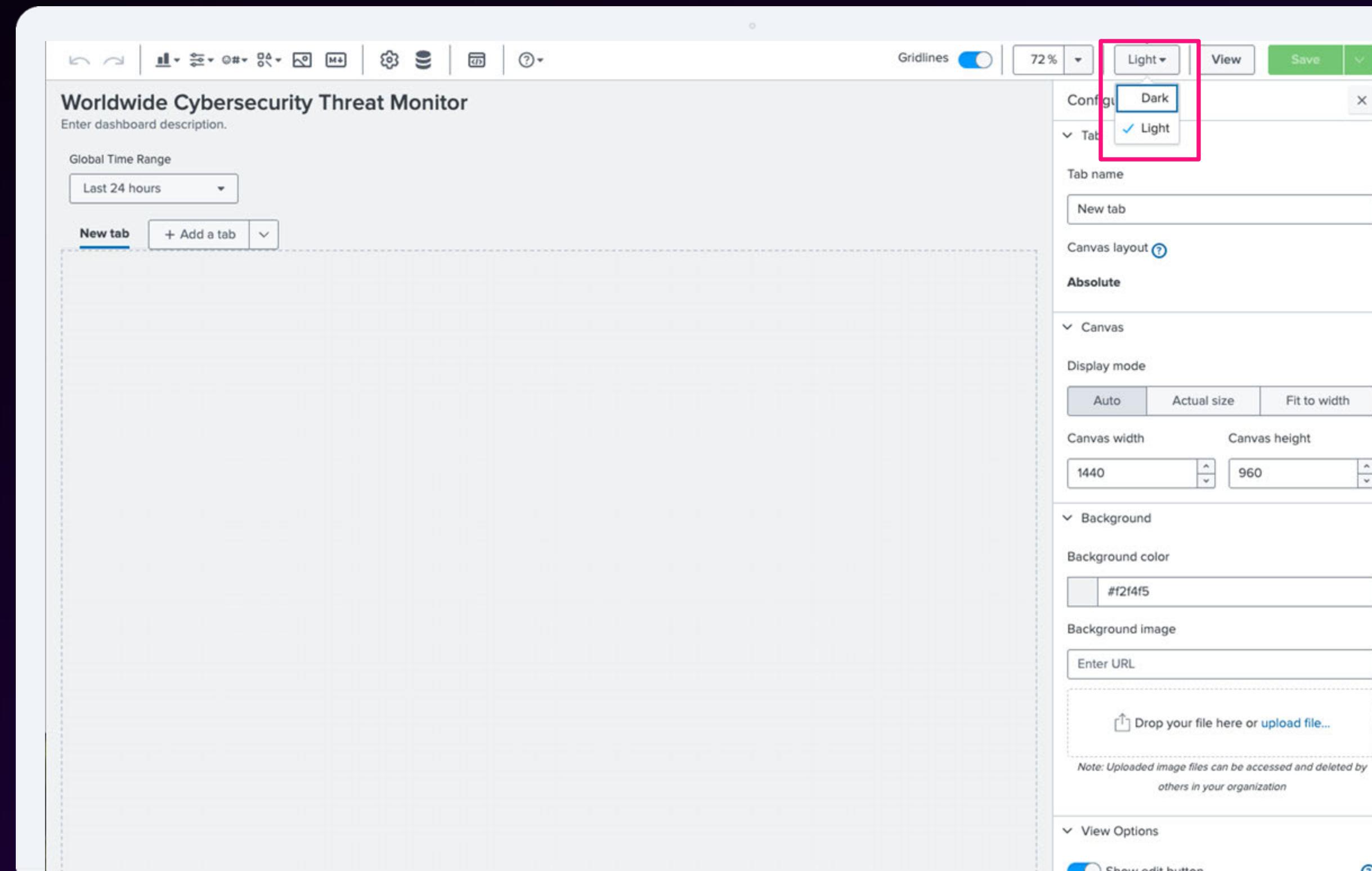


1. Using the **Apps** dropdown in the top left, go to the **Search & Reporting** app.
2. Click the **Dashboards** tab in the top banner.
3. In the upper right corner, click **Create New Dashboard**.
4. Title your dashboard "Worldwide Cybersecurity Threat Monitor <Name>".
5. Keep permissions as **Private**.
6. Select dashboard type **Dashboard Studio**.
7. Select layout mode **Absolute**.
8. Click **Create**.

Let's All Go Dark Mode!

The default dashboard setting is light mode. Let's switch it to dark.

1. In the upper right corner, click the dropdown that says **Light** and select **Dark** to change the display mode.
2. Save!



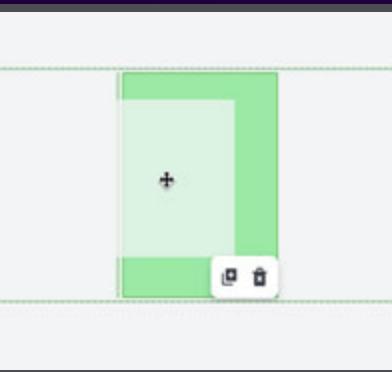
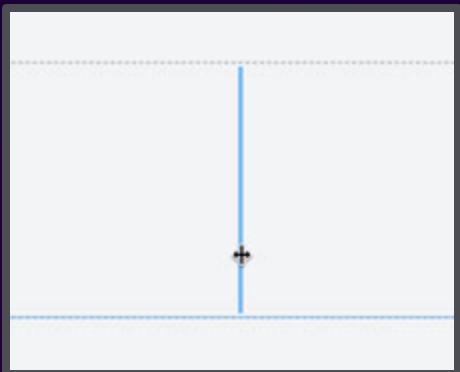
Let's Talk About Layouts

Absolute layout

- Provides pixel-perfect control and allows for object layering
- Good for use cases that require visual representations of physical spaces or objects
- Usually more time-consuming and may take multiple iterations to perfect the spacing and alignment

Grid layout

- Good for quickly assembling dashboards that don't require advanced visuals or design
- Has snap-to alignment with easy and/or auto resizing
- Does not support layering, single value icons, non-rectangular shapes, or background images



Dashboard Layout Tips

- Break the dashboard into **key sections**.
- Ensure your dashboard follows a strong **information hierarchy**:
 - High-level or summarized information should go near the top or left.
 - Detailed or supporting information should go near the bottom or right.
 - Place controls directly above the charts they manipulate when possible.
- When in doubt, arrange the charts **based on your data**.
 - Look for a logical sequence in your data, like a sales funnel or production line.

Dashboard Elements

Charts

- Events
- Table
- Single Value
- Single Value Radial
- Area
- Bar
- Bubble
- Column
- Line
- Timeline

Illustrative Elements

Absolute Layout

- Rectangle
- Circle
- Line
- Markdown
- Icon
- Image

Grid Layout

- Space
- Markdown
- Icon
- Image

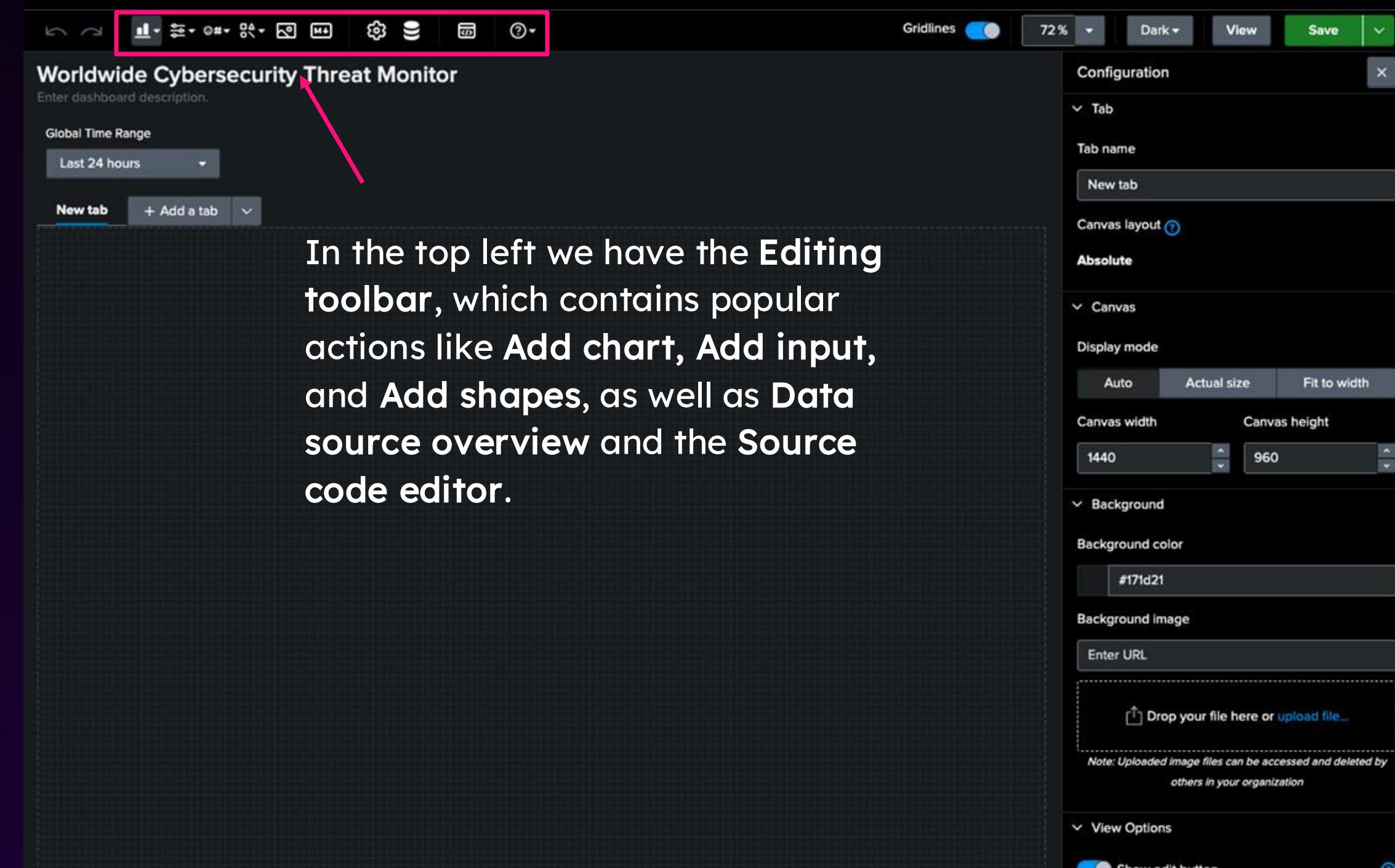
Controls

Inputs

- Dropdown
- Multiselect
- Number input
- Text input
- Timerange
- Button

Editor Tour

Editor Tour (Edit mode)



Editor Tour (Edit mode)

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.

The Configuration panel includes sections for Tab, Canvas, Display mode, Background, and View Options. It also features a file upload area and a note about uploaded image files.

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...
 - Note: Uploaded image files can be accessed and deleted by others in your organization
- View Options**
 - Show edit button

Editor Tour (View mode)

The screenshot shows the Splunk Dashboard Editor interface in View mode. The main area displays a dashboard titled "Worldwide Cybersecurity Threat Monitor" with a global time range set to "Last 24 hours". A sidebar on the right contains configuration options for tabs, canvas layout, absolute positioning, and background settings. A pink arrow points from the text "Note the Configuration panel is only visible in Edit mode." to the "View" button in the top right corner of the editor header.

There are 2 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 in **View** mode.

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

2

Add a Table summarizing our security events

Add a new **table** summarizing all security data for the selected time range.

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	74.31.30.127	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	201.93.87.40	31.44.56.175
2025-09-05T09:56:34.000+00:00	Medium	Intrusion	Segment B	61.05	195.105.112.38	142.31.30.247
2025-09-05T09:17:50.000+00:00	High	Intrusion	Segment A	40.23	35.9.31.89	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	72.5.121.9
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 >

Create a Table

Step 1 of 3 Add data

1. From the Visualizations dropdown, select **Table**.
2. In the Select data source panel, click **+ Create search**.
3. Enter "Data Table" for the **Data source name**.
4. Put the following search in the **SPL query** input:
`index="threat-activity"
| table _time severity_level attack_type
network_segment anomaly_scores source_ip
destination_ip`
5. Select **Apply and close** at the bottom of the panel.

The screenshot shows the Splunk user interface with five numbered steps:

1. A dropdown menu titled "Visualizations" is open, showing options like Table, Events, Single value, Single value radial, Area, Column, Line, and Timeline. The "Table" option is highlighted with a pink box and a pink number "1".
2. A "Select data source" modal window is open. It has a "Search" section with a dropdown and a button labeled "+ Create search" highlighted with a pink box and a pink number "2".
3. A "New data source" panel is open. It shows a "Data source name" field containing "Data Table", a checkbox for "Access search results or metadata" which is unchecked, and an "SPL query" field containing the search command from step 4. This panel is highlighted with a pink box and a pink number "3".
4. The same "New data source" panel is shown again, with the SPL query field containing:
`index="threat-activity"
| table _time severity_level attack_type
network_segment anomaly_scores source_ip
destination_ip`
5. The bottom of the interface shows a summary of the visualization: "1 visualization", "0 inputs", and "0 chain searches". It also shows a "Source code" link, a message "1 visualization will be updated", and buttons for "Cancel" and "Apply and close".

Where's My Data?

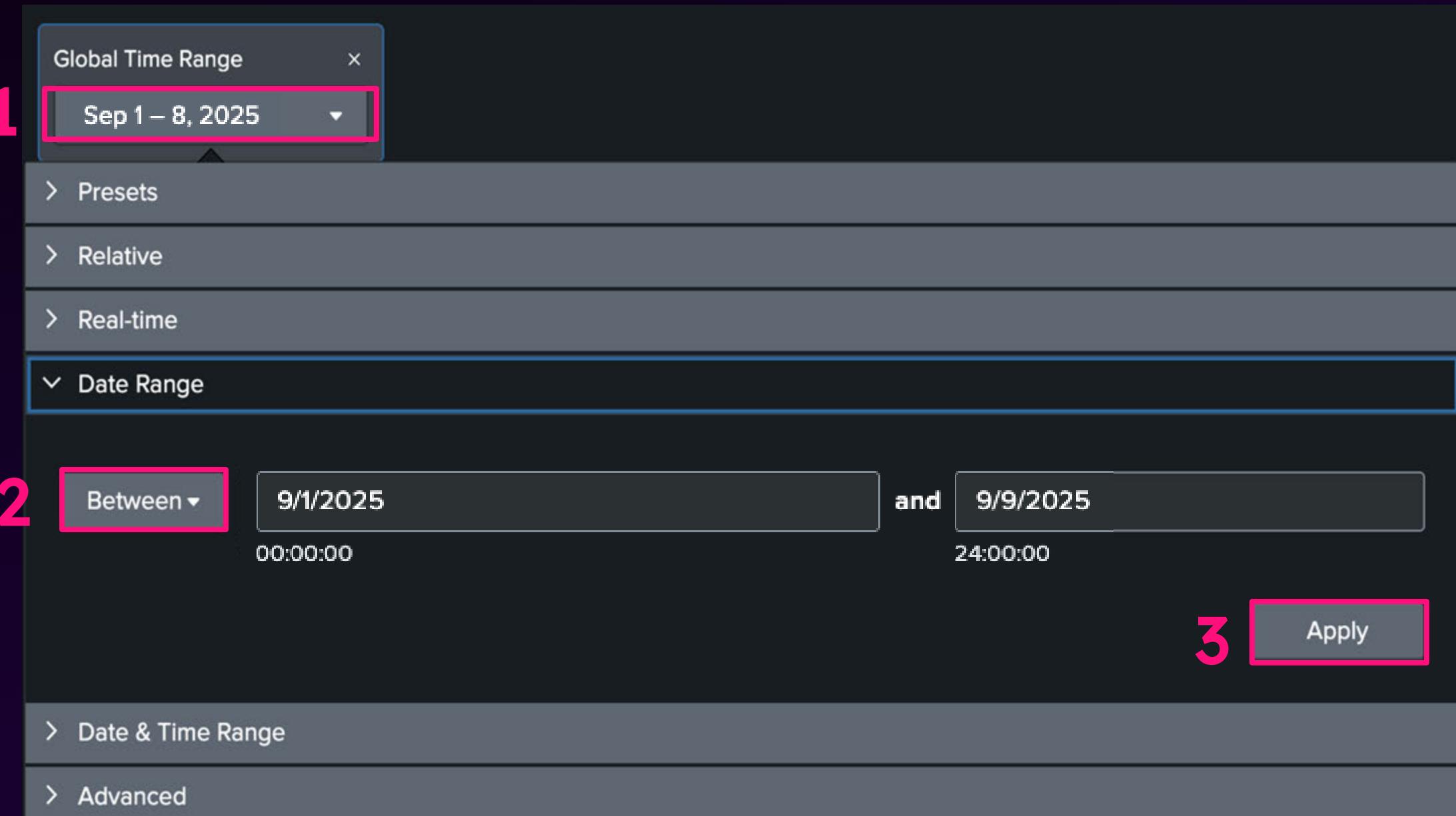
Create a Table

Step 2 of 3

Set time range

The default time range is “Last 24 hours”, which *may* produce no data!

1. Click the **Global Time Range picker**, just above the canvas. If you can't find it, it's possible it was accidentally removed. You can find the steps to add it back in the Appendix.
2. Select **Date Range > Since** and select **Between** in the dropdown.
3. Input dates: **9/1/2025** to **9/9/2025**.
4. Click **Apply** at the bottom right and the table will update!
5. Click **Save!**



Create a Table

Step 3 of 3

Format table

1. Click the table.
2. Under **General > Title** input “Data Table”.
3. Under **General > Description** input “This is the raw data”. The Title and Description show up automatically as soon as you hit enter or click away from the editor.
4. Click **Save!**

The screenshot shows the Splunk Configuration interface for creating a new visualization. The 'Visualization type' is set to 'Table'. The 'Title' field contains 'Data Table' and the 'Description' field contains 'This is the raw data'. Both fields are highlighted with a pink border. Step 1 points to the 'Title' field, step 2 points to the 'Description' field, and step 3 points to the preview window below which shows the table with the configured title and description.

_time	severity_level	attack_type	network_seg...	anomaly_scores	source
2025-09-11T23:46:15.000+00:00	Low	Intrusion	Segment A	86.95	14.53.5
2025-09-11T22:47:19.000+00:00	Medium	Malware	Segment A	75.28	24.183.
2025-09-11T22:40:29.000+00:00	Medium	Intrusion	Segment A	42.27	120.149
2025-09-11T22:04:22.000+00:00	High	Malware	Segment B	76.35	189.102
2025-09-11T21:26:29.000+00:00	Low	Malware	Segment B	67.38	115.140.

Checkpoint

Your dashboard should now have a Table filtered to the time range you want.

Make sure to save often!

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

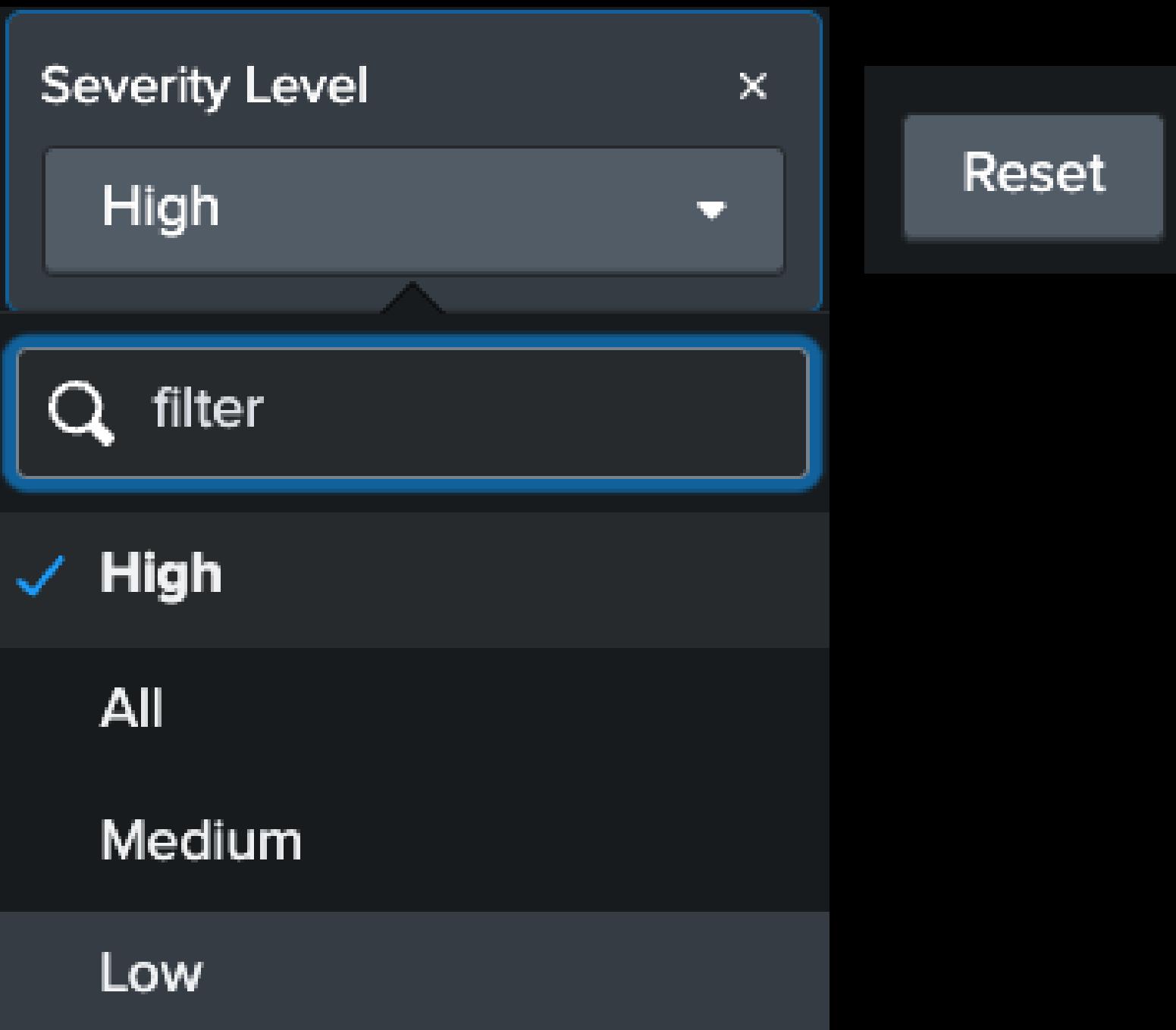
< Prev 1 2 3 4 5 ... Next >

Filtering with Tokens

to improve
dashboard
usability

3

Add a “Severity Level” dropdown so we can to **filter visualizations on the dashboard** by the selected severity level



About Tokens

A token represents **a value that can change**, such as a selection from a dropdown. You can use tokens to access and pass these values to create more **interactive and dynamic** dashboards.

In this example, we will create a Severity Level dropdown, which you can use to filter data on the dashboard by the attack severity level. Selecting the value from the dropdown sets the value of the associated token, `severity_level_token`, to the selected value. You can use the syntax `$severity_level_token$` in data sources to dynamically reference the value of `severity_level_token`.

Here's an example of a search that uses the `severity_level_token` value:

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

For example, when you select High from the Severity Level dropdown, the search uses High as the value of `severity_level_token`:

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

Adding Tokens

Step 1 of 4

Setting up the input

1. From the **Inputs dropdown**, select **Dropdown**.
2. In the dropdown's **Configuration panel**:
 - a. Under **General > Title** input "Severity Level".
 - b. Under **Token > Token name** put "severity_level_token".
 - c. Fill the **Static menu configuration** section with the same fields as you see over there (they're also in your lab guide). Clicking **+ Add new** will add a row.
 - d. Under **Default selected values** select **First value**.

The screenshot shows the Splunk UI interface. At the top, there is a toolbar with various icons. Below it is a dropdown menu labeled "Inputs" with the number "1" above it, which is highlighted with a pink box. The dropdown menu lists several input types: "Dropdown", "Multiselect", "Text", "Number", "Time range", and "Button". The "Dropdown" option is currently selected and highlighted with a blue box. To the right of the dropdown menu is a configuration panel for a "Dropdown" token. The configuration panel has the following sections:

- Display:** Set to "Above canvas".
- Title:** "Severity Level".
- Token:** "severity_level_token".
- Menu configuration:** A table with four rows:

Label	Value
All	*
High	High
Low	Low

A button "+ Add new" is available to add more rows.
- Default selected values:** A section with three buttons: "Choose default", "First value" (which is highlighted with a pink box), and "None". A tooltip below the "First value" button states: "Assigns the first value returned from the data source as the default".

Adding Tokens

Step 2 of 4

Adding a token

1. Open the **Data source overview** panel. You can do so by clicking the database icon in the toolbar.
2. Click the pencil icon next to **Data Table**. (This is the data source we created earlier for our table.)
3. Change the **SPL Query** to (differences highlighted):

```
index="threat-activity"
severity_level = "$severity_level_token$"

| table _time severity_level attack_type
network_segment anomaly_scores source_ip
destination_ip
```

If you selected the right data source, you'll see a message that says “1 visualization will be updated”.

1. Select **Apply and close** at the bottom of the panel.

The screenshot shows the Splunk interface with the following components:

- Toolbar:** Includes icons for search, dashboard, reports, and settings. The database icon (highlighted with a pink box) is located in the top right corner.
- Data source overview panel:** A sidebar with sections for Search, Saved search, and Chain search. The "Data Table" section is expanded, showing a pencil icon (highlighted with a pink box) next to it.
- Edit data source dialog:** A modal window titled "Edit data source".
 - Data source name:** Set to "Data Table".
 - Access search results or metadata:** An unchecked checkbox.
 - SPL query:** A code editor containing SPL code. The line `severity_level = "$severity_level_token$"` is highlighted with a pink box. The entire code block is also highlighted with a pink box.
 - Time range:** Set to "Input" (selected) and "Global Time Range (global_time)".
 - Event Sampling:** Set to "1: 1".
 - Usage:** Shows "1 visualization". A message at the bottom states "1 visualization will be updated".

Adding Tokens

Step 3 of 4

Testing out the dropdown

1. Click the **Severity Level** dropdown. “All” should be selected by default. Select any other option.

You will see the search rerun and then the table values will change!

The small circle in the top right corner of the Table indicates that the data source’s search is running.

Worldwide Cybersecurity Threat Monitor					
Global Time Range		Severity Level			
Sep 1 – 8, 2025		All	Reset		
Data		attack_type	network_segment	anomaly_scores	source_ip
Dashboard		High	Malware	Segment A	195.213.72.164
_time		Medium	Intrusion	Segment A	171.203.93.126
2025-09-03T20:22:09.000+00:00		Low	DDoS	Segment A	13.111.158.190
2025-09-03T18:49:21.000+00:00		Medium	Intrusion	Segment B	66.73.202.94
2025-09-03T17:58:06.000+00:00		Low	Malware	Segment A	82.23 183.211.191.179
2025-09-03T16:13:11.000+00:00		Medium	Intrusion	Segment B	46.63 135.119.183.105
2025-09-03T16:10:11.000+00:00		High	Malware	Segment A	86.168.51.39
2025-09-03T13:47:04.000+00:00		Medium	Intrusion	Segment B	43.174.225.214
2025-09-03T11:55:43.000+00:00		High	Intrusion	Segment B	132.231.71.60
2025-09-03T11:19:27.000+00:00		Medium	Malware	Segment A	105.193.254.47
2025-09-03T11:19:27.000+00:00		Medium	Intrusion	Segment B	67.43 71.41.31.239
2025-09-03T11:19:27.000+00:00		Medium	Malware	Segment A	22.246.227.69
2025-09-03T11:19:27.000+00:00		Medium	Intrusion	Segment B	59.162.11.61

We now have an input that anyone can use to control the results they are shown.

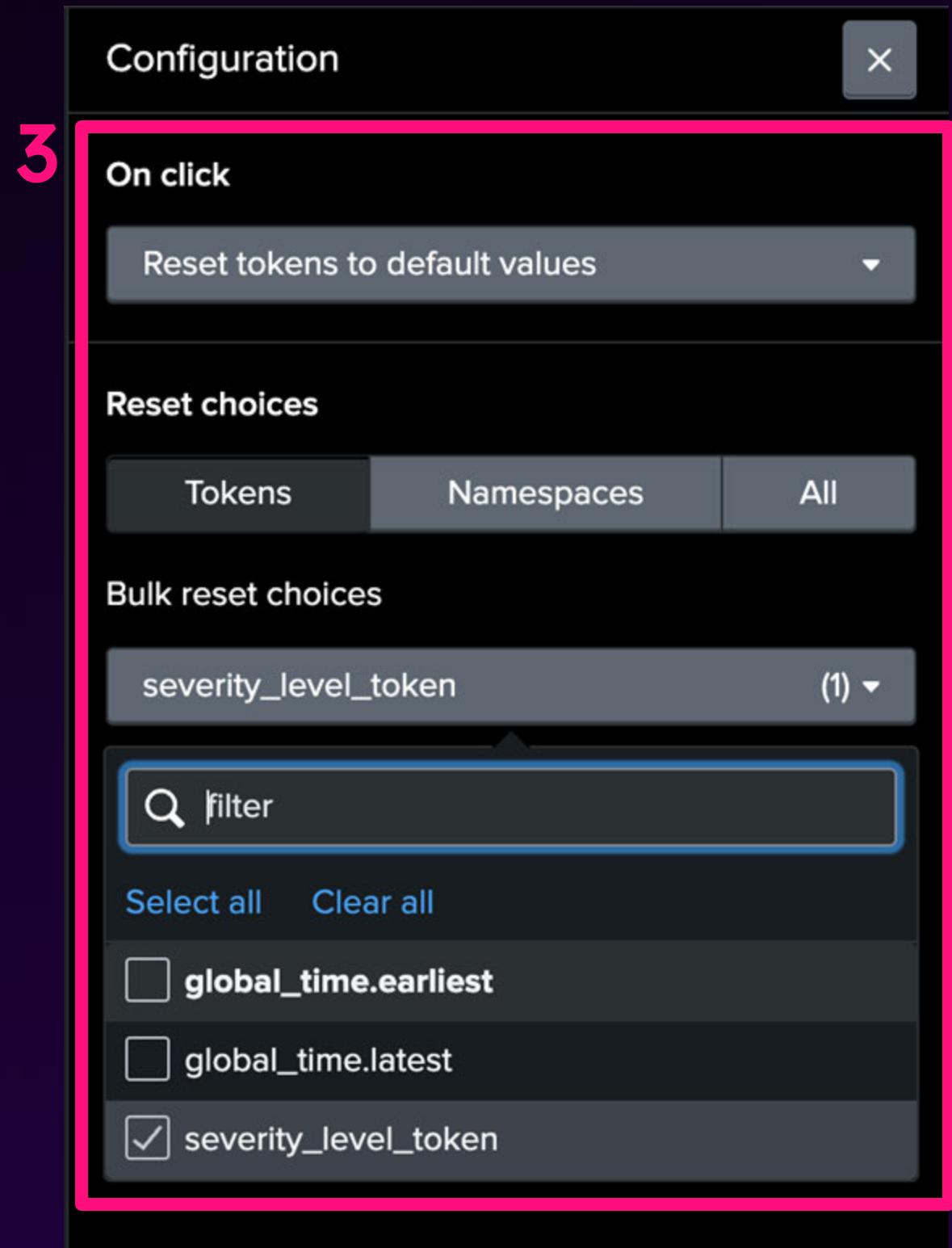
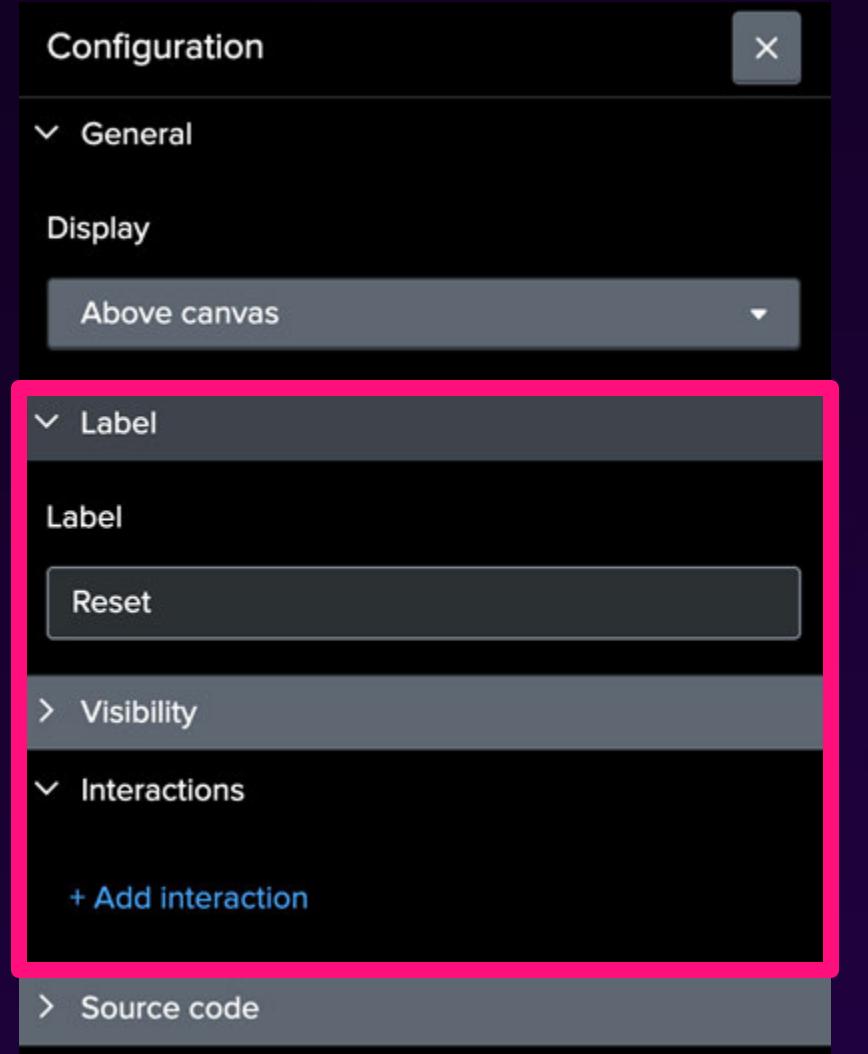
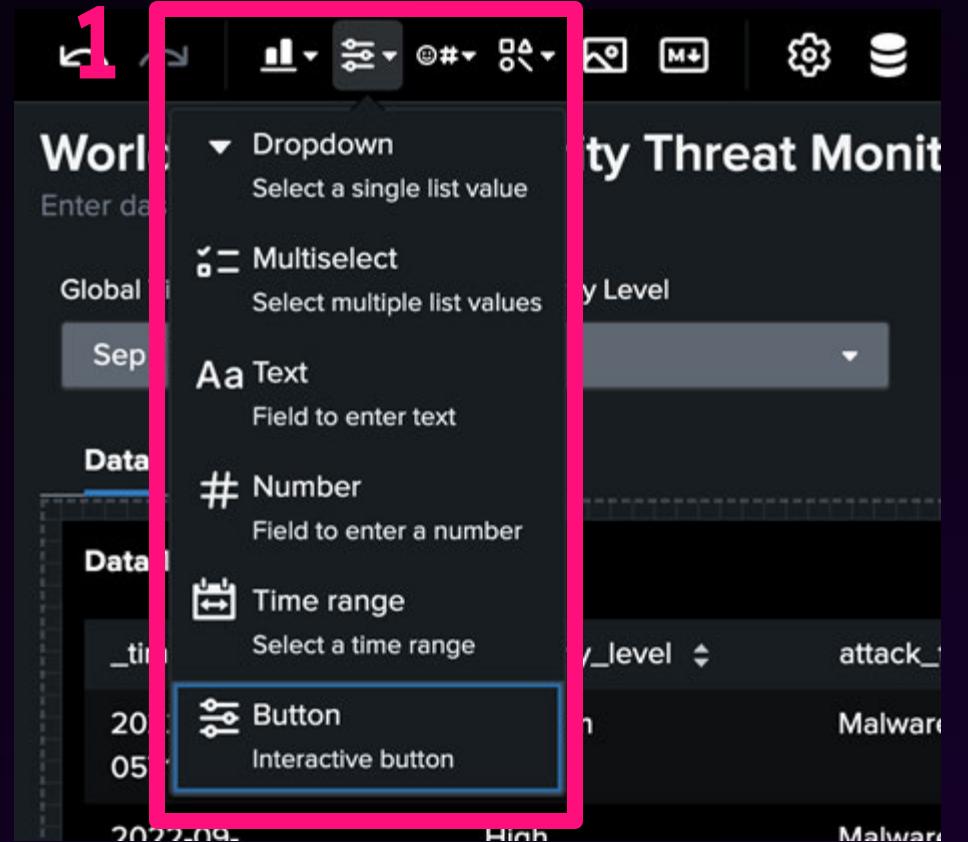
(OPTIONAL)

Adding Tokens

Step 4 of 4

Adding a reset button

1. From the **Inputs** dropdown, select **Button**.
2. In the button's **Configuration** panel:
 - a. Under **Label > Label** input “Reset”.
 - b. Under **Interactions** click + Add interaction.
 - c. Select **On click** and set it to **Reset tokens to default values**.
 - d. For the **Reset choices**, select **Tokens**.
 - e. Under **Bulk reset choices** select our new **severity_level_token** token.
 - f. Save!



Checkpoint

Your dashboard should now have a dropdown to set a filter by severity level.

(And maybe even a Reset button.)

Don't forget to save!

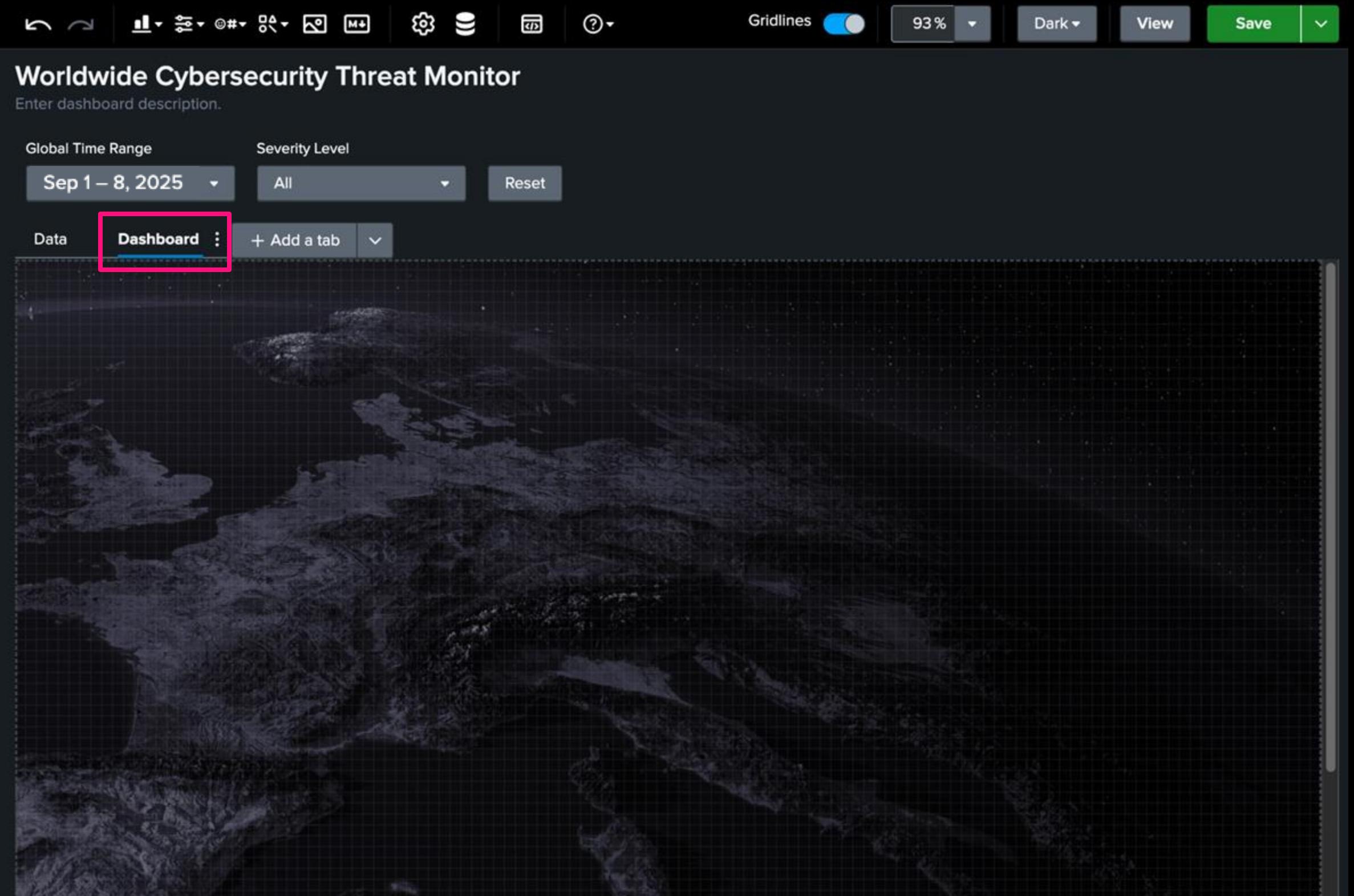
The screenshot shows a dashboard titled "Worldwide Cybersecurity Threat Monitor". At the top, there is a "Global Time Range" set to "Sep 1 – 8, 2025" and a "Severity Level" dropdown menu set to "All", which is highlighted with a red box. Below this, there is a "Data Table" tab selected, showing a table of raw data. The table has columns for _time, severity_level, attack_type, network_segment, anomaly_scores, source_ip, and destination_ip. The data consists of ten rows of threat information, including various attack types like Malware, Intrusion, and DDoS across different network segments and with different severity levels and scores.

_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	74.31.107.127	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
2025-09-	Medium	Intrusion	Segment A	22.47	152.114.200.223	28.231.50.198

4

Add a
New Tab
to help organize
the dashboard

Add a new “Dashboard” tab to hold the remaining visualizations and organize data without cluttering the Data tab



Add a New Tab

Step 1 of 4

1. Select **+ Add a tab** (it will be just above the canvas on the left).
2. In the Configuration panel, on the right, set the **Tab name** to “Dashboard”.
3. Under **Canvas layout** you will see that the default is Grid. Click **Change**.
4. Select **Absolute** and click **Change** in the bottom to submit.

Worldwide Cybersecurity Threat Moni
Enter dashboard description.

Global Time Range Severity Level

Sep 1 – 8, 2025 All

Data + Add a tab 1

Data Table

_time	severity_level	attack_type
2025-09-05T11:37:08.000+00:00	Medium	Malware

Configuration

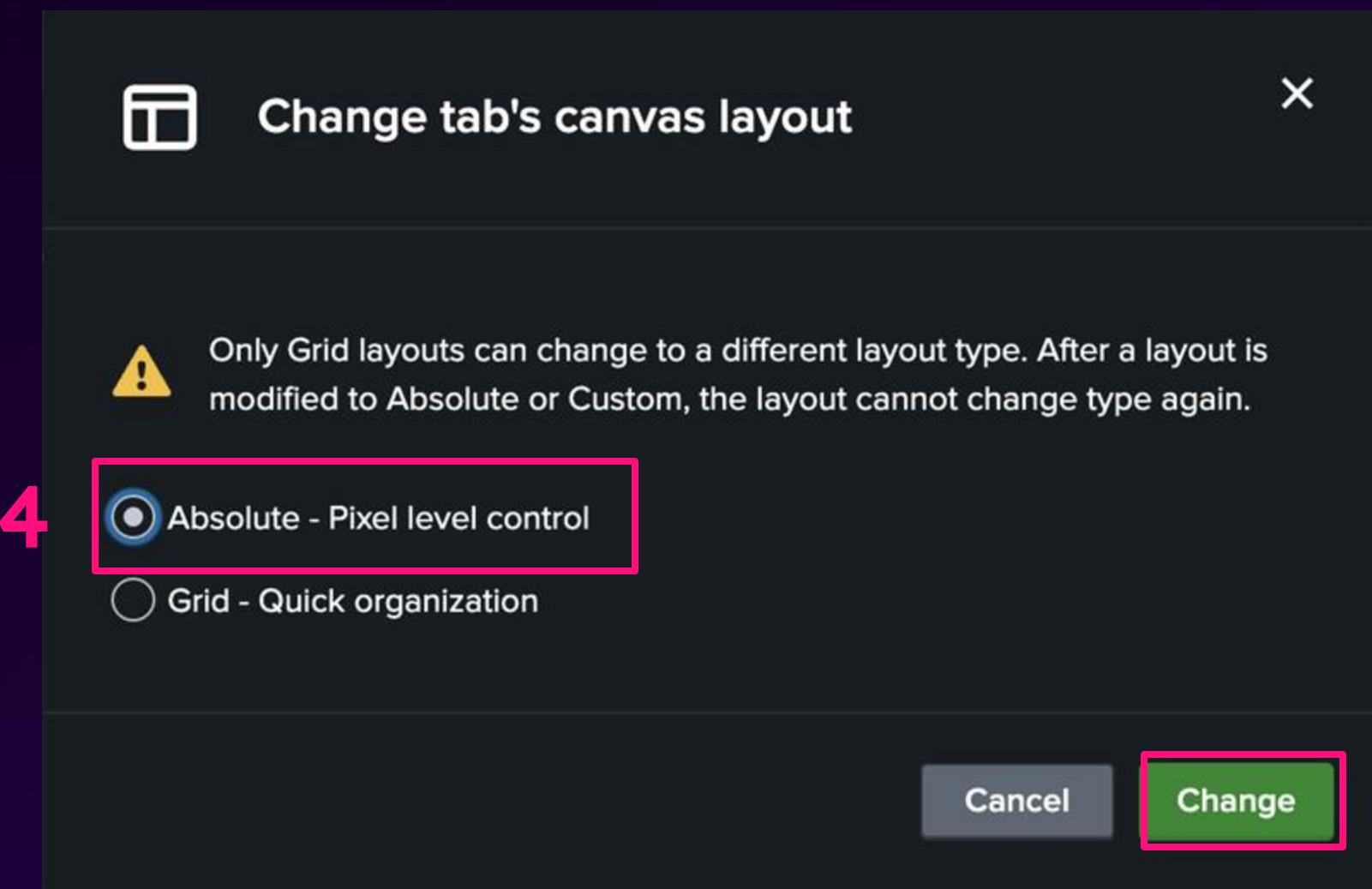
Tab

Tab name

Dashboard

Canvas layout ?

Grid 3 Change

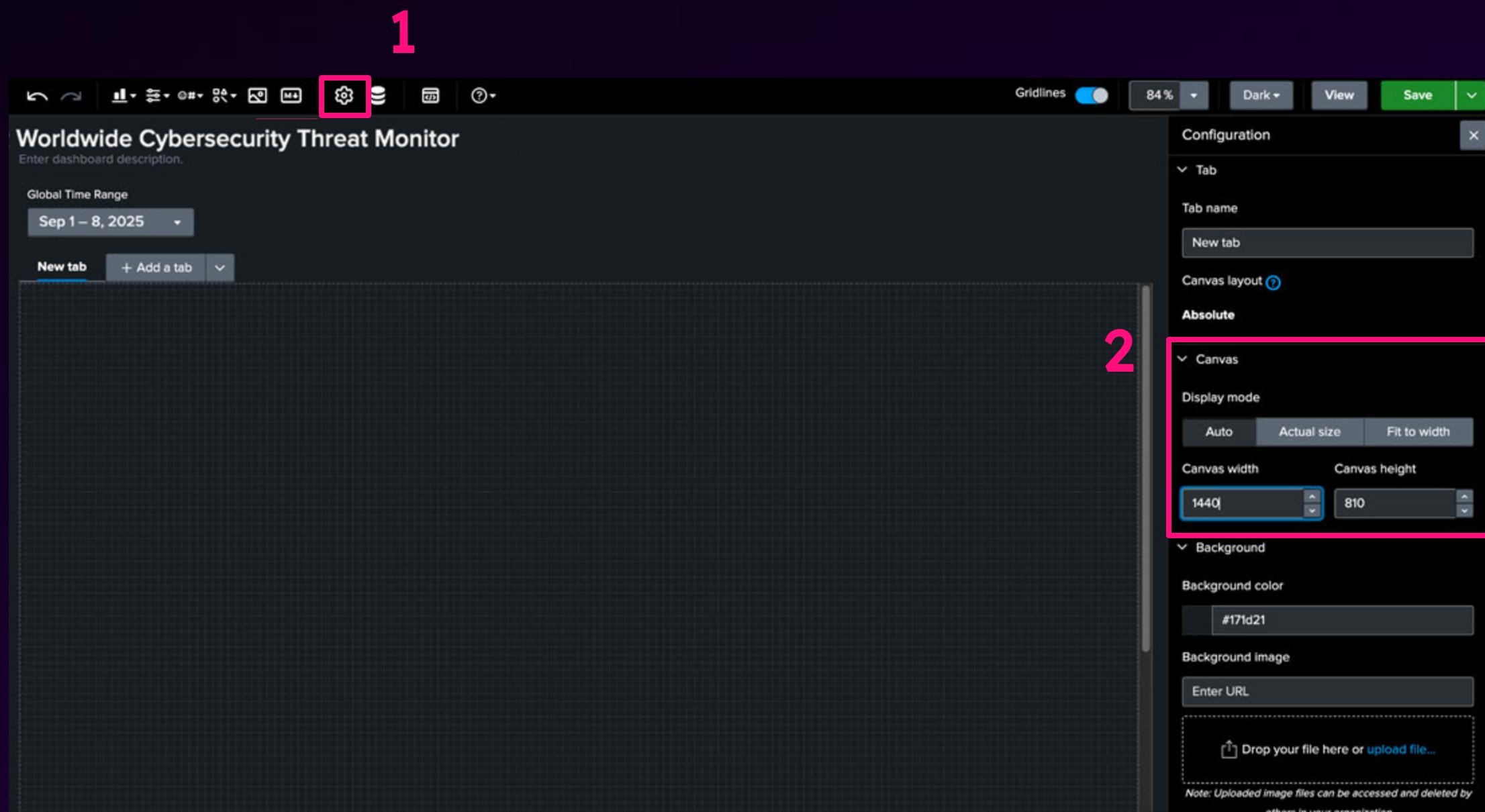


Set the Properties

Step 2 of 4

Set the dashboard size

1. Open the **Configuration** panel for the dashboard (click the gear icon in the menu bar or anywhere on the dashboard canvas that isn't an added element).
2. Find the **Canvas** section:
 - a. Set **Display mode** to **Auto**.
 - b. Set **Canvas width** to **1440** and **Canvas height** to **810**.
3. **SAVE!**



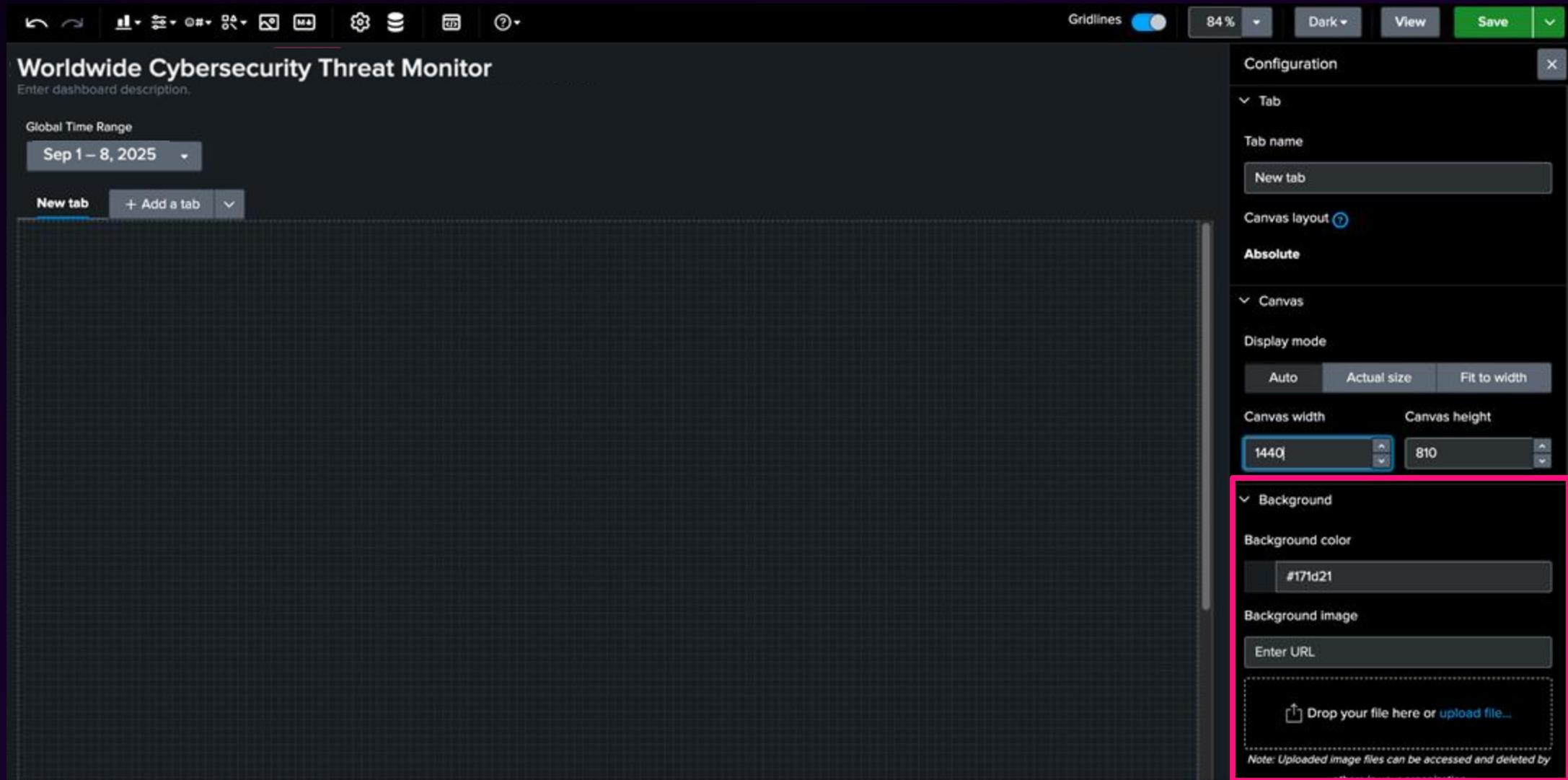
Add a Background

Step 3 of 4

Add the image

There are several ways to add an image to use as a background. Today we're going to use an image that was included with an installed app.

1. In the Configuration panel, find the section titled **Background**.
2. In the **Enter URL** field, enter the following (copy/paste it to avoid typing errors!):
`/static/app/splunk-dashboard-studio/images/examples-hub/europe_network_hub/europe_network_hub_background_image.jpg`
3. Click away from the input box and the image should populate.



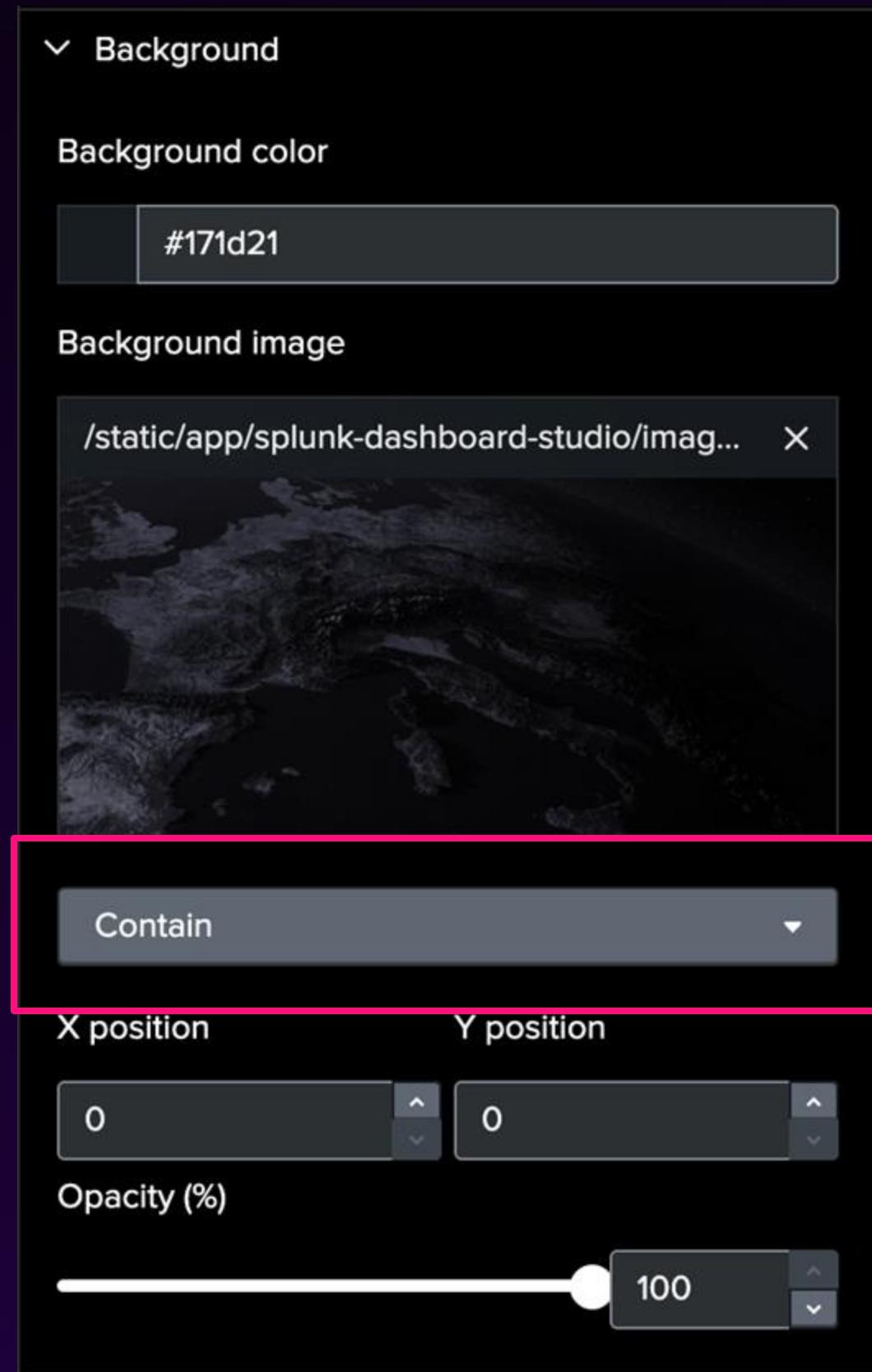
Set the Properties

Step 4 of 4

Set up the background settings

If you have successfully added the URL, a small version of the image will show up, in the place of the input.

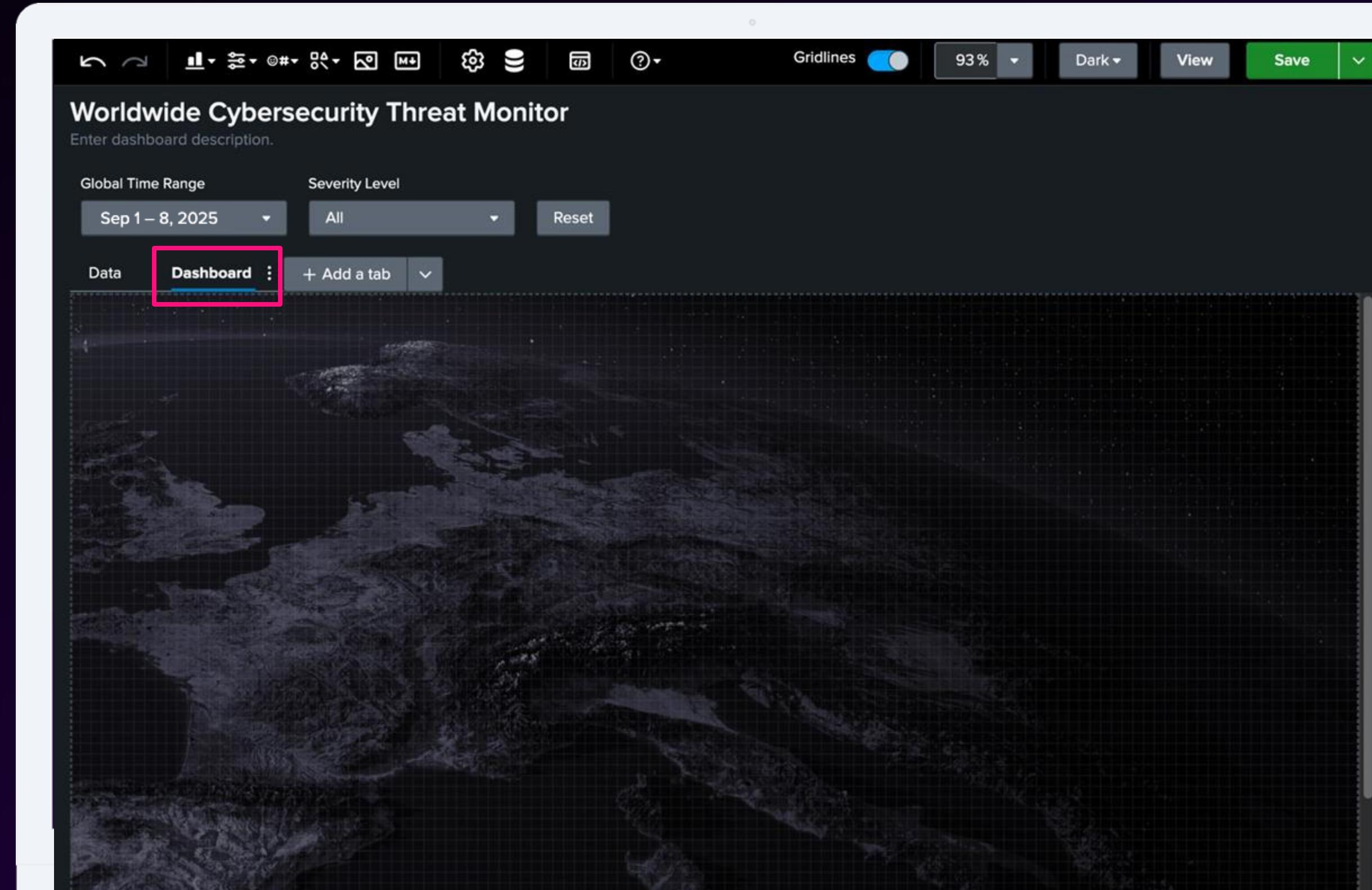
1. Below the image, there will be a dropdown that currently shows **Contain**. Select **Cover** instead. You can leave the rest of the settings as-is.
2. Save your dashboard!



Checkpoint

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

[OPTIONAL] Feel free to go and rename the first tab to “Data” (instructions can be found on slide 35)!



5

Create a
Single Value
Visualization

Add the **Total Attacks** single value visualization to provide a quick reference for the **total number of attacks**



Create a Single Value Visualization

Step 1 of 2

Add Total Attacks data

Make sure you are on your **Dashboard** tab!

1. From the Visualizations dropdown, select **Single value**.
2. In the **Select data source** panel, click **+ Create search**.
3. Enter "Single value search" for the **Data source name**.
4. Put the following search in the **SPL query** input:

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

5. Select **Apply** and **close** at the bottom of the panel.
6. Save!

The screenshot shows the Splunk interface for creating a new data source. On the left, a sidebar lists visualizations: Table, Events, Single value (which is selected and highlighted in blue), Single value radial, Area, Column, and Line. On the right, a panel titled 'New data source' contains fields for 'Data source name' (set to 'Single value search') and an 'SPL query' input field. The SPL query is set to:

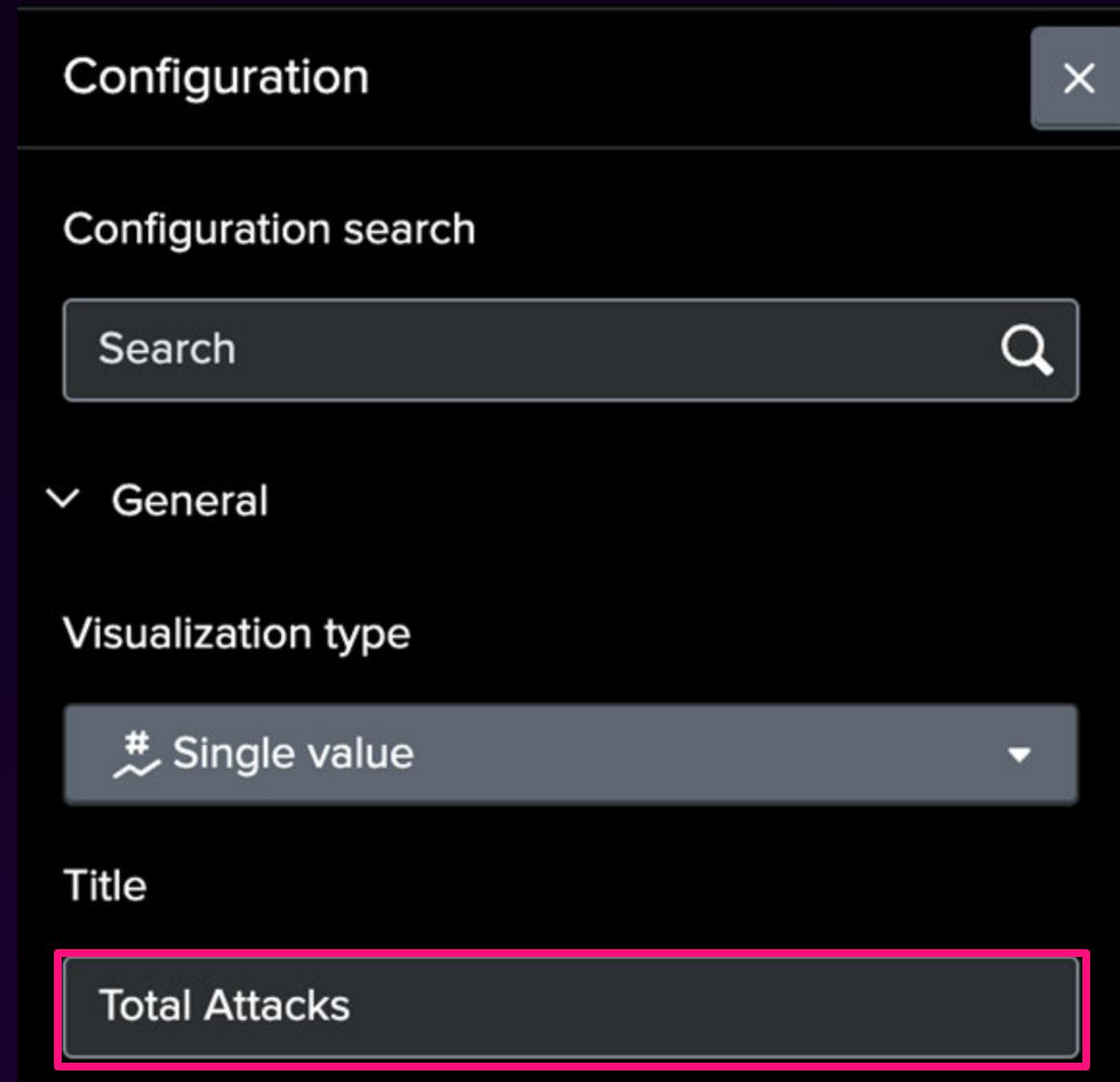
```
index="threat-activity" severity_level =
$severity_level_token$
| stats count
```

Create a Single Value Visualization

Step 2 of 2

Format single value visualization

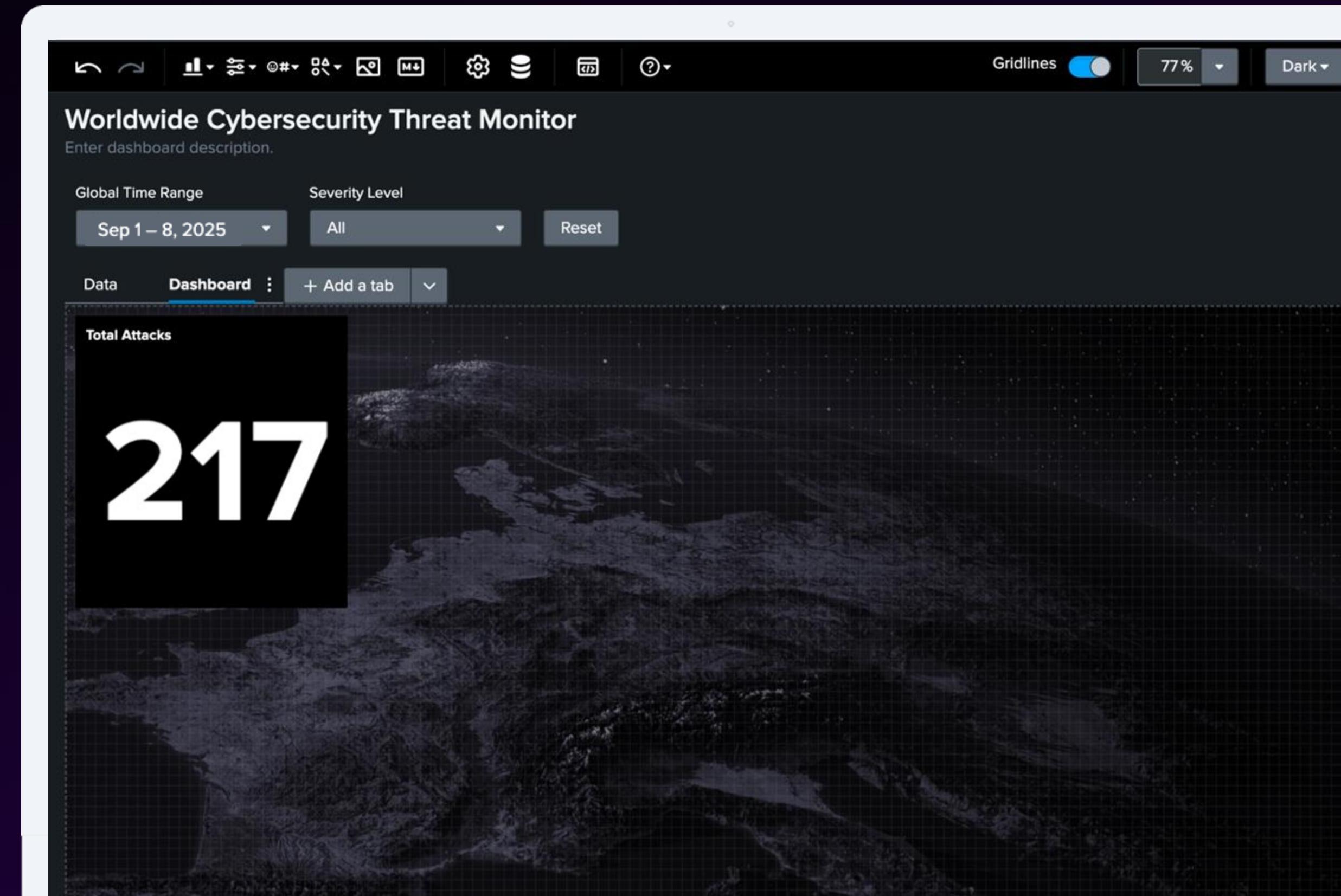
1. Make sure the single value **Configuration** panel is open (click the visualization if it isn't).
2. Under **General > Title** input “Total Attacks”.
3. You’re done! (But don’t forget to save).



Checkpoint

Your dashboard should now have a single value visualization!

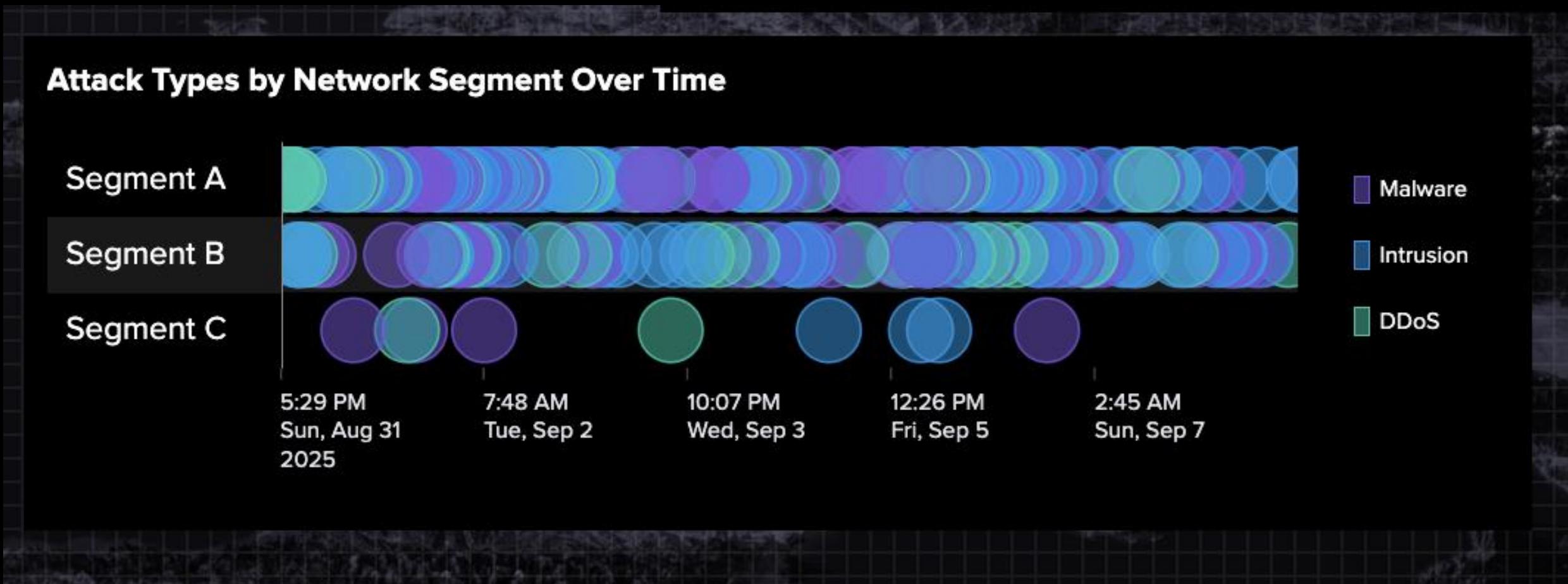
Make sure you save your dashboard!



6

Add a Timeline

Add a timeline visualization called “Attack Types by Network Segment Over Time” to show threat activity intervals and events over time by network segment and threat category.



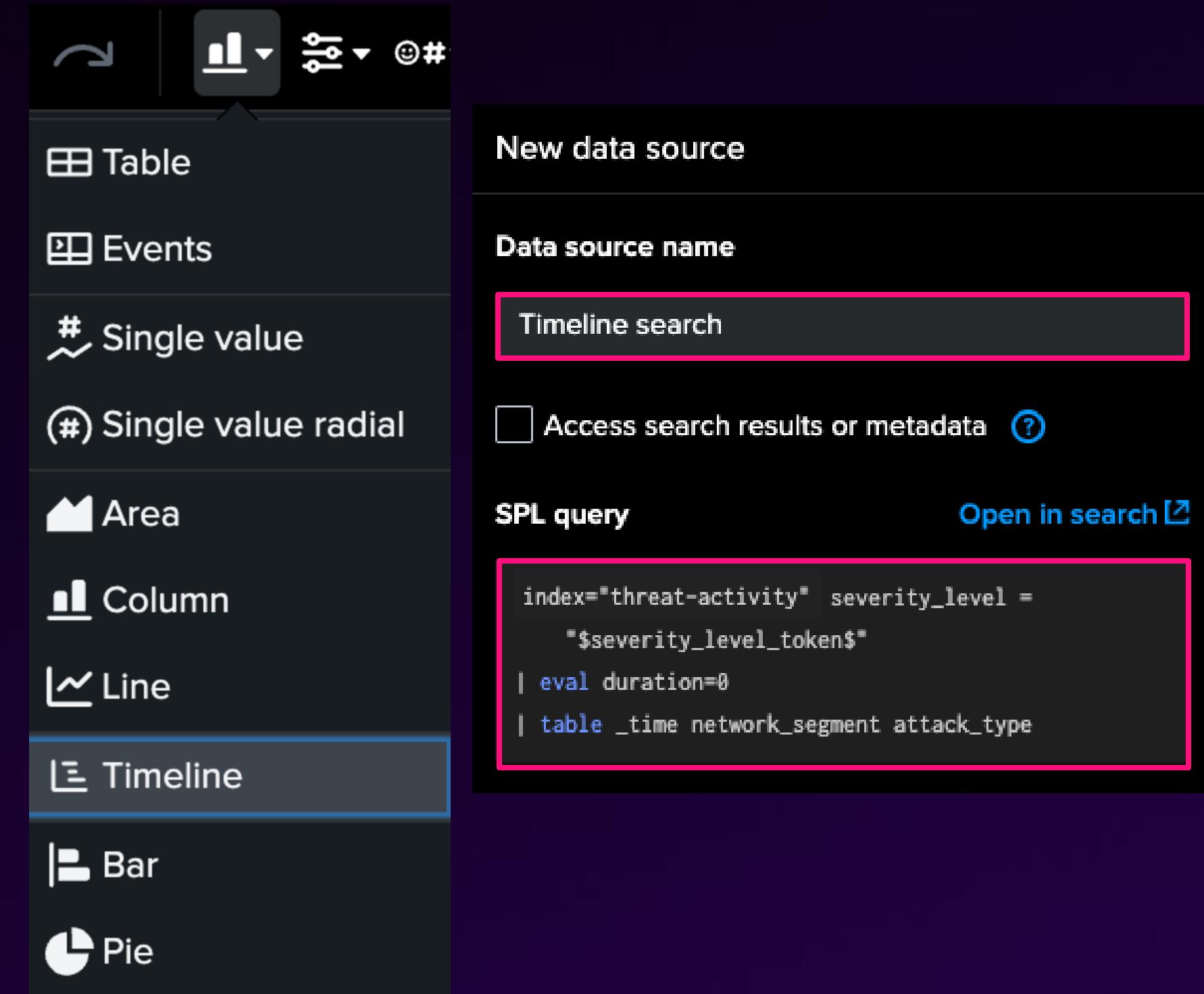
Create the Timeline

Step 1 of 2

Add chart and data source

1. From the Visualizations dropdown, select **Timeline**.
2. In the **Select data source** panel, click on **+ Create search**.
3. Enter "Timeline search" for the **Data source name**.
4. Put the following search in the **SPL query** input

```
index="threat-activity"
severity_level = "$severity_level_token$"
| eval duration=0
| table _time network_segment attack_type
```
5. Select **Apply and close** at the bottom of the panel.
Click **Save!**



Create the Timeline

Step 2 of 2

Name and styling

1. In **General > Title**, input “Attack Types by Network Segment Over Time”.
2. Under **Data configurations**, make sure the following settings are set:
 - a. X is set to **_time**
 - b. Y is **network_segment**
 - c. Duration is **_time**
 - d. Category is **attack_type**
3. Under **Legend display**, select **Right**.
4. Move and resize the timeline to fit below the single value visualization.
5. Click **Save!**

The screenshot shows the Splunk UI interface for configuring a visualization. The left side displays the configuration steps, and the right side shows the corresponding UI elements with pink boxes highlighting specific fields.

Step 1: Under **General > Title**, the title "Attack Types by Network Segment Over Time" is highlighted with a pink box.

Step 2: Under **Data configurations**, the following settings are highlighted with pink boxes:

- X: _time (time)
- Y: network_segment (string)
- Duration: _time (time)
- Category: attack_type (string)

Step 3: Under **Legend display**, the setting "Right" is highlighted with a pink box.

Checkpoint

Your dashboard should now have a timeline visualization!



New! Custom visualizations

Custom Visualizations

- One of the most exciting things for Dashboard Studio is the addition of the Custom Visualization framework.
- This allows anyone to create their own custom visualizations, using any frontend web framework, and use them in their dashboards.
- Most Custom Viz that already exist will also work in Dashboard Studio.
- Visit splunkbase.splunk.com and search for “viz”

Welcome to the new Splunkbase! To return to the old Splunkbase, [click here](#).

splunkbase Collections Apps

Find an app

Main Page / Apps

Discover Apps

BUILT BY

- Splunk
- Cisco
- Partners
- Community

PLATFORM

- SPLUNK
 - > PRODUCT
 - > VERSION
- SPLUNK SOAR
 - > PRODUCT
 - > VERSION

CATEGORY

- Artificial Intelligence

Showing 1-21 of 29 Results for **Viz**

Sort by

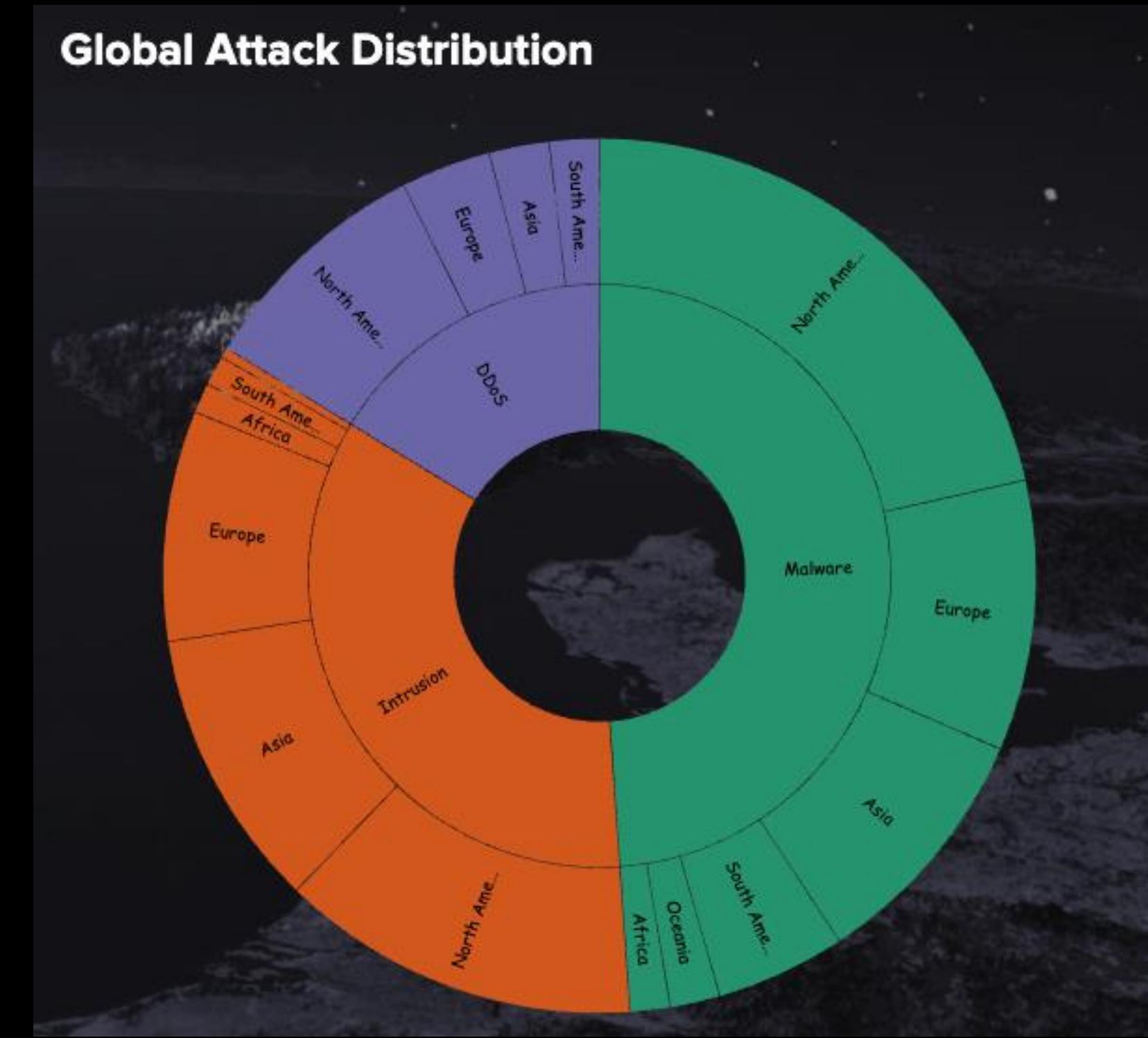
Sort By Best Match

App Name	Builder	Description	Platform	Rating
Flow Map Viz	By Chris Younger	A visualization used to show the volume of traffic across links. By default, this addon will normalise the traffic flows s...	Splunk Enterprise, Splunk Cloud	★★★★★ (15)
Network Diagram Viz	By Daniel Spavin	This app gives you a new way to visualize your data, allowing you to better communicate information in dashboard...	Splunk Enterprise	★★★★★ (23)
Event Timeline Viz	By Daniel Spavin	This app gives you a new way to visualize your data, allowing you to better communicate information in dashboard...	Splunk Enterprise, Splunk Cloud	★★★★★ (14)
Heat Map Viz	By Daniel Spavin	This app gives you a new way to visualize your data, allowing you to better communicate information in dashboard...	Splunk Enterprise, Splunk Cloud	★★★★★ (7)
Carousel Viz	By Daniel Spavin	This app gives you a new way to visualize your data, allowing you to better communicate information in dashboard...	Splunk Enterprise, Splunk Cloud	★★★★★ (6)
Animated Chart Viz	By Daniel Spavin	This app gives you a new way to visualize your data, allowing you to better communicate information in dashboard...	Splunk Enterprise, Splunk Cloud	★★★★★ (4)

7

Add a Sunburst Visualization

To show **Global Attack Distribution**, add a sunburst chart - a custom visualization - to see the **attack type distribution breakdown by location**.



Create a Sunburst Chart

Step 1 of 2

Add datasource

1. From the Visualizations dropdown, select **Sunburst** (it'll be all the way at the bottom).

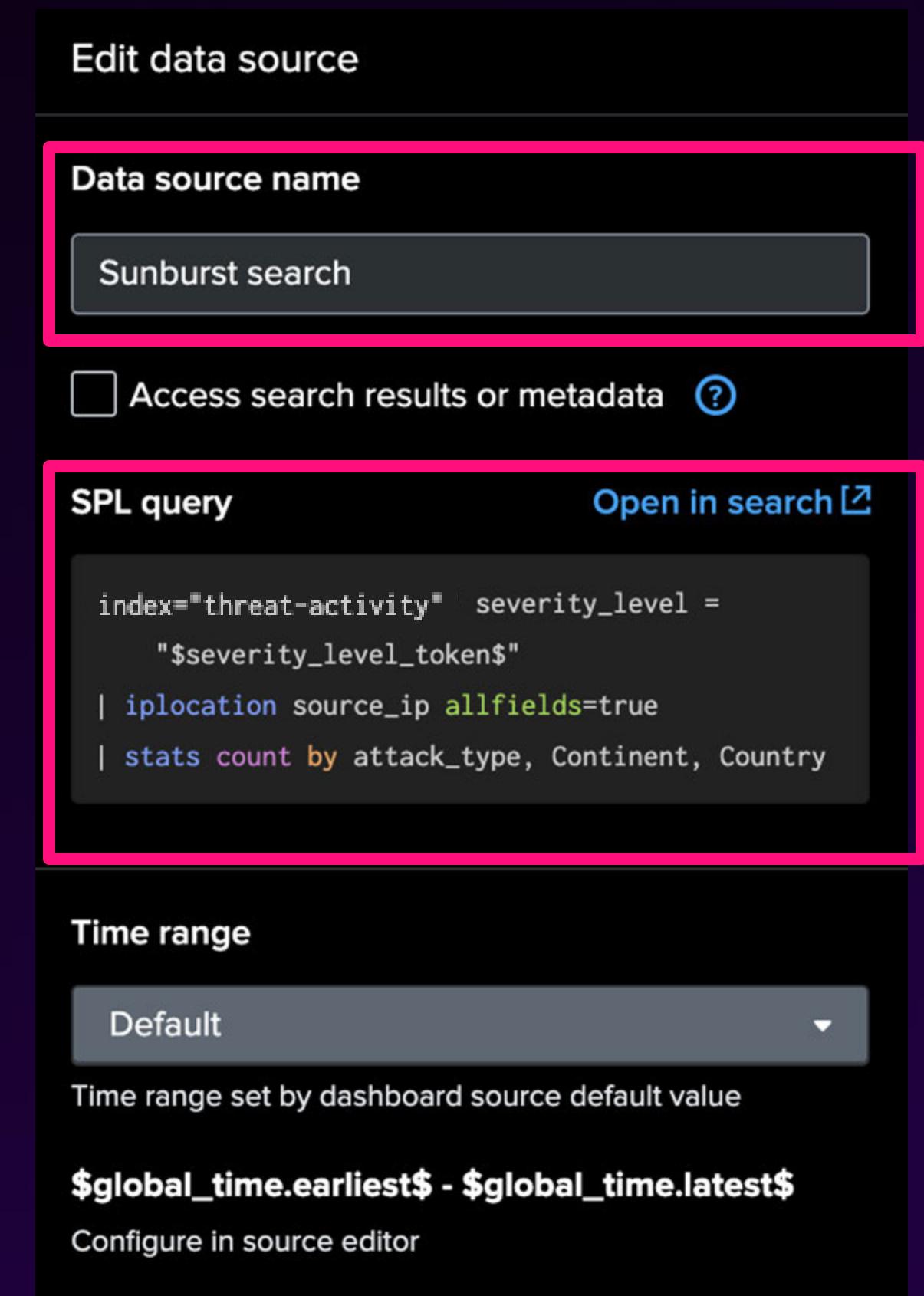
2. In the **Select data source** panel, click on **+ Create search**.

3. Enter "Sunburst search" for the **Data source name**.

4. Put the following search in the **SPL query** input:

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

5. Select **Apply** and **close** at the bottom of the panel.



Create a Sunburst Chart

Step 2 of 2

Format Chart

1. In General > Title, input “Global Attack Distribution”.
2. In the Sunburst: General panel, set the following:
 - a. Click action to Zoom in
 - b. Color set to Dark
 - c. Set color by to Base ring name
 - d. Breadcrumbs to Hide
3. Move and resize so it fits next to the single value visualization.

For this visualization, several of the changes/interactions will only show (or even be possible) in View mode.



Configuration

✓ Sunburst: General

Click action

Zoom in

Color set

Dark

Set color by

Base ring name

Color overrides

Breadcrumbs

Show Hide

Labels

Show Hide

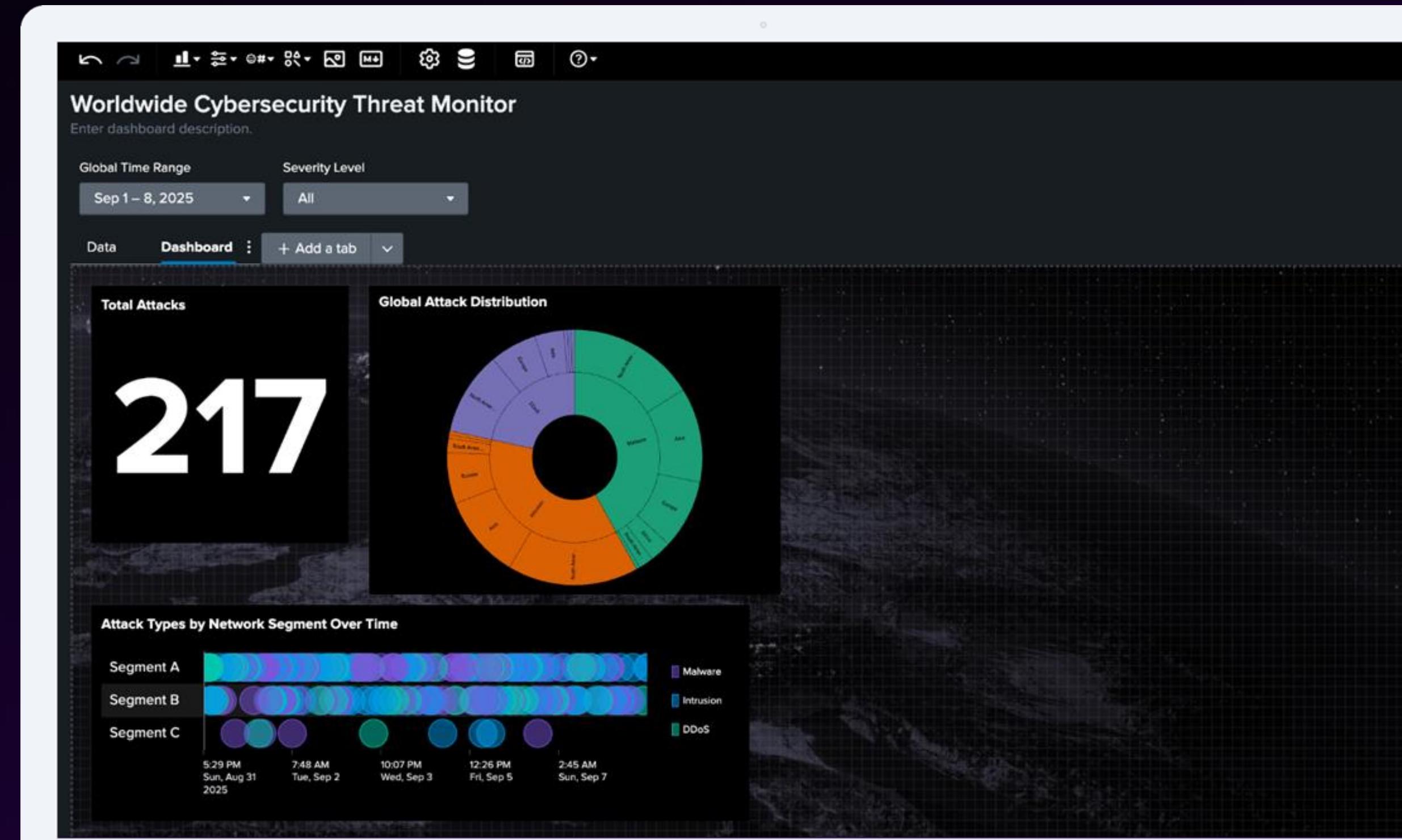
Labels

X

This panel shows the configuration options for the sunburst chart. The "Click action" dropdown is set to "Zoom in". The "Color set" dropdown is set to "Dark". The "Set color by" dropdown is highlighted with a red box and set to "Base ring name". The "Breadcrumbs" section is also highlighted with a red box and has "Show" selected. The "Labels" section has both "Show" and "Hide" buttons available.

Checkpoint

Your dashboard now has an interactive sunburst chart!



8

Map + Dynamic Coloring

Add a “Geographic Distribution of Source IPs” map to show **geographic distribution** of threats. Configure **dynamic coloring** to easily identify locations with high threat levels



Create the Map

Step 1 of 4

Add visualization and data source

1. From the Visualizations dropdown, select **Map**.
2. In the **Select data sources** panel, click on **+ Create search**.
3. Enter "Map search" for the **Data source name**.
4. Put the following search in the **SPL query** input:

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

The screenshot shows a Splunk dashboard titled "Worldwide Cybersecurity Threat Monitor". The dashboard includes a world map, a large numerical visualization, and a donut chart. On the right side, there is a configuration panel for a new data source. The "Data source name" field is set to "Map search". The "SPL query" field contains the following search command, which is highlighted with a red box:

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

The configuration panel also includes sections for "Time range" (set to "Default") and "Event Sampling" (set to "t: 1"). At the bottom, there are "Cancel" and "Apply and close" buttons.

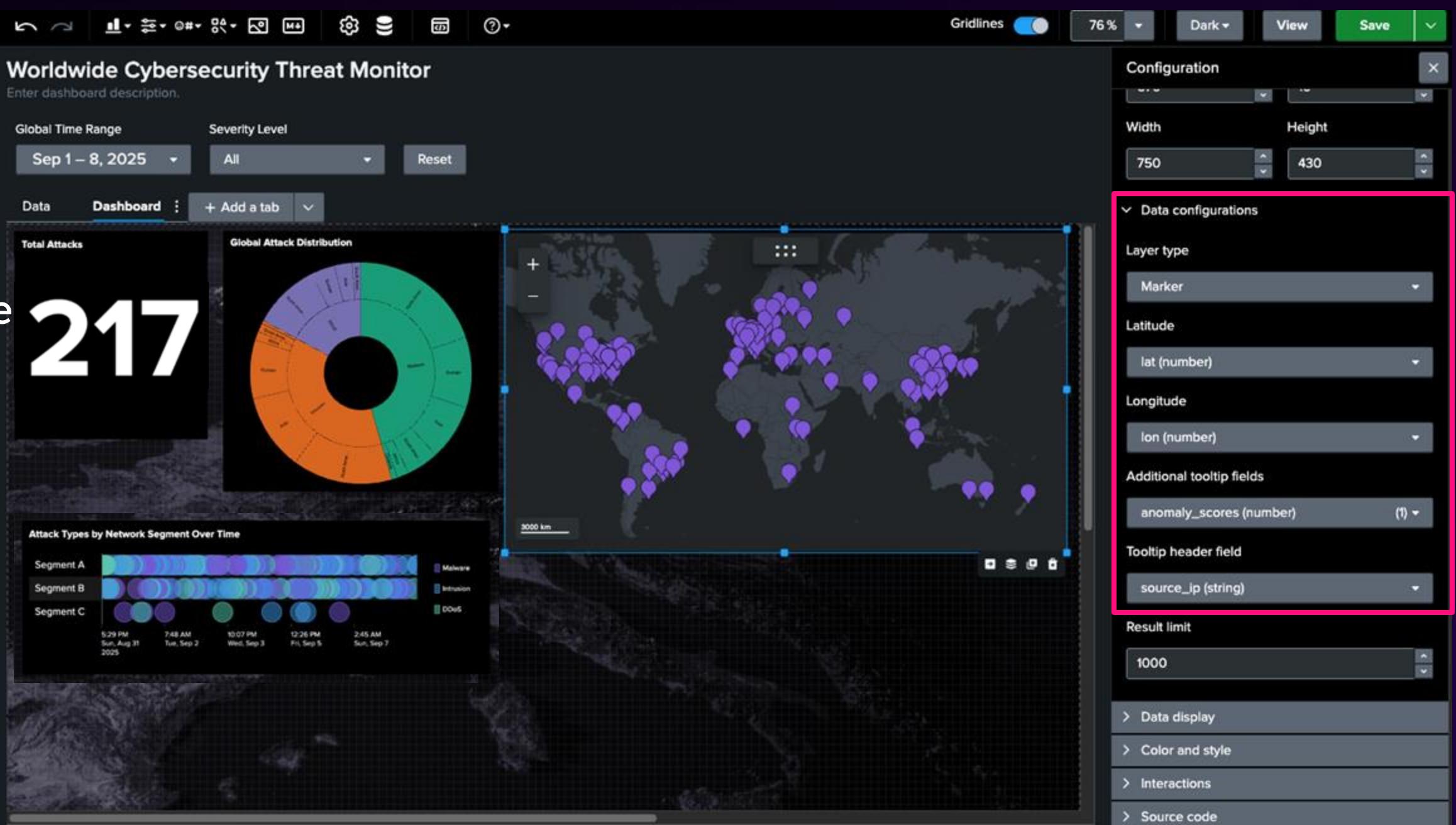
5. Select **Apply and close**.

Create the Map

Step 2 of 4 Set up data configurations

In the Map's Configuration panel, find the **Data configurations** section:

1. For **Layer type** select **Marker**.
2. For **Latitude** select **lat (number)**.
3. For **Longitude** select **lon (number)**.
4. For **Additional tooltip fields** select **anomaly_scores (number)**.
5. For **Tooltip header field** select **source_ip (string)**.



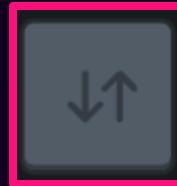
Create the Map

Step 3 of 4

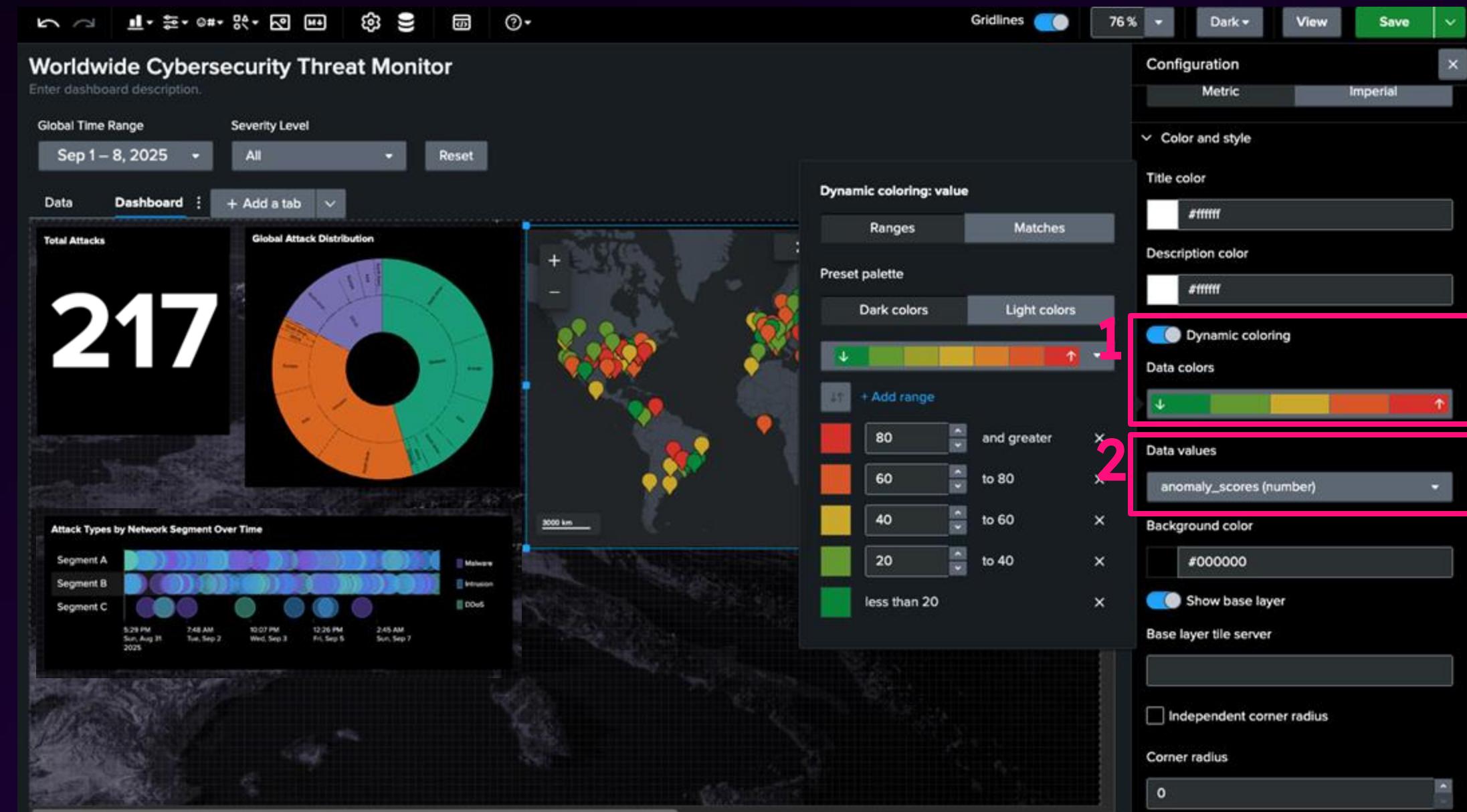
Set up dynamic coloring

In the **Color and style** panel:

1. Toggle on **Dynamic coloring**.
2. Click on the **Data colors** and switch the direction of the color palette by clicking this icon:



1. Under **Data values** select **anomaly_scores (number)**.



Create the Map

Step 4 of 4

Final touches (title and position)

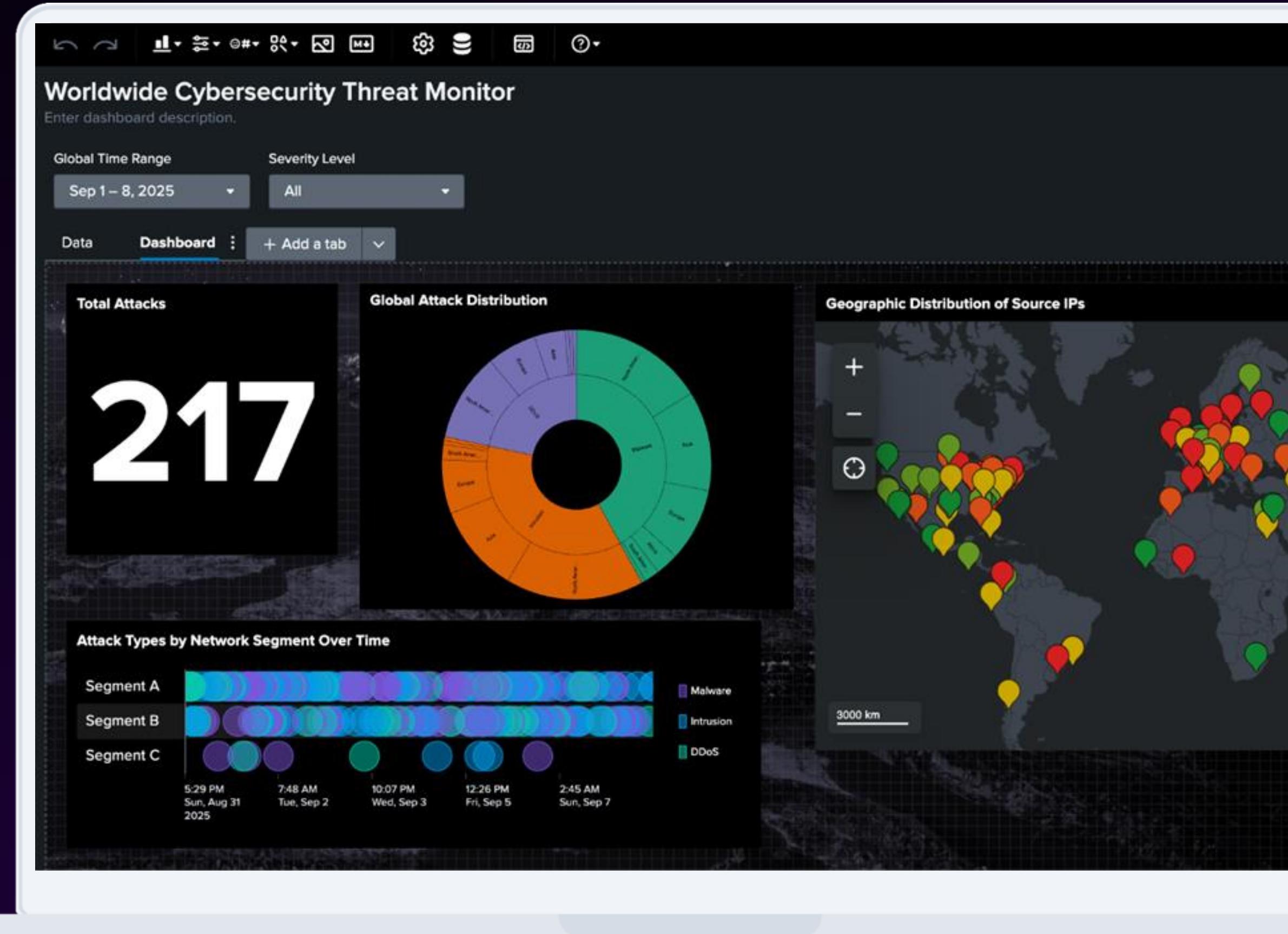
1. Under General > Title put “Geographic Distribution of Source IPs”.
2. Drag and resize the map to fit in the top right side of the canvas.



Checkpoint

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

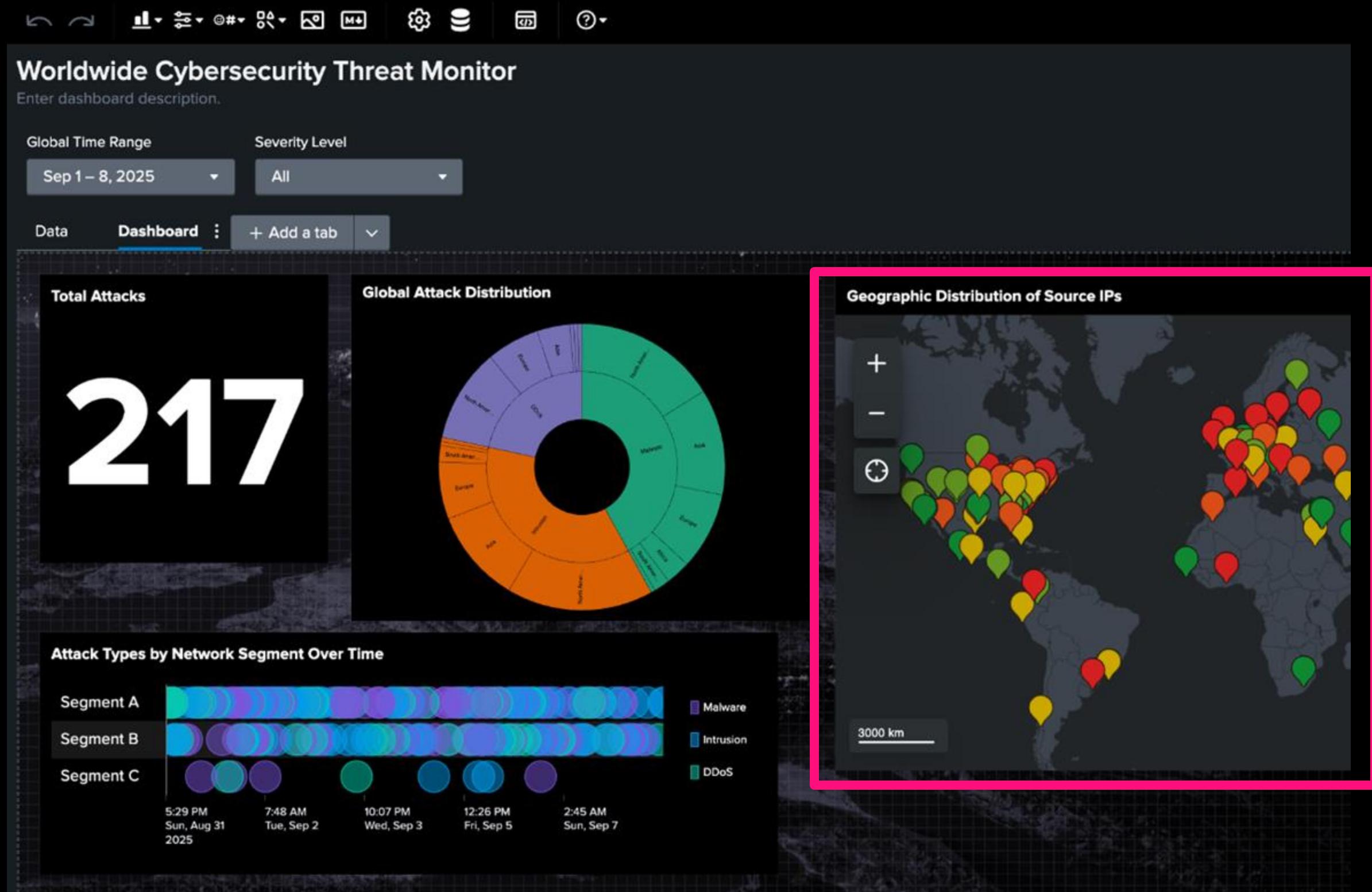
Make sure to save your dashboard periodically, so you don't lose any work!



Interact with Tokens

9

Configure the **Set tokens interaction** option on the **Geographic Distribution of Source IPs** map for more **interactivity** and **drilldown** capabilities on specific IP addresses

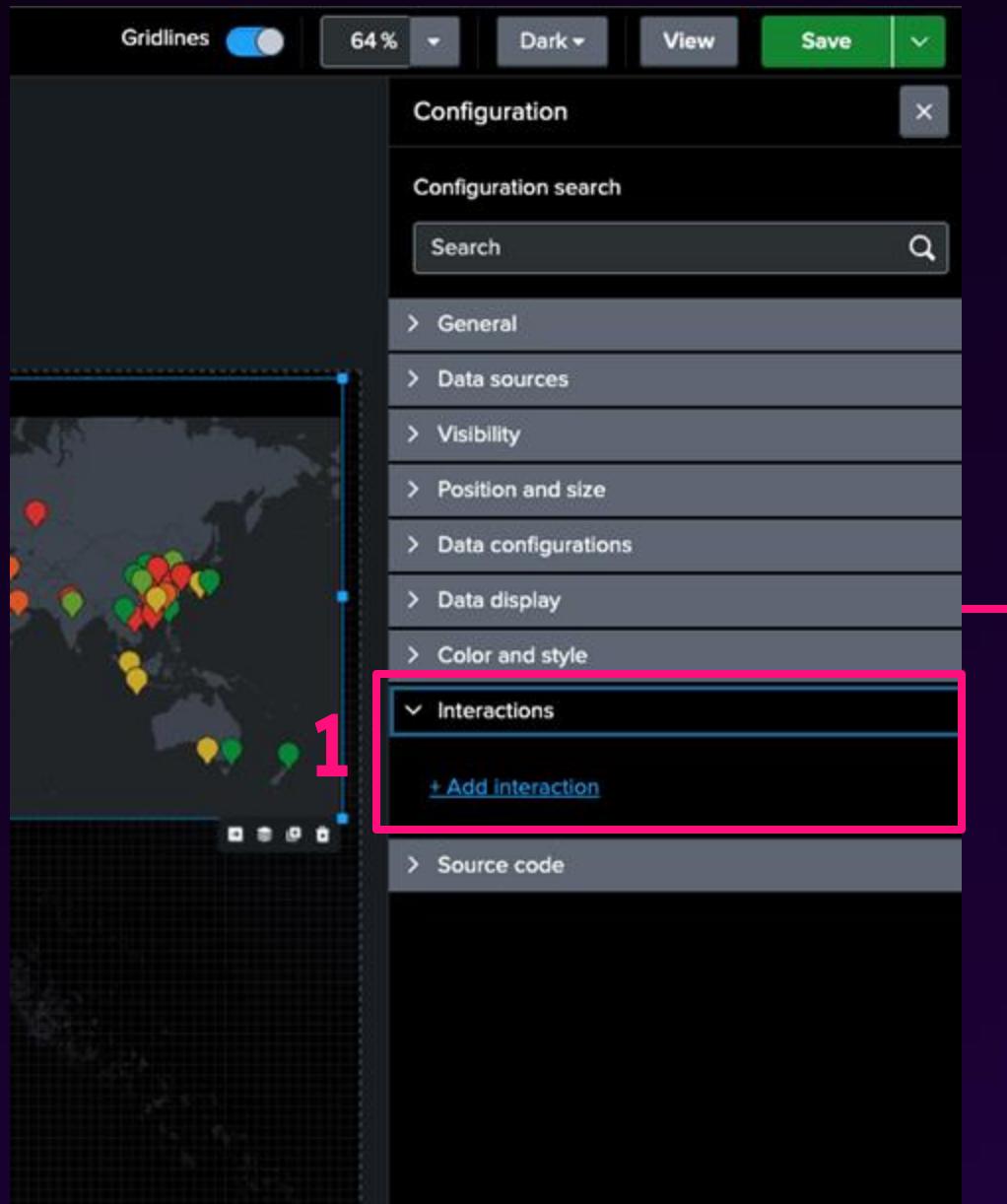


Map Interactivity

Step 1 of 2

Map marker interaction

1. Click on your map visualization to open its **Configuration** panel.
2. Scroll down to **Interactions** and select **+ Add interaction**.
3. Under **On click** select **Set tokens**:
 - a. For **Token name**, enter “map_value”.
 - b. For **Token value**, enter “row.source_ip.value”.
4. Select **Apply** at the bottom of the panel.



2

On click

Set tokens

Tokens are used to configure interactivity in the dashboard.
For example: host = row.host.value

Set token (map_value)

Use predefined token

A predefined token captures information when a user clicks different visualization elements.

Token name ? Token value
map_value = row.source_ip.value

Default value ?
Enter a default value

+ Set another token

3

This panel shows the configuration for the 'Set tokens' interaction. It includes fields for 'Token name' (set to 'map_value') and 'Token value' (set to 'row.source_ip.value'). There are also fields for 'Default value' and a button to '+ Set another token'.

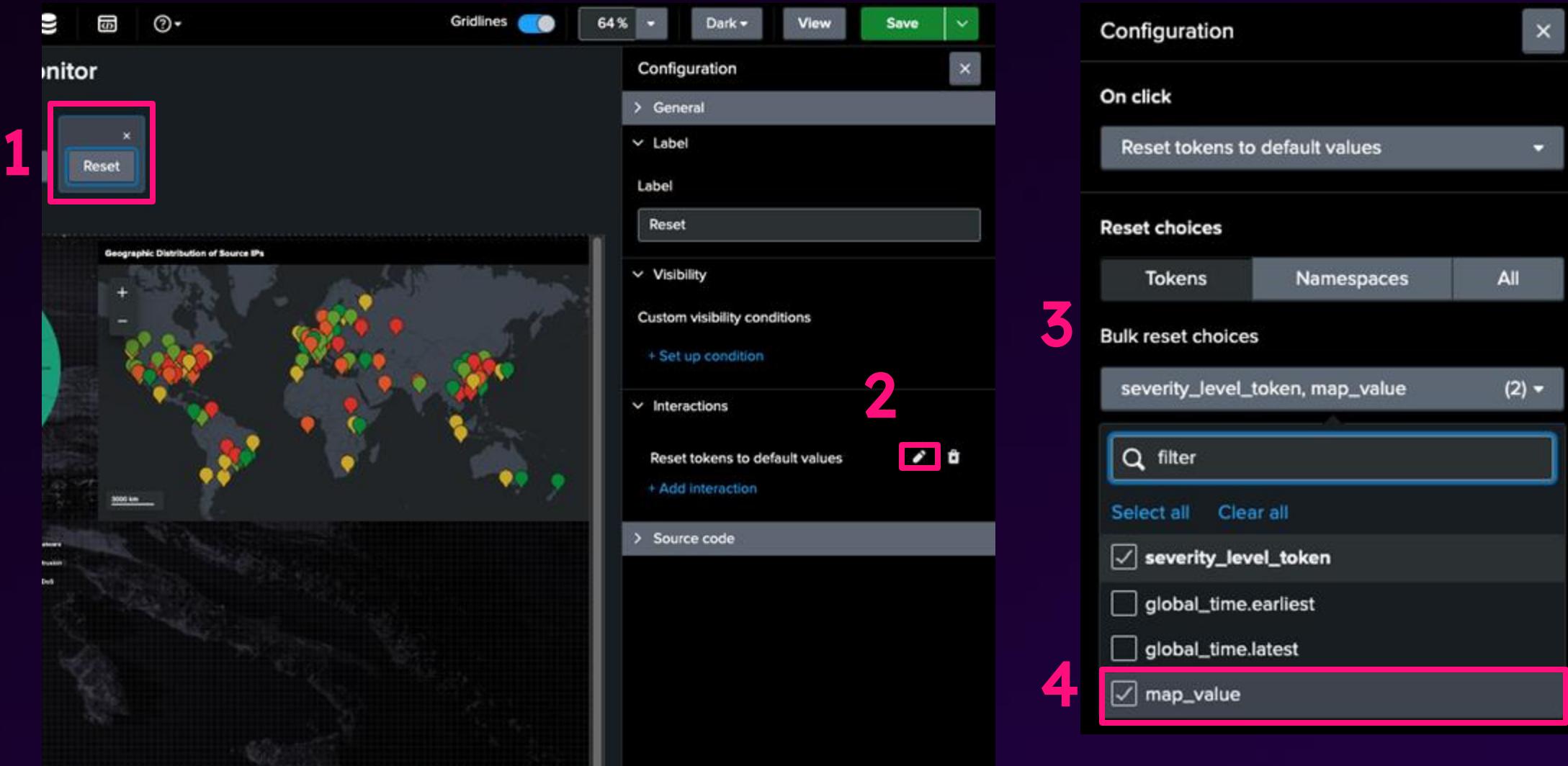
(OPTIONAL)

Token Resetting

Step 2 of 2

Reset button interaction

1. Click on our **Reset** button above the canvas to open its **Configuration** panel.
2. Under **Interactions**, click the pencil icon 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.



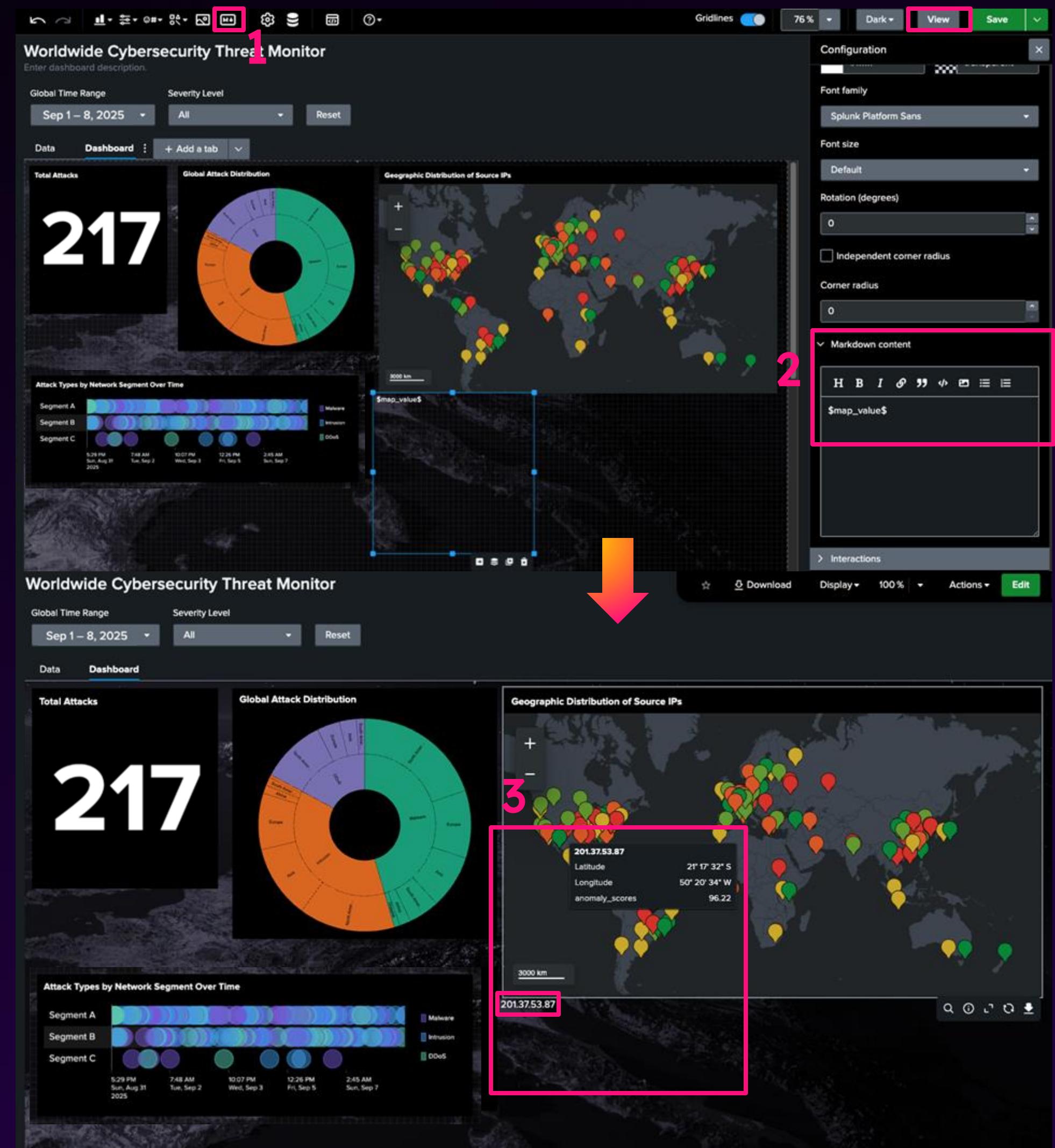
(OPTIONAL)

Checkpoint

Optional step

Review set up token interaction

1. From the menu bar, add a **Markdown** component.
2. Under **Markdown content** put “\$map_value\$” (quotation marks not necessary).
3. In the top right of the page, select **View**.
4. Click on a marker on the map and you should see the Markdown value change.
5. Click the **Reset** button and it should go back to displaying only \$map_value\$.
6. You can now delete Markdown component by clicking it and then the trash can icon in the bottom right corner.



Conditionally Visible Tables

10

For more **interactivity** and **drilldown** capabilities, create a conditionally visible table that appears and displays relevant data when you select a data point in the **Geographic Distribution of Source IPs** map



Create the Table

Step 1 of 4

Add visualization and data source

1. From the Visualizations dropdown, select **Table**.
2. In the Select data sources panel, click on **+ Create search**.
3. Enter "Map Table Search" for the Data source name.
4. Put the following search in the SPL Query input:

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

5. Select **Apply and close**. Click **Save**!

If your table is not displaying data, it's likely because there is no map value selected. The next slide will show you how to test it out.

The screenshot shows a Splunk dashboard titled "Worldwide Cybersecurity Threat Monitor". The dashboard features several visualizations: a large number "217" representing total attacks, a donut chart showing global attack distribution across categories like Malware, Intrusion, and DDoS, and a world map showing the geographic distribution of source IPs with colored dots indicating severity levels. Below these is a timeline visualization showing attack types by network segment over time, with segments A, B, and C and specific timestamps from August 31 to September 7, 2025. On the right side of the interface, there is a sidebar for creating a new data source. The "Data source name" field is set to "Map table search" and is highlighted with a pink box. The "SPL query" field contains the following search command:

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

The sidebar also includes sections for "Time range" (set to "Default"), "Event Sampling" (set to 1:1), and "Usage" (showing 1 visualization and 0 inputs). At the bottom of the sidebar, there are "Cancel" and "Apply and close" buttons, with "Apply and close" being the active button.

Set the Map Value Token

Step 2 of 4

Preview table interactivity

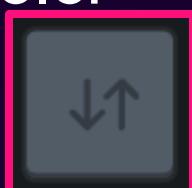
1. On the upper right, click **Save** and then **View**.
2. Click on any marker on the map. The new table should update.
3. To get back to building, select **Edit** from the upper right corner (you're now back in edit mode).

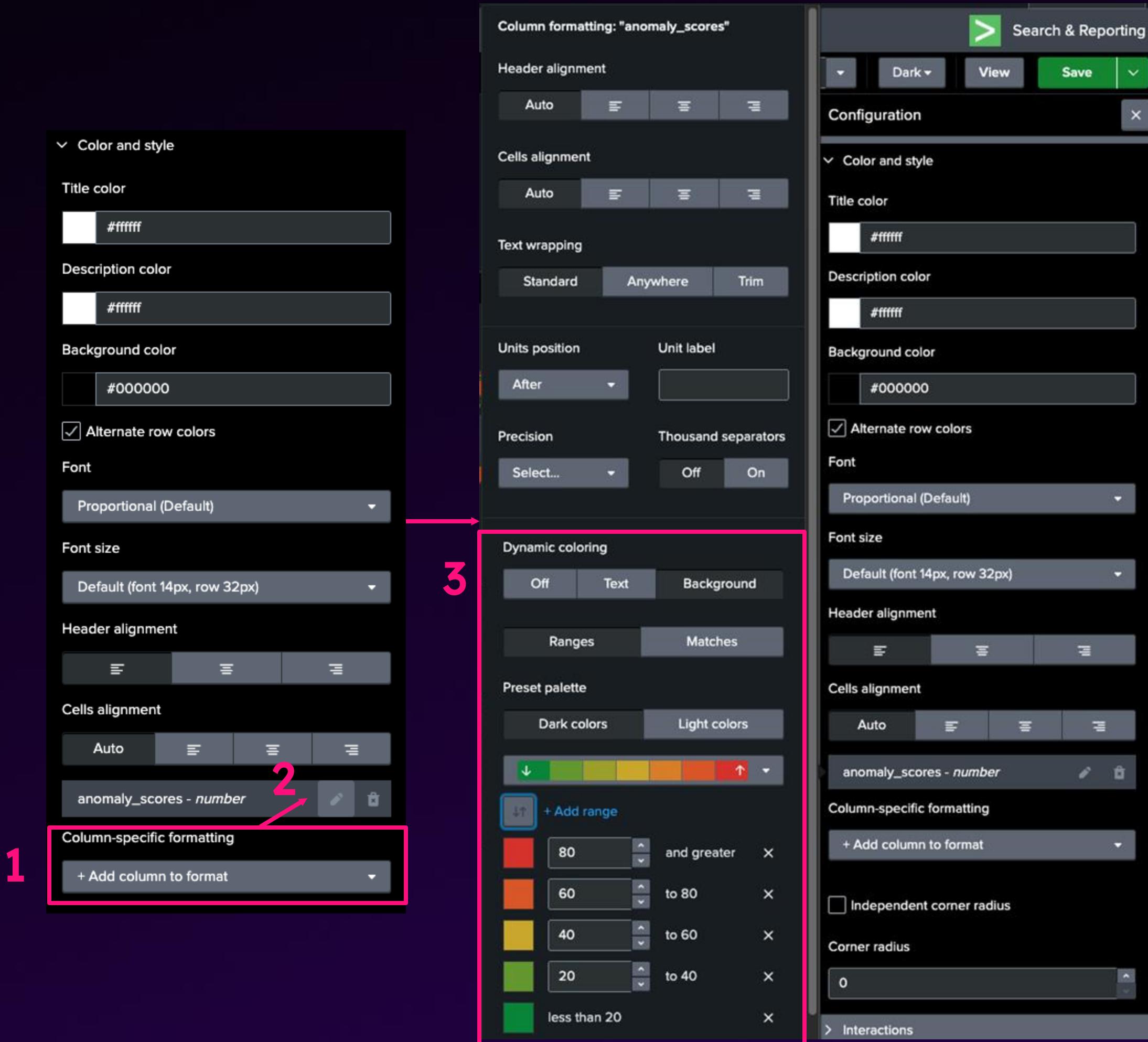


Create the Table

Step 3 of 4

Set up dynamic coloring

1. Click the new Table visualization to open its Configuration panel.
2. Find the Color and style section:
 - a. Under Column-specific formatting find **anomaly_scores - number** and click the pencil icon to edit.
 - b. In the pop-over, under Dynamic coloring select **Background**.
 - c. Switch the direction of the color palette by clicking this icon: 



Column formatting: "anomaly_scores"

Header alignment

Cells alignment

Text wrapping

Units position Unit label

Precision Thousand separators

Dynamic coloring

Off Text Background

Ranges Matches

Preset palette

Dark colors Light colors

+ Add range

Value	Condition	Remove
80	and greater	X
60	to 80	X
40	to 60	X
20	to 40	X
less than 20		X

anomaly_scores - number

Column-specific formatting

+ Add column to format

Independent corner radius

Corner radius

0

Interactions

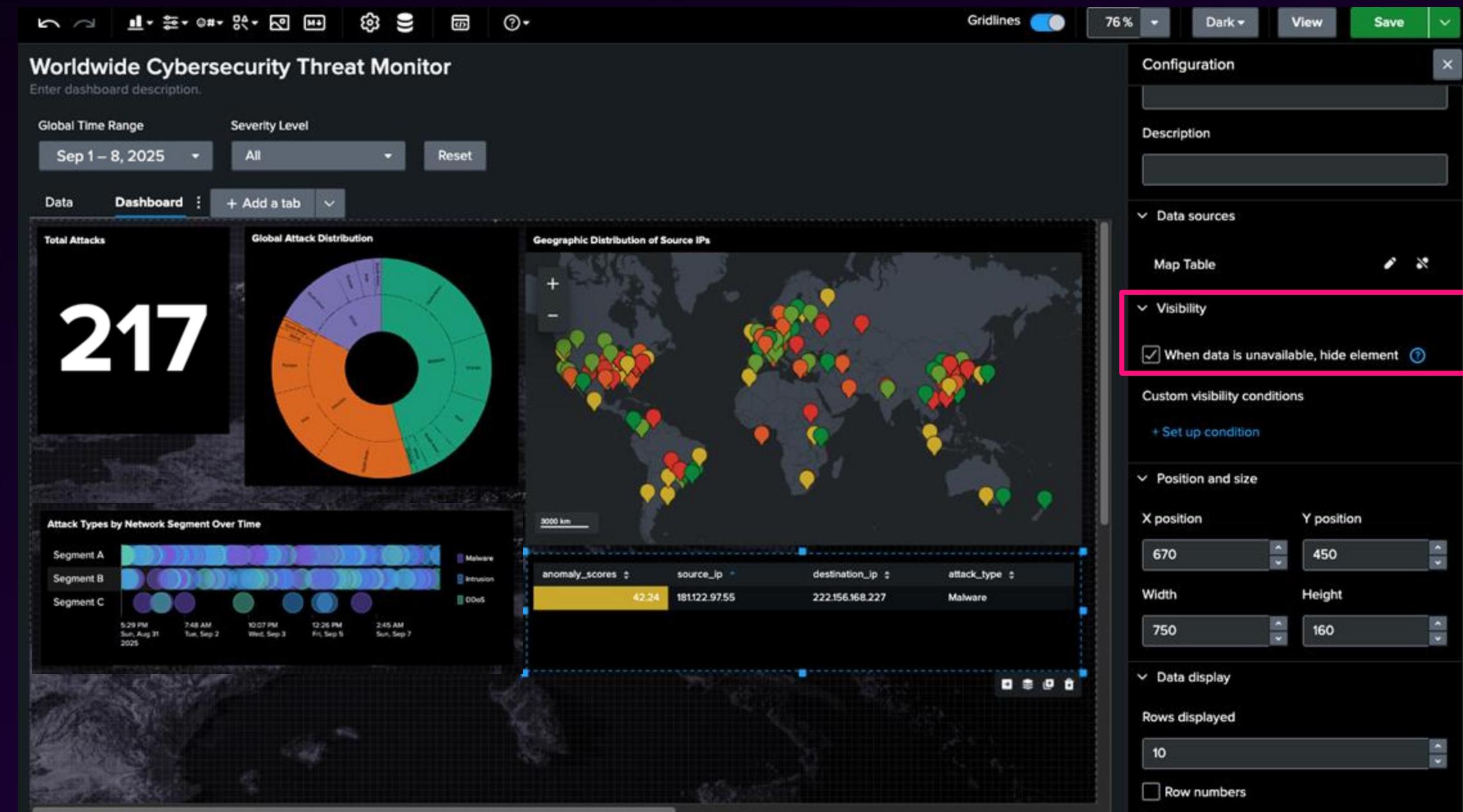
Create the Table

Step 4 of 4

Set up conditional visibility

Let's hide the panel when the map_value token is not set.

1. Click the new table to open its Configuration panel.
2. Scroll to the Visibility section.
3. Check When data is unavailable, hide element (you might have to open the section to see this option).
4. Click Save!



Checkpoint

Your dashboard should now look like this.

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

Make sure to save your dashboard periodically, so you don't lose any work!



Improve Dashboard Styling

11

Apply a transparent background to visualizations for a more **visually appealing and attractive** dashboard



(OPTIONAL)

Transparent Background

Step 1 of 1

Transparency for all panels

For each visualization:

1. Under **Color and style**, select **transparent** as the **Background color**.

You can do this by selecting the checkerboard icon from the color palette or by typing “transparent” into the color input field.

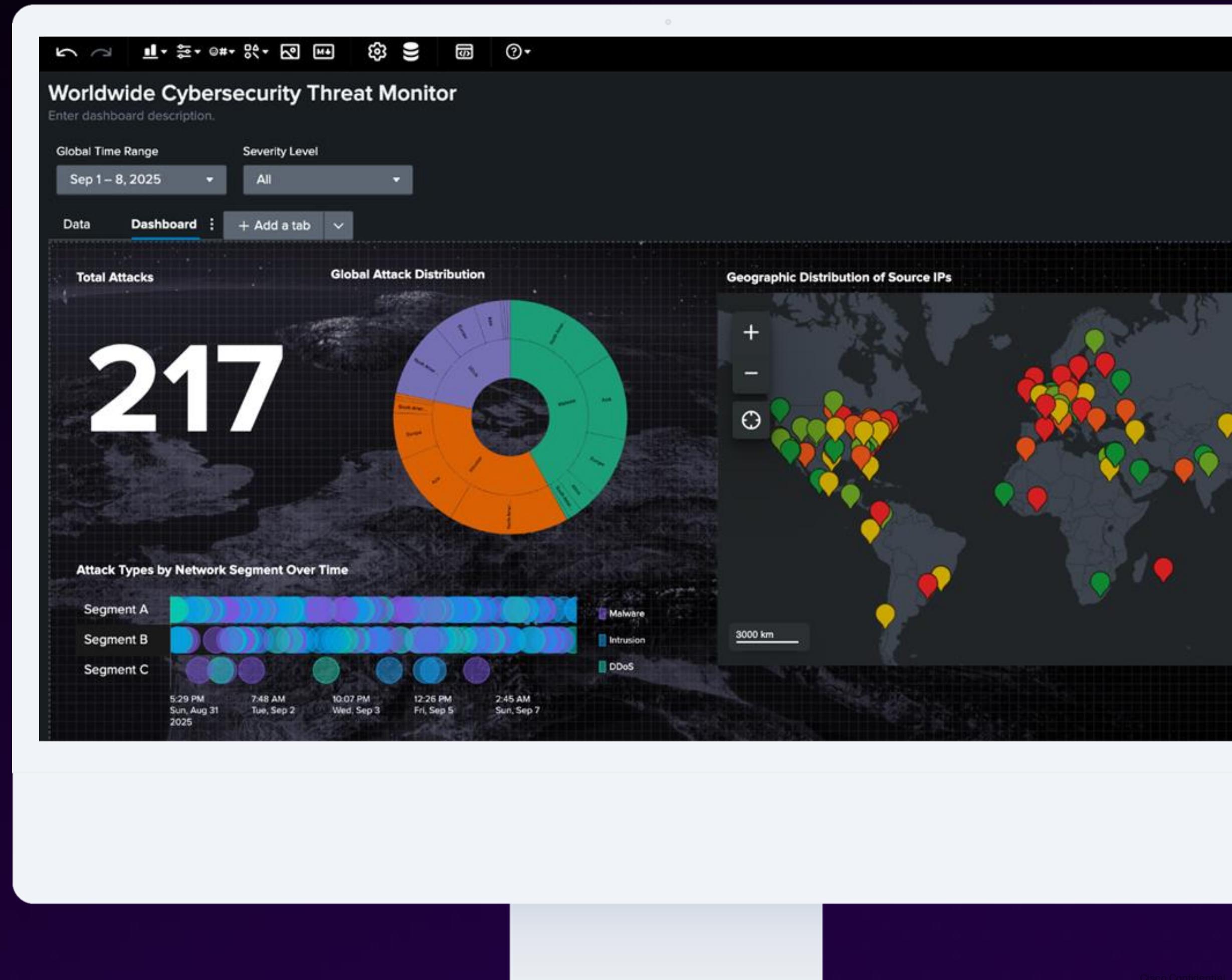
The screenshot shows a Splunk dashboard titled "Worldwide Cybersecurity Threat Monitor". The dashboard includes three main visualizations: a large number "217" representing total attacks, a sunburst chart showing global attack distribution by source and type, and a world map of source IP locations. On the right, the "Configuration" panel is open for the first visualization. A pink box highlights the "Background color" section, which shows a color palette with a checkerboard icon labeled "transparent". Another pink box highlights the color input field, which also displays "transparent". Other configuration options visible include "Title color" (#ffffff), "Description color" (#ffffff), and "Dynamic elements" settings for "Select...", "Major value", and "Trend value".

Final Checkpoint

Congratulations! You have learned the fundamentals of:

- ✓ Creating a dashboard and visualizations
- ✓ Setting up interactivity
- ✓ Layout and styling

As always, make sure you save your dashboard!



Tip: Optimizing Data Sources

Data Sources in Dashboard Studio

Data sources are their **own objects** in Dashboard Studio. This means:

- We can manage them in one place.
- We can manage them separately from inputs or charts.

Data sources are associated with other options via a **unique identifier**. This means:

- We can reuse data sources for multiple objects and chain searches.
- We can make updates in one place and it will be applied everywhere the data source is used.

Dashboard Studio supports **3** data source types:

- Ad-hoc searches
- Saved searches
- Chain searches

About Chain Searches

Chain searches allow you to build off of existing data sources in your dashboard.

Instead of running **2 separate searches**:

1. index="threat-activity" severity_level = "\$severity_level_token\$" | eval duration=0
2. index="threat-activity" severity_level = "\$severity_level_token\$" | eval duration=0 | iplocation source_ip
allfields=true | stats count by attack_type, Continent, Country

We can run the **shared part of the searches once**:

```
index="threat-activity" severity_level = "$severity_level_token$" | eval duration=0
```

And run a chain search to do further evaluations on the **results of this base search**:

```
| eval duration=0 | iplocation source_ip allfields=true | stats count by attack_type, Continent, Country
```

Sharing

Dashboard Sharing

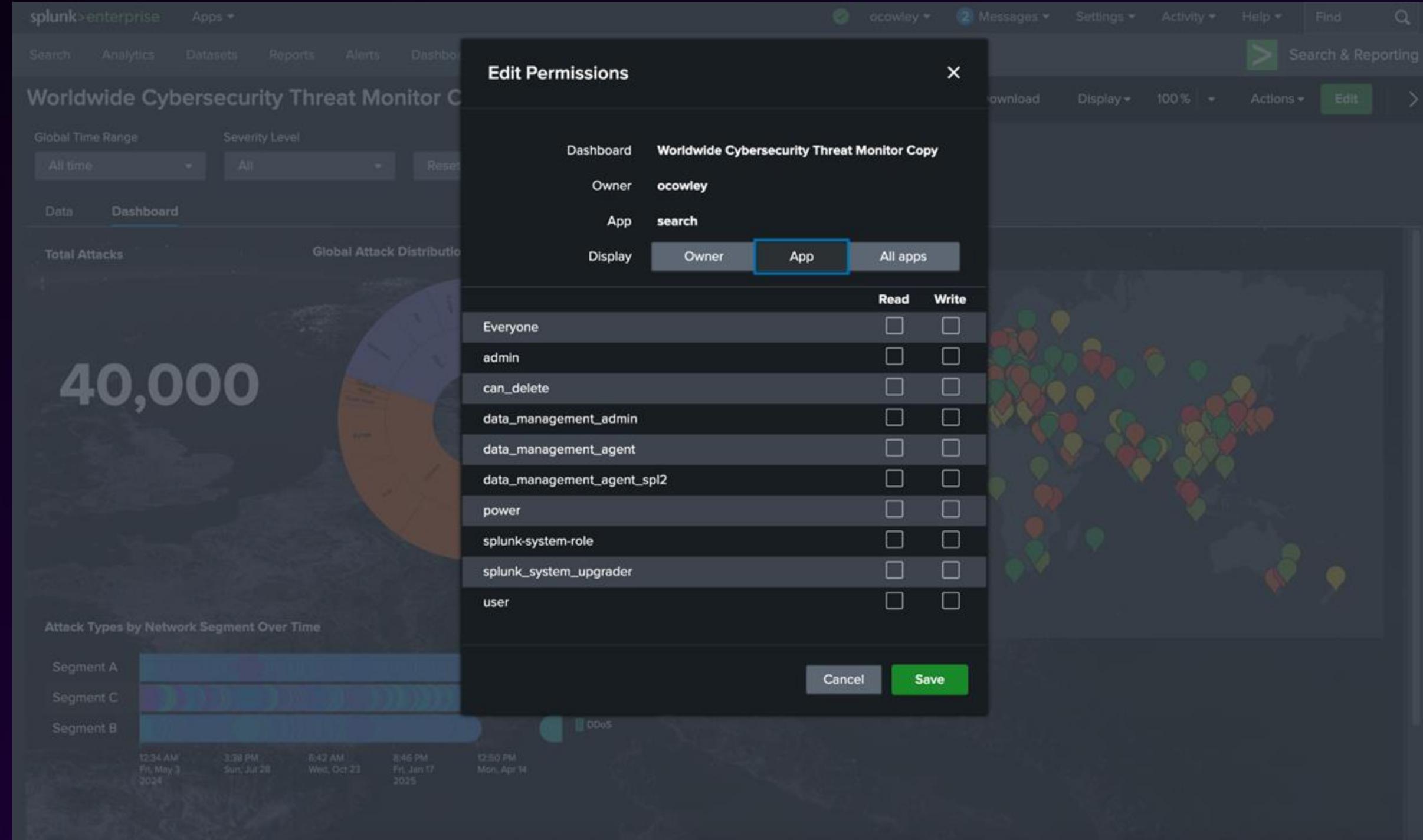
Once the dashboard is ready, it's time to decide how to share it with others. The main choices are:

- Directly access the dashboard (for users with a login)
 - Ensure the dashboard permissions are set to your target audience's role
 - Share the View mode URL
- Scheduled email export (for anyone with an email address)
 - Send the dashboard as PDF or PNG, via email, on a regularly scheduled basis
 - (This instance doesn't include scheduled export.)
- Publish the dashboard (for anyone!)
 - You can publish a Dashboard Studio dashboard so that anyone with the custom link can view it.

Direct Access

In View mode, navigate to Actions > Edit permissions.

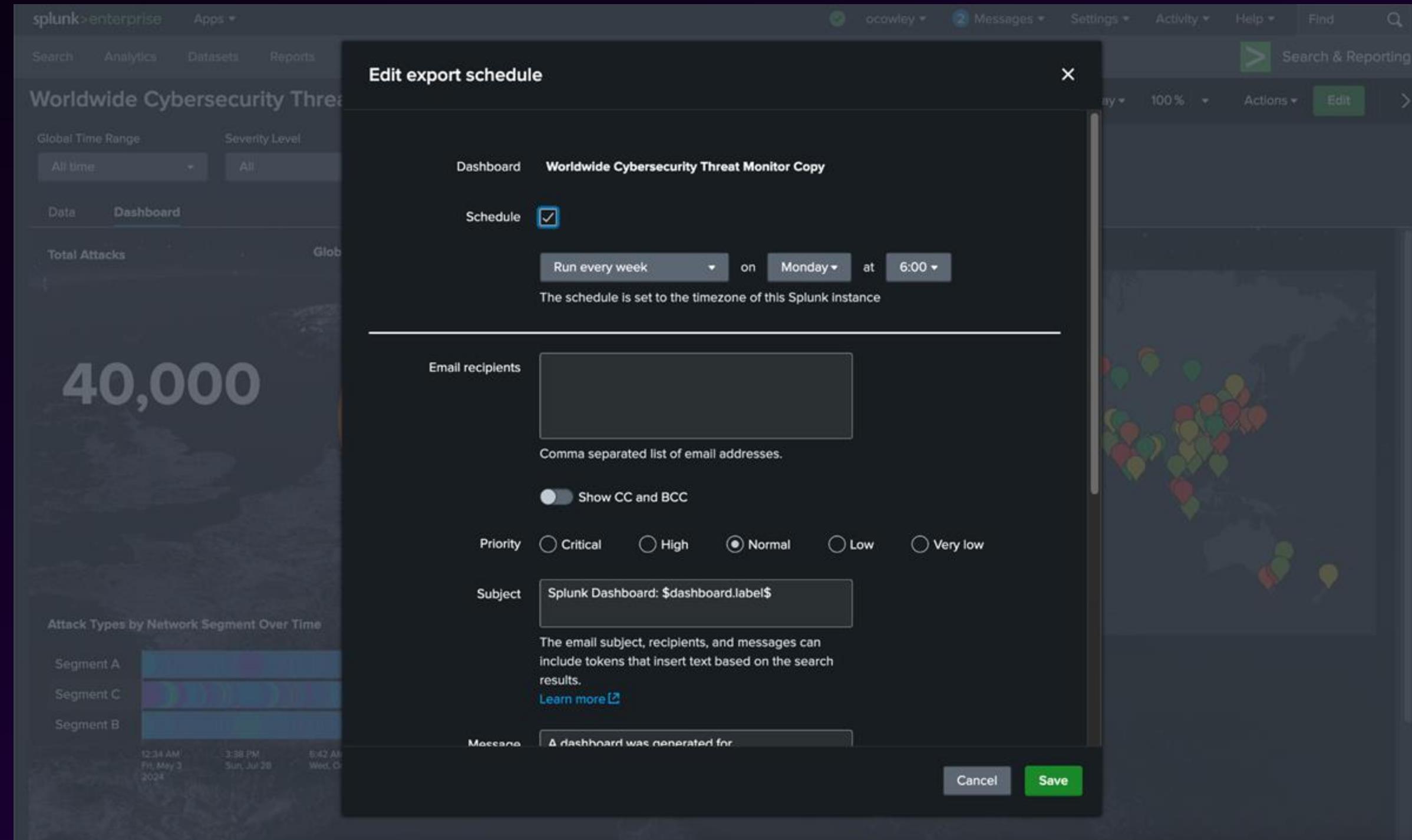
This pop-up allows you to grant read and write permissions based on users' roles, as well as if the dashboard can be accessed from other apps.



Scheduled Export

In View mode, navigate to Actions > Schedule export.

This pop-up allows you to set a schedule for when the dashboard will be snapshotted and emailed out to the list of email recipients.

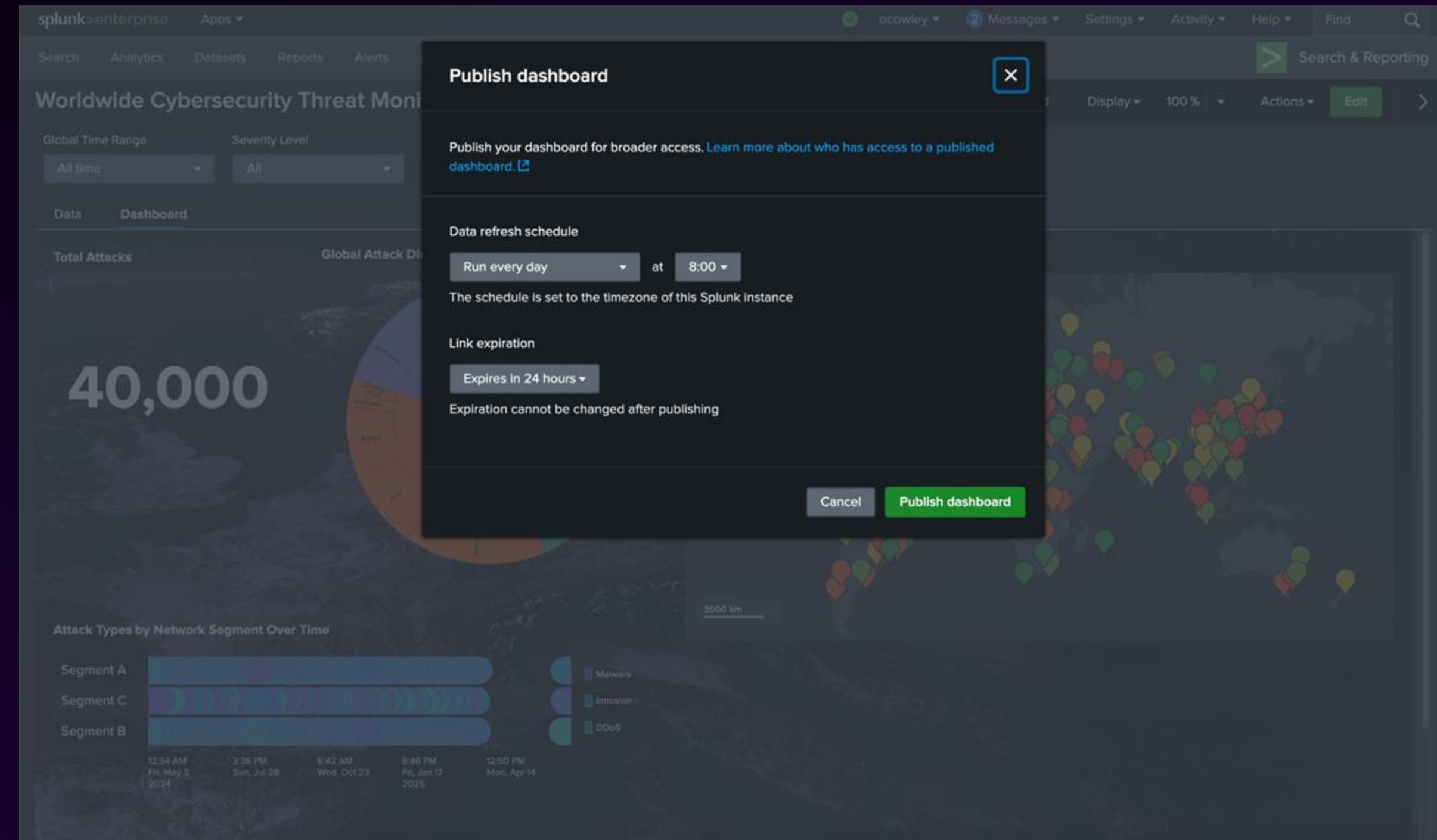


Publish a Dashboard

In **View** mode, navigate to **Actions > Publish dashboard**.

This pop-up allows you to set the schedule for the dashboard to run all of its searches and populate with data, as well as when the published link should expire.

After publishing, anyone with the link will be able to view the dashboard.

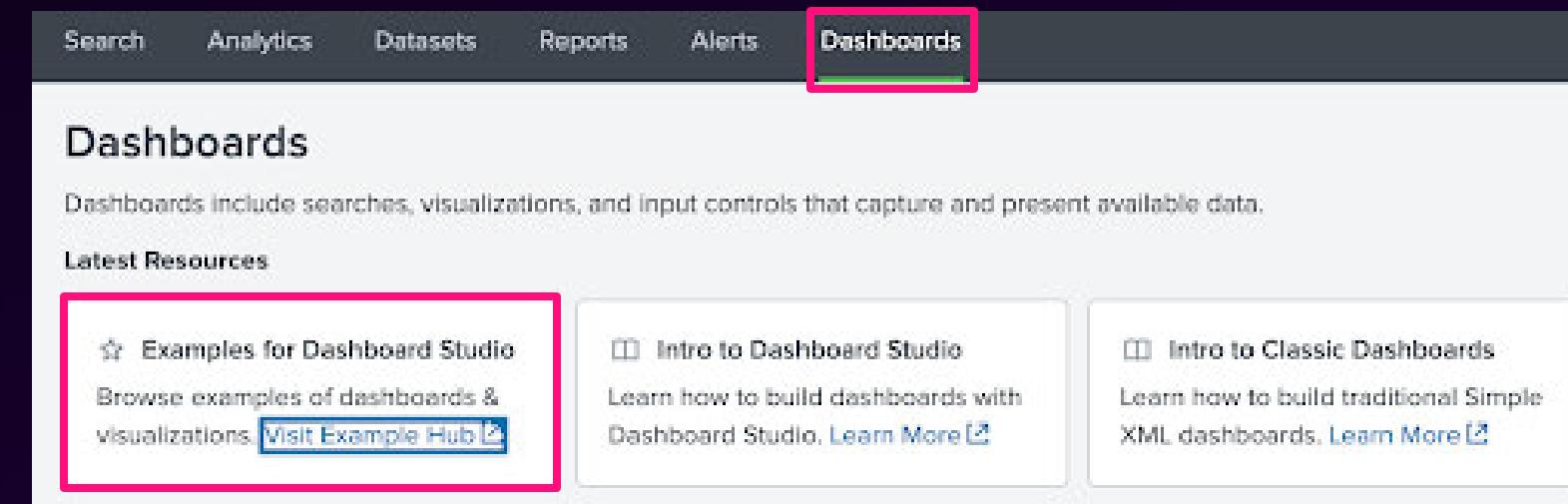


Wrap up

Additional Resources

Learn more about Dashboard Studio

- [Documentation](#)
- [#dashboard_studio user group in Slack](#)
- [EDU courses](#)
- [Splunk Dashboard Studio Examples Hub](#)



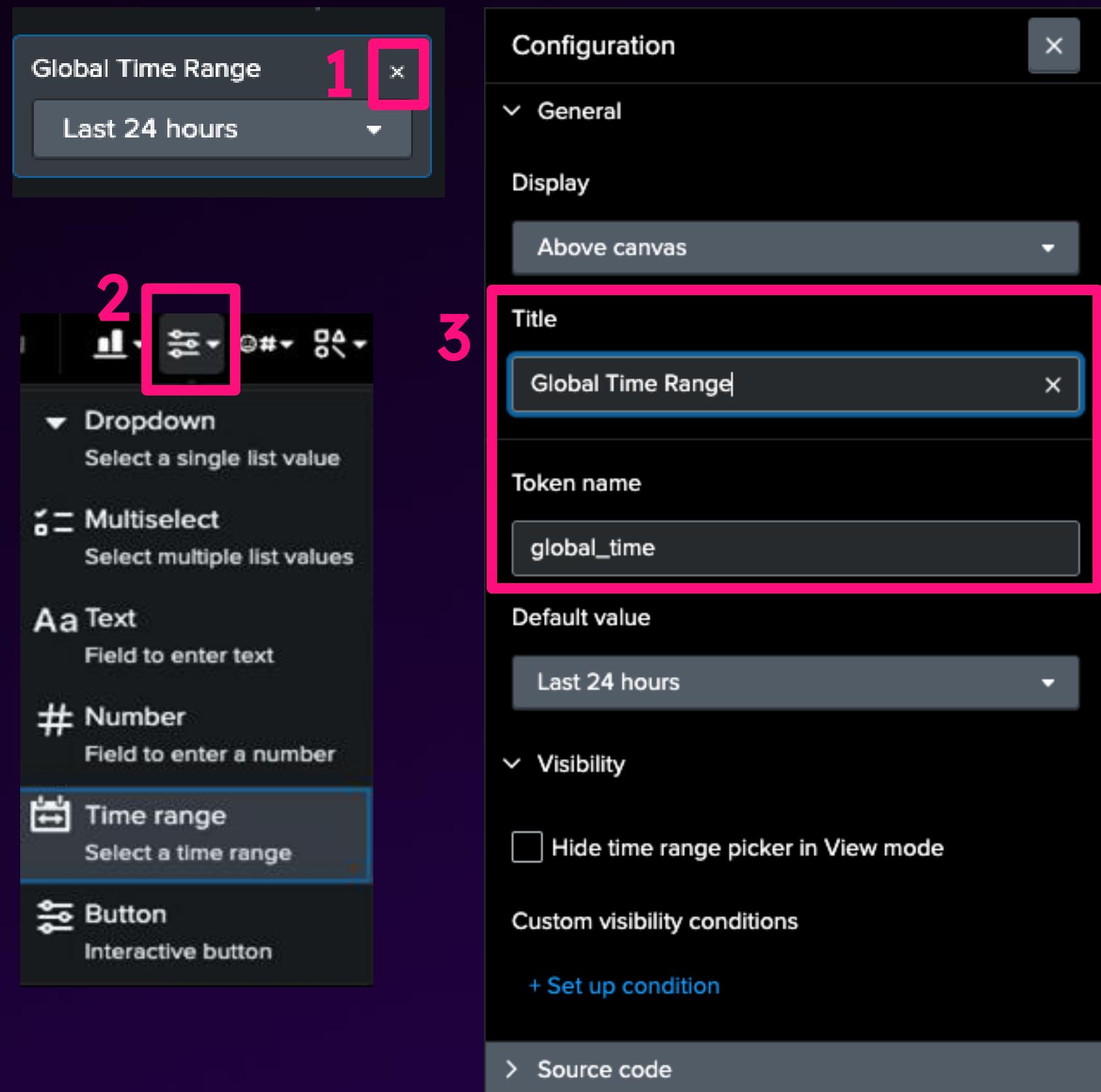
- [Splunk blogs for new features and tips & tricks](#)

Appendix

(OPTIONAL) Adding a Time Range Picker

By default, the entire dashboard uses the Global Time Range picker! You can set up additional time range pickers for each visualization. Here we will teach you how to add the global time range picker back if you remove it by accident.

1. Select the Global Time Range picker. Click x in the top right corner to remove.
2. From the Inputs dropdown, select Time range.
3. In the input's Configuration sidebar:
 - a. Under General > Title put “Global Time Range”.
 - b. Under Token name, put “global_time”. This is the key to make it global!
4. Press enter, or click outside the configuration panel to update. Click Save! Go to slide 28 to change the time range.



Thank you