Splunk4Rookies - Dashboard Studio

Lab Guide

Overview

The purpose of this workshop is to familiarize Splunk users with Dashboard Studio.

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the Splunk Show portal and you will need a Splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one here before proceeding with the rest of the workshop.

⚠️ Troubleshooting Connectivity

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

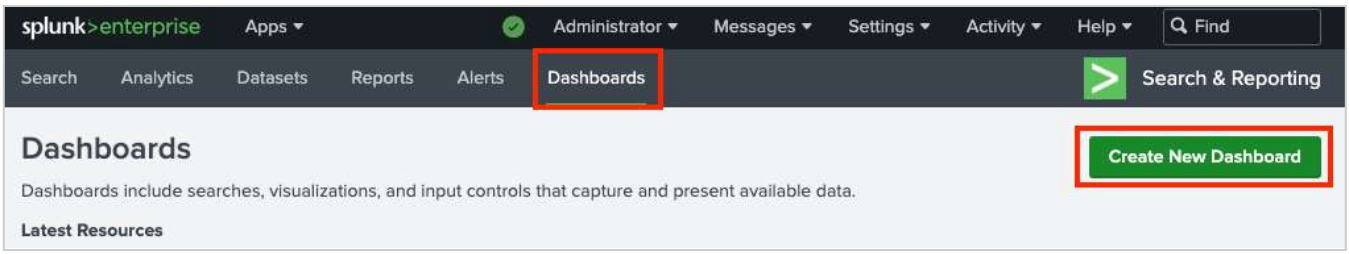
- **Use Google Chrome** (if you're not already)
- If the event page (i.e. *https://show.splunk.com/event/<eventID>*) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using 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! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Lab 1 – Create a Dashboard

Create the 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.

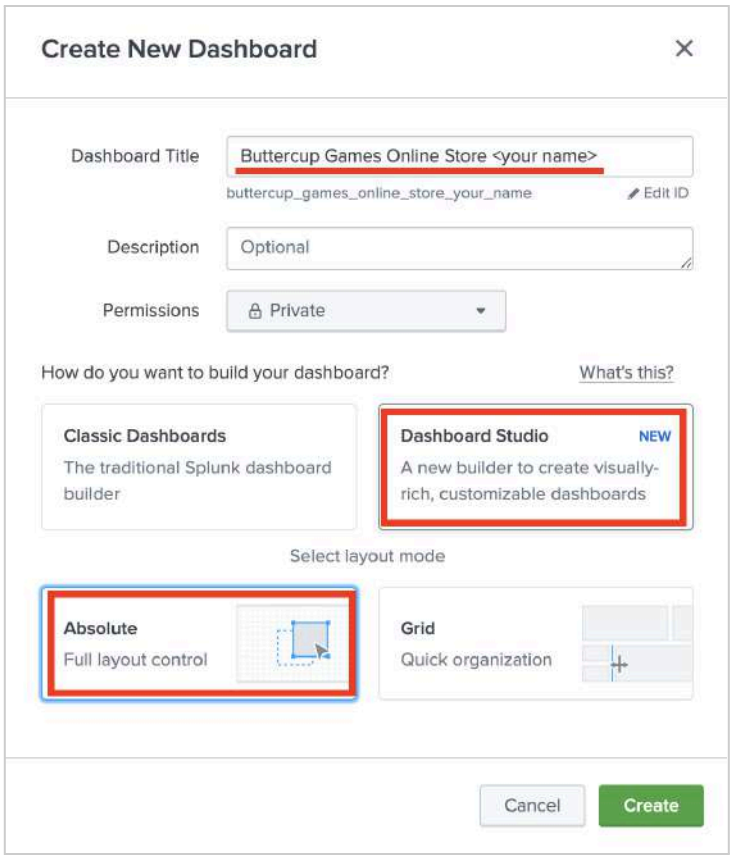


2. Title your dashboard ***Buttercup Games Online Store <your name>***

3. Select the **Dashboard Studio** option to build your dashboard.

4. Select the **Absolute layout**.

5. Click on **Create**.



splunk>

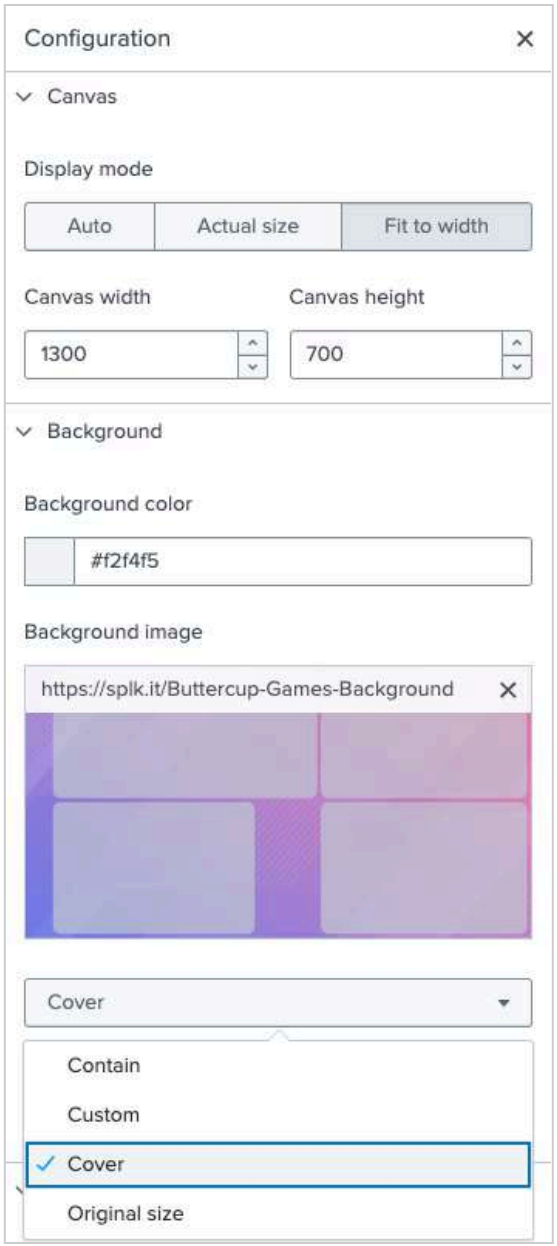
Setup the Canvas

6. Using the **Configuration** panel, make sure the Display Mode is set to **Fit to Width**.

7. Change Canvas Width to **1300** and Canvas Height to **700**.

8. In the **Background Image** section, paste the following image URL into the **Enter URL** box: **https://splk.it/Buttercup-Games-Background**

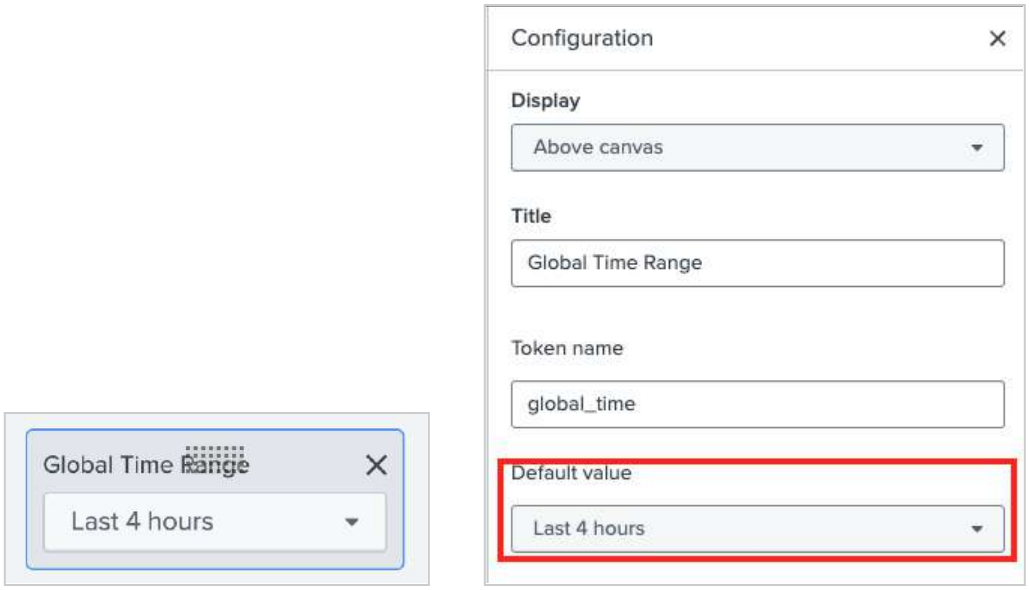
9. Change the background image size setting from **Contain** to **Cover**.



splunk>

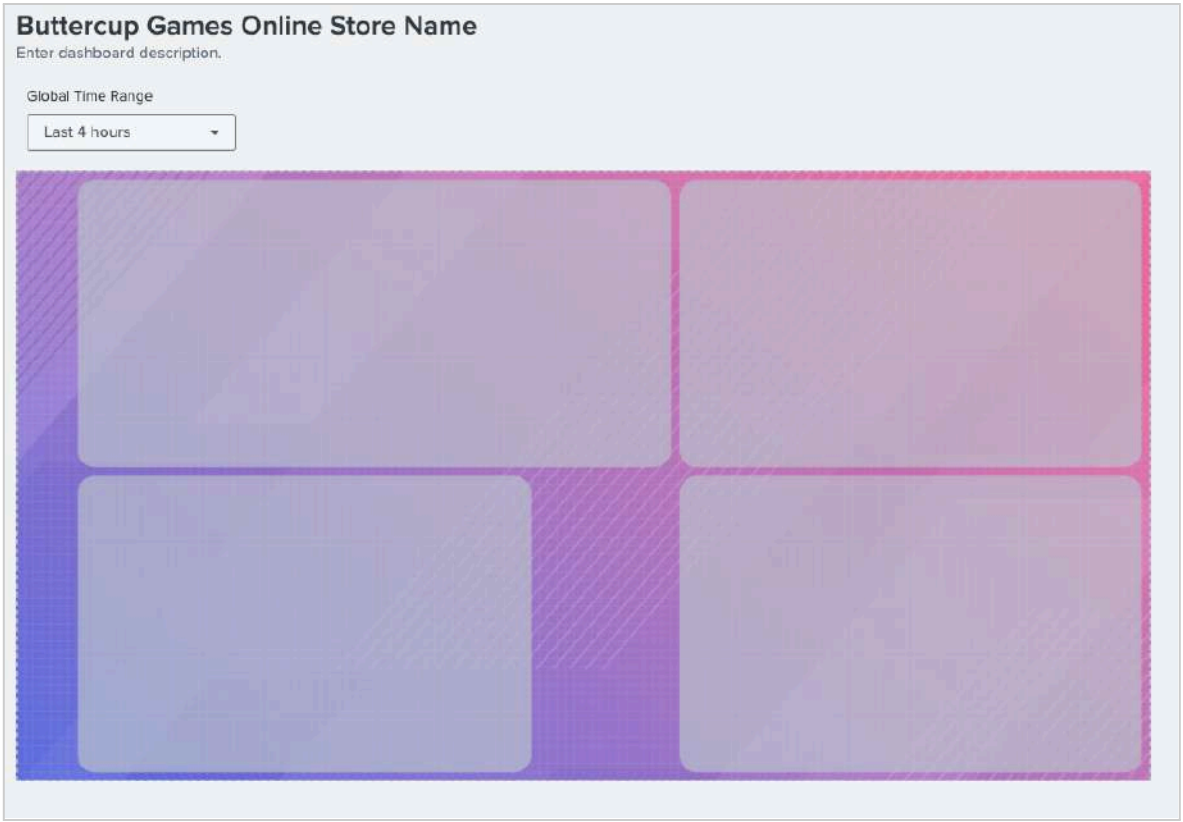
Change the Time Range Picker

10. Change the default time range for the dashboard by clicking on the **Global Time Range** input and in the **Configuration** panel changing the **Default Value** to **Last 4 hours**.



11. Save your changes by clicking on the **Save** button in the top right hand corner.

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



Lab 2 – Add a Table

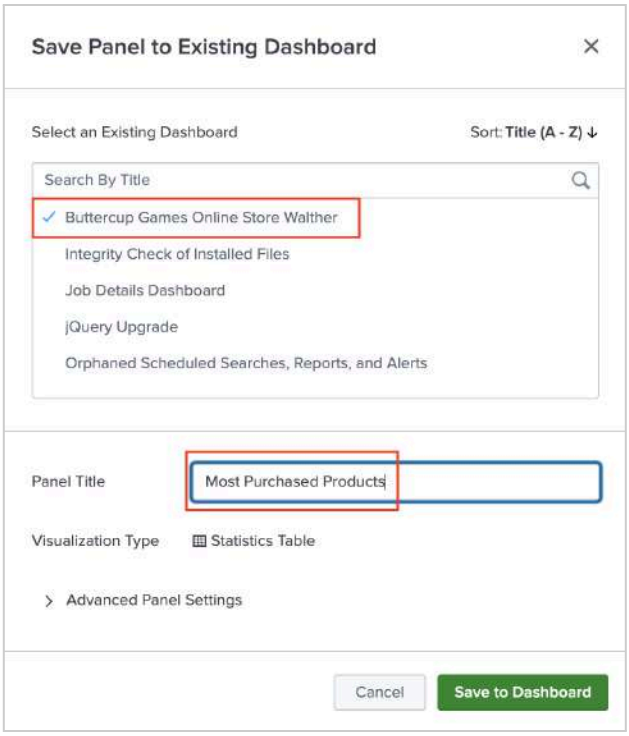
Add a Table

1. Navigate to the **Search** tab.

2. Run the following search into the Search bar:

```
index=main sourcetype=access_combined action=purchase status=200
| lookup product_codes.csv product_id
| stats count as Purchases by product_name product_price
| table product_name Purchases product_price
| eval Revenue=Purchases*product_price
| table product_name Purchases Revenue
| sort -Purchases
| rename product_name as "Product"
| head 8
```

3. Click on **Save As** > **Existing Dashboard**



4. Select the dashboard you just created and title the panel **Most Purchased Products**.
5. Click on **Save to Dashboard** and then on **View Dashboard**.

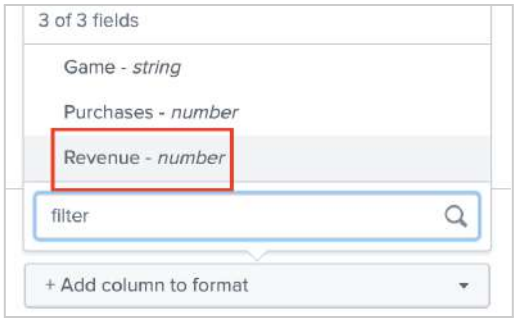
Configure the Table

6. Put your dashboard into edit mode by clicking on the **Edit** button at the top of the screen. Click on the table you just added and in the **Configuration** panel, under **Data sources**, edit the **Most Purchased Products search** data source.

7. Change the **Time range** to **Input** to your search uses the Global Time Range input we configured earlier. Click on **Apply and Close** to save it.

8. In the **Color and style** section, change the **Background** to **transparent**.

9. In the same section, under **Column-specific formatting**:
    a. Click on **+ Add column to format** and select **Revenue - *number***.



    b. Click on the pencil/edit button.

c. Change the **Units Position** option to **Before** and for the **Unit Label** enter a dollar symbol (**$**).

d. Increase the **Precision** value to "**2 (0.00)"** and set **Thousand Separators** to **On**.

e. Click on **+ Add Column to format** again, but this time choose the **Purchases - *number*** column.

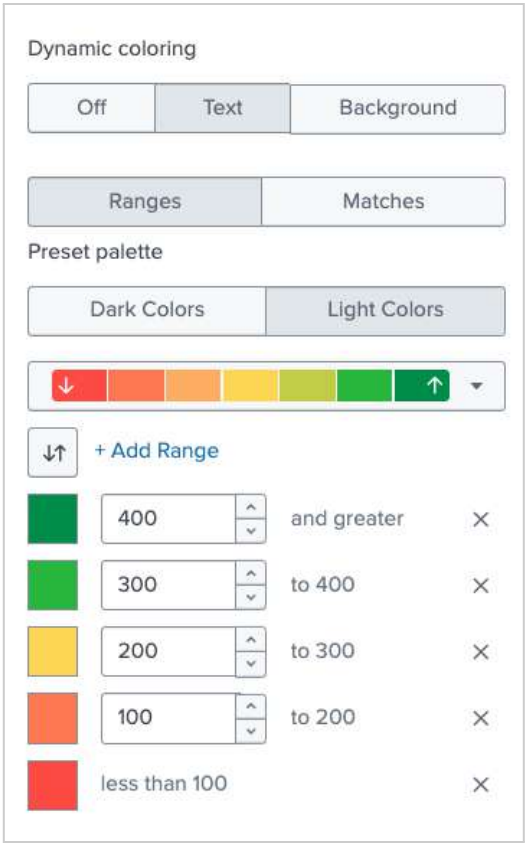
f. Click on the pencil/edit button.

g. Change the **Dynamic Coloring** option to **Text**.

h. For the **Preset Palette**, choose **Light Colors**.

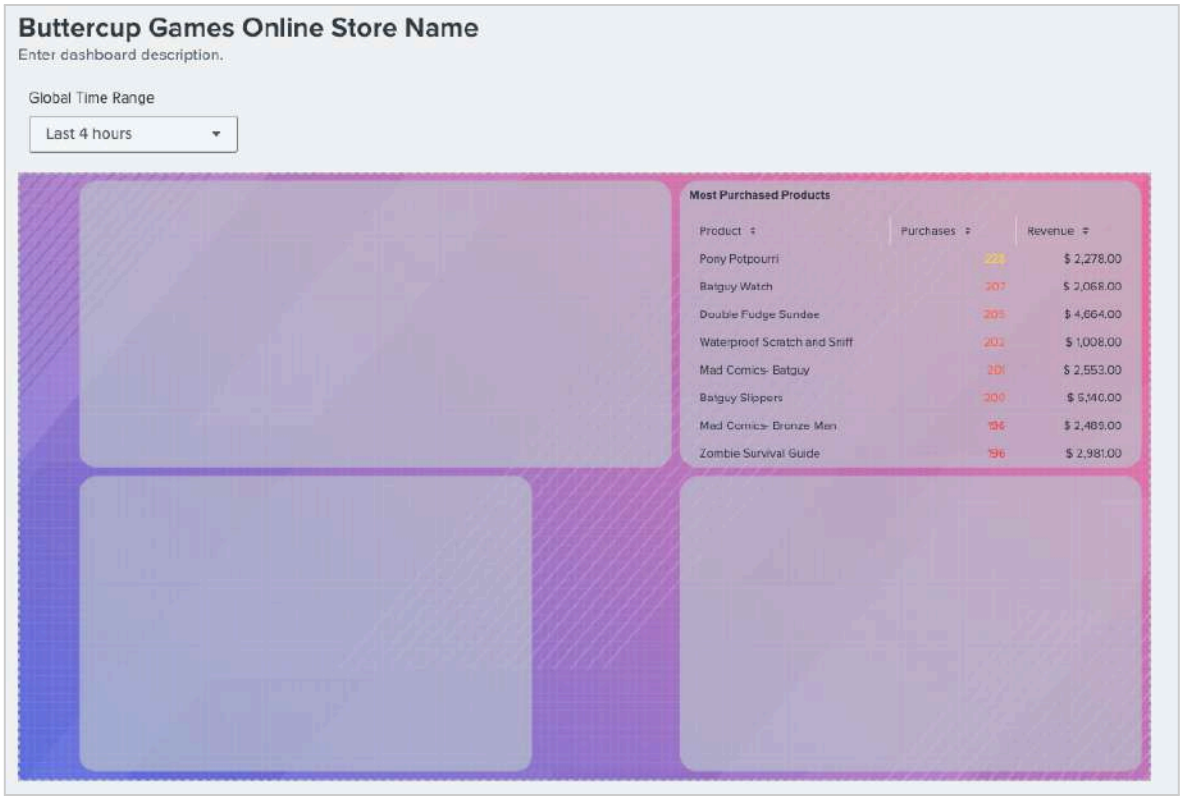
i. For this exercise, enter the following five ranges:

400 and greater
300 to 400
200 to 300
100 to 200
Less than 100



10. Move and resize your table to center it in the top right panel.

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



splunk>

Lab 3 – Add Chart Visualizations

Add a Pie Chart Visualization

1. Click on the add chart icon ( ) in the editing toolbar, and then select **Pie**.

2. In the **Select data source** panel, click on **+ Create search** and add the following search into the **SPL query** box:

```
index=main sourcetype=access_combined action=purchase status=200
| lookup product_codes.csv product_id
| stats count values(product_price) as Price by product_name product_id
| table product_name product_id count Price
| eval revenue=count*Price
| fields product_name revenue
| rename product_name as "Product" revenue as "Revenue"
| sort -Revenue
```

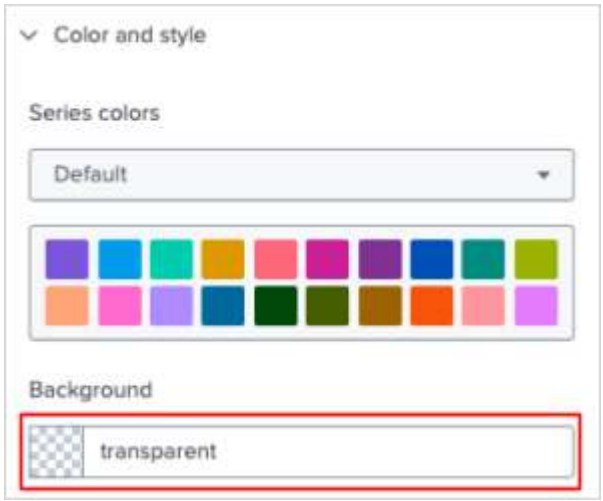
3. For the **Data source name** put '**Revenue by Product search**'.

4. Set the **Time range** to **Input**.

5. Click on **Apply and Close**.

6. Title your pie chart **Revenue by Product** and leave the description box empty.

7. In the **Color and style** section of the **Configuration** panel, change the **Background** to **transparent**.



8. Move and resize your pie chart to center it on the bottom left gray rectangle.

Add a Column Chart

9. Click on the add chart icon ( ) in the editing toolbar, and then select **Column**.

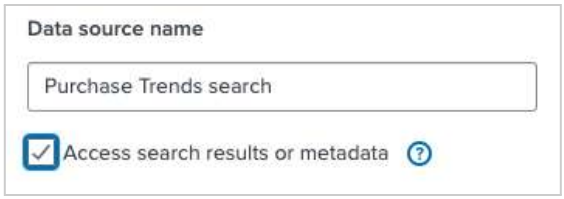
10. Create a search as you did previously (Select data source > click on **+ Create search**) and add the following search into the **SPL query** box:

```
index=main sourcetype=access_combined action=purchase status=200
| lookup product_codes.csv product_id
| fields _time category clientip
| timechart count by category
```

11. Name the data source **Purchase Trends search**.

12. Set the **Time range** to **Input**.

13. Check the **Access search results or metadata** box.



14. Click on **Apply and Close**.

15. Title your chart **Purchase Trends** and leave the description box empty.

16. In the **Configuration** panel, follow these steps:

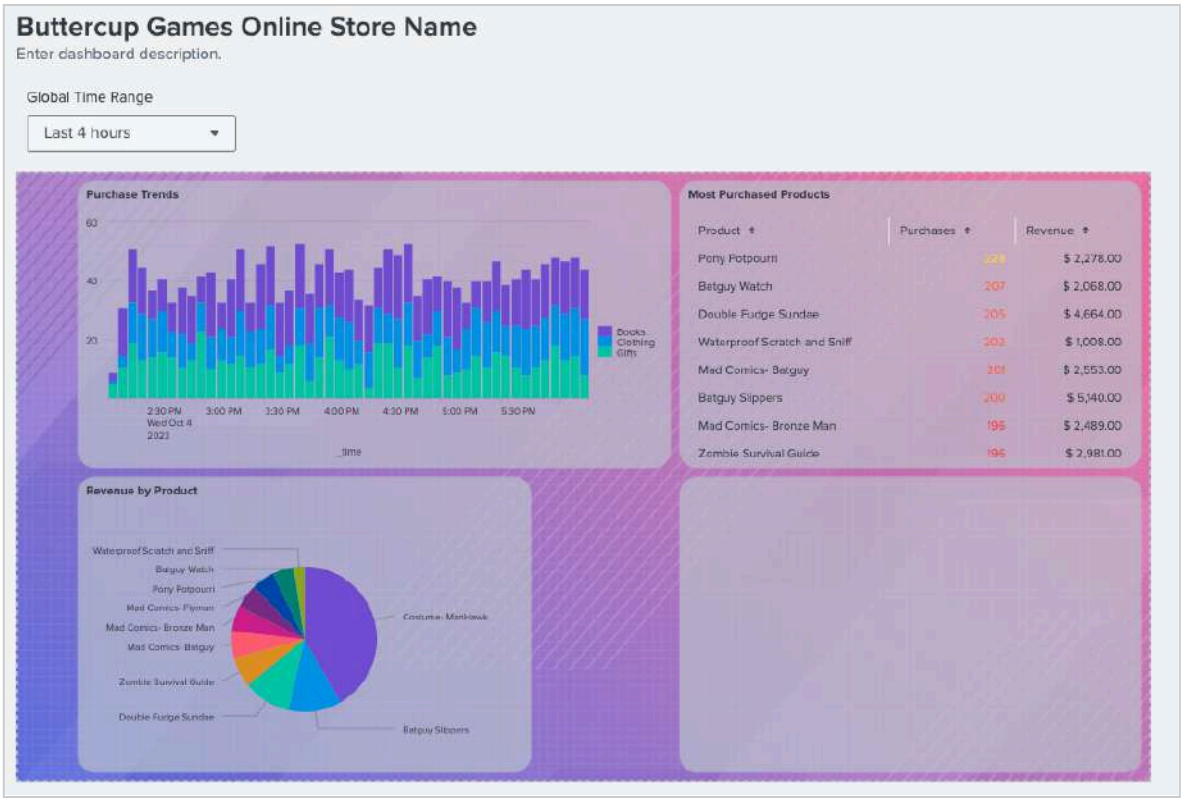
    a. In the **Color and style** section change the **Background** to **transparent**.

    b. In the **Data display** section change the **Stack Mode** to **Stacked**. The stacked option builds the area for each value vertically on top of one another instead of creating layers beginning at the x-axis.

    c. In the **Legend** section change the **Legend display** to **Right**.

17. Move and resize your column chart to the center of the top left gray rectangle and save your dashboard.

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



splunk>

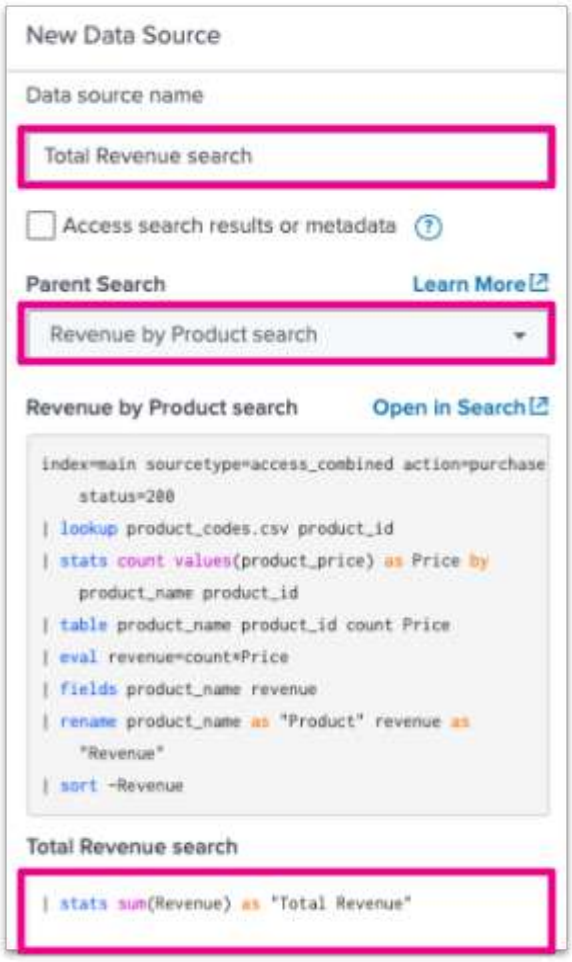
Lab 4 – Create a Chain Search

Create a Chain Search

1. In the **Data source overview** ( ) panel, select **+ Create chain search**.
2. For the **Data Source Name** put **Total Revenue search** and for the **Parent Search** select **Revenue by Product search**.
3. Add your extended search into the **Total Revenue search** box:

```
| stats sum(Revenue) as "Total Revenue"
```

4. Click on **Apply and Close**.



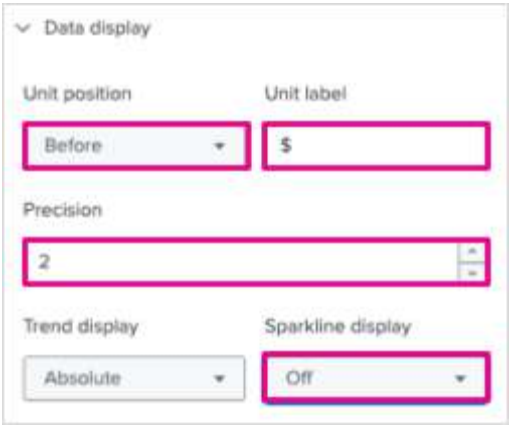
Add a Single Value Visualization

5. Click on the add chart icon ( ) in the editing toolbar, and then select **Single Value**.

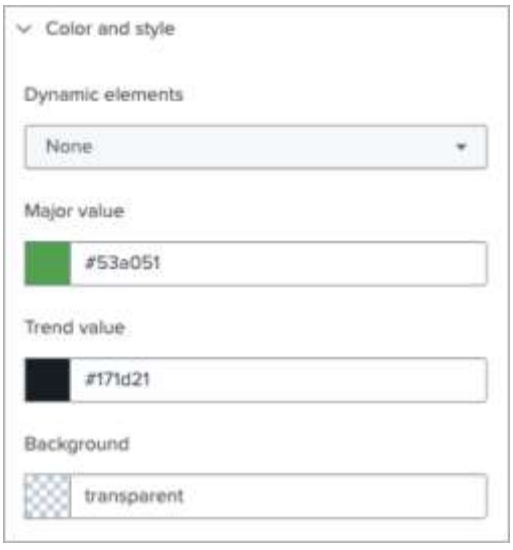
6. In the **Select Data** panel, under the **Chain Search** section, click on **Total Revenue search (Unused)**.

7. Under the **Data configurations** section, for the **Value** select **Total Revenue (number)**.

8. Under the **Data display** section, set the following:
    a. Change the **Unit Position** to **Before**.
    b. For the **Unit Label** enter a dollar symbol (**$**).
    c. Increase the **Precision value** to **2**.
    d. Set **Sparkline display** to **Off**.



9. Under the **Color and style** section, set the following:
    a. Change the **Major value** to **#53a051**
    b. Change the **Background** to **transparent**.



10. Move and resize the single value so that it fits inside the bottom right corner box of your dashboard.

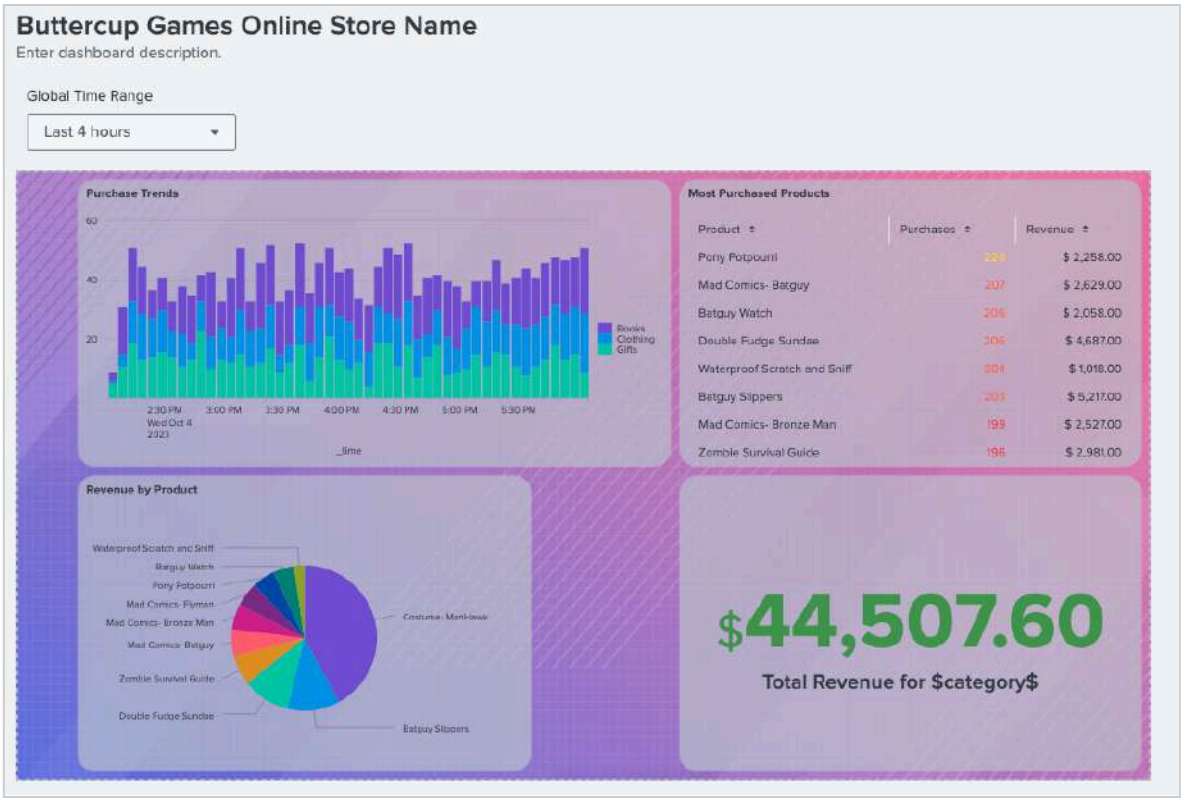
11. In the main toolbar click the markdown (M↓) button.

12. Type **# Total Revenue for $category$** into the **Markdown content** text box.
    Note: The # makes the text extra large.

13. Place the title beneath the total revenue visualization.

14. Click on the **Save** button in the top right corner.

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



splunk>

Lab 5 – Setup Annotations and Token

1. Click on your **Purchase Trends** chart. Under **Data sources**, select, **+ Set up annotation data source**.

2. Click on **+ Create search** and add the following into the **SPL query** box:

```
| makeresults count=1
| streamstats count
| eval annotation_label= case(count=1 ,"Book Sale Starts")
| eval _time=now()-count*2000
```

3. Set the **Time range** to **Input**.

4. Name the data source **Book Sale**.

5. Click on **Apply and Close**.

6. With your **Purchase Trends** chart still selected, under the **Data configurations** section, for **Annotation x** select **_time (time)**.

7. For **Annotation labels** choose **annotation_label (string)**

Configure Searches with an Input Token

8. In the **Configuration** panel for **Purchase Trends**, scroll down to **Interactions**.

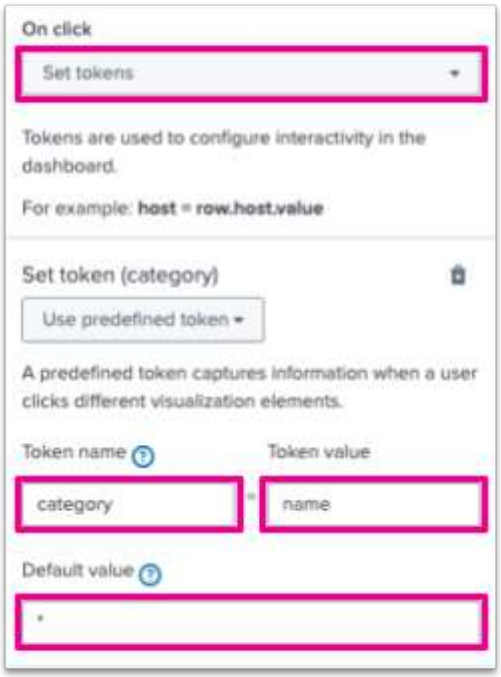
9. Click on **+ Add interaction** and from the **On click** dropdown select **Set tokens**

10. Set the following:

    a. Set the **Token name** to **category**

    b. Set the **Token value** to **name**

    c. Set the **Default value** to ***



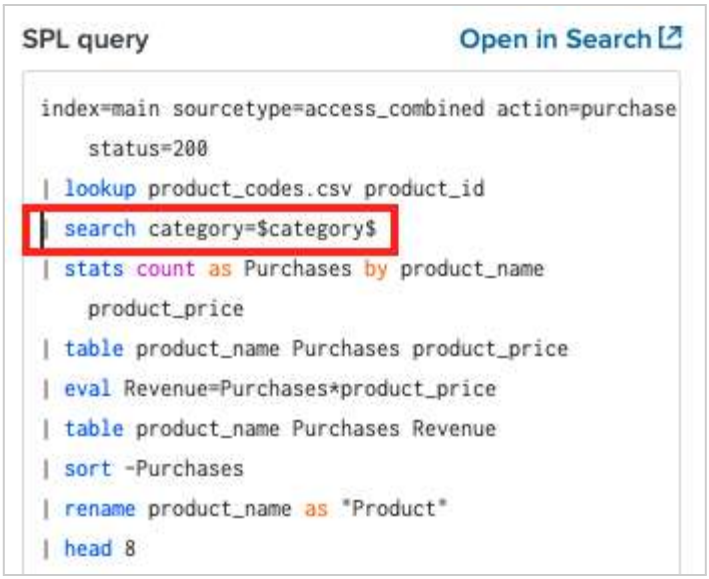
splunk>

11. Click on **Apply**.

12. Select the **Data source overview** icon ( ) and open the **Most Purchased Products search** with the edit icon.

13. Add your input token to the search by copying and pasting the following SPL after the `| lookup…` line:

```
| search category=$category$
```



14. Click on **Apply and Close**.

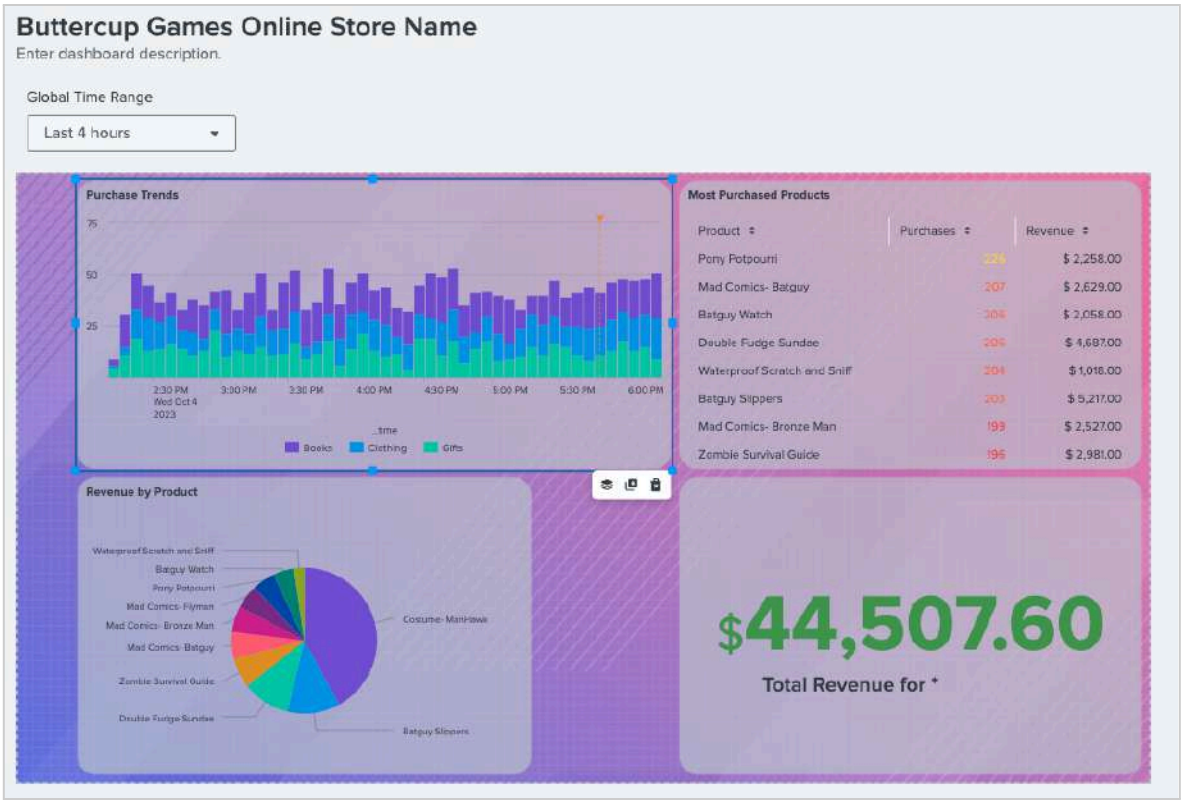
15. Repeat steps 12–14 for **Revenue by Product search**

    Note: Your visualizations may disappear and say 'No search results returned'. That's okay!

16. Save your dashboard and click on **View** to view your dashboard.

17. Click on a category on the **Purchase Trends** chart to see your visualizations update!

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



splunk>

Lab 6 – Add a Reset Button

Create the “Reset Selection” button

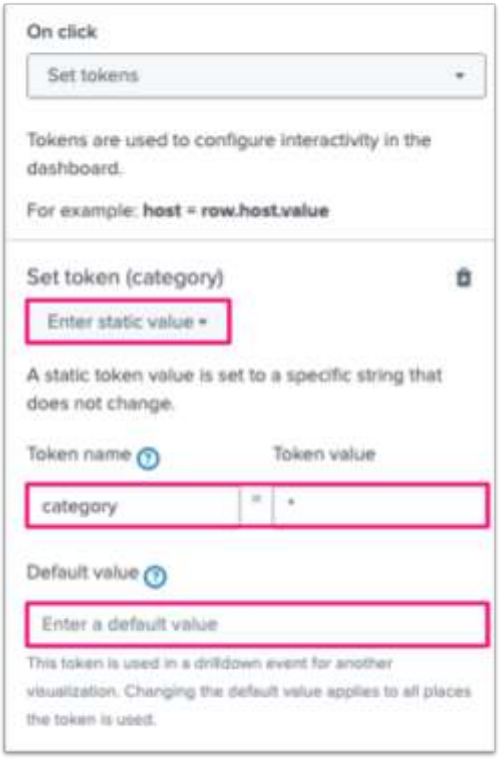
1. Add a Rectangle
2. Move and resize the rectangle to fit in the space between the two bottom panels
3. Change Fill and Stroke colors to **blue #0877a6**
4. Add the following markdown (M↓) text:

   ```
   ## Reset Selection
   ```

5. Move and resize the markdown text box to fit inside the rectangle
6. Change font color of the markdown text to **white**

Configure the Set Token drilldown

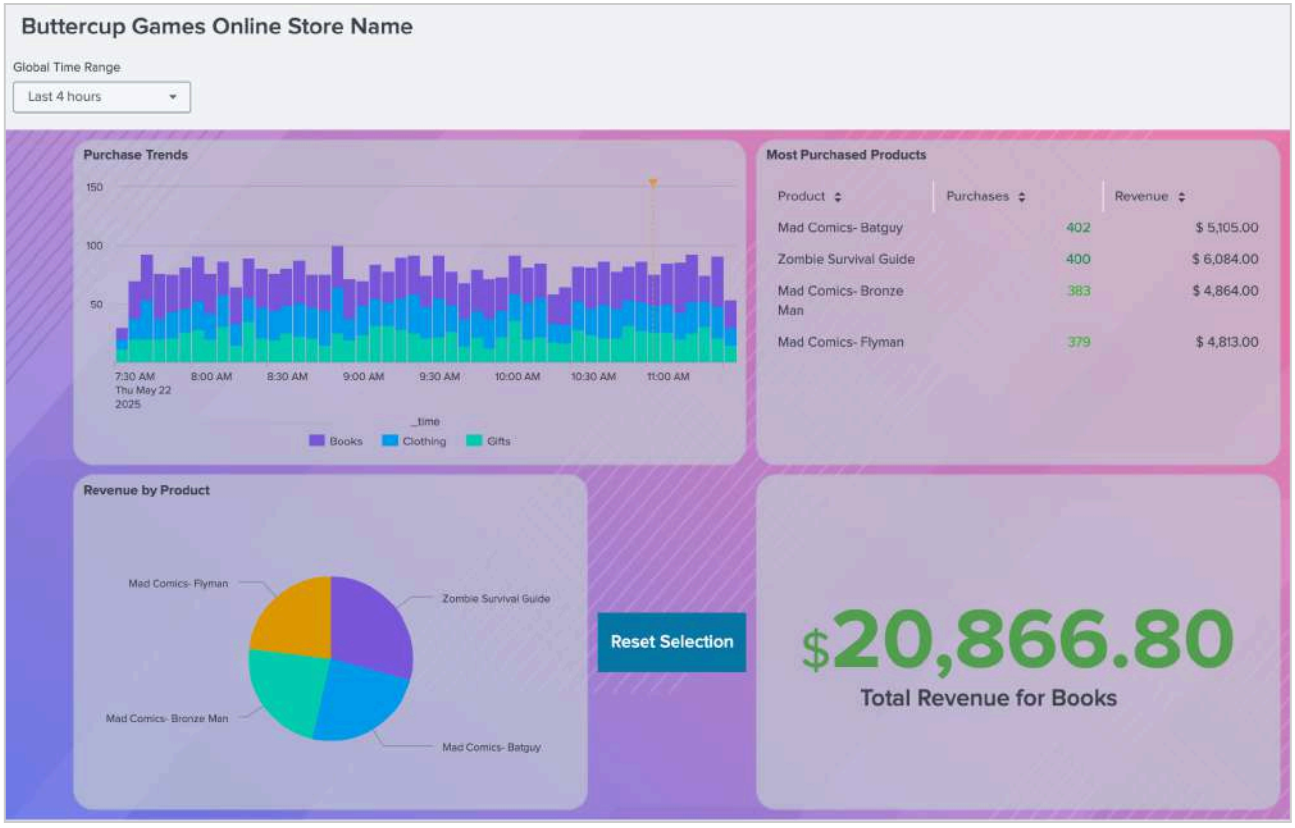
7. Add another Rectangle
8. Move and resize the rectangle to cover the "**Reset Selection**" text you previously added
9. Change Fill and Stroke colors to **transparent**
10. In the **Configuration** panel, scroll down to **Interactions**.
11. Click on **+ Add interaction** and from the **On click** dropdown select **Set tokens**.
12. Select ‘**Enter static value**’ and set the following:
    a. Set the **Token name** to **category**
    b. Set the **Token value** to ***
    c. Leave **Default value** empty
13. Save your dashboard and switch to **View** mode.



splunk>

Completed Dashboard

Congratulations – you finished! At this point your dashboard should look like this:



Try selecting elements on your dashboard - such as clicking on different categories on the Purchase Trends panel to filter the dashboard - and then click the Reset Selection button to reset the dashboard.

Note: Check out our resources on Dashboard Design Best Practices and Visualization Choices and Configurations

---