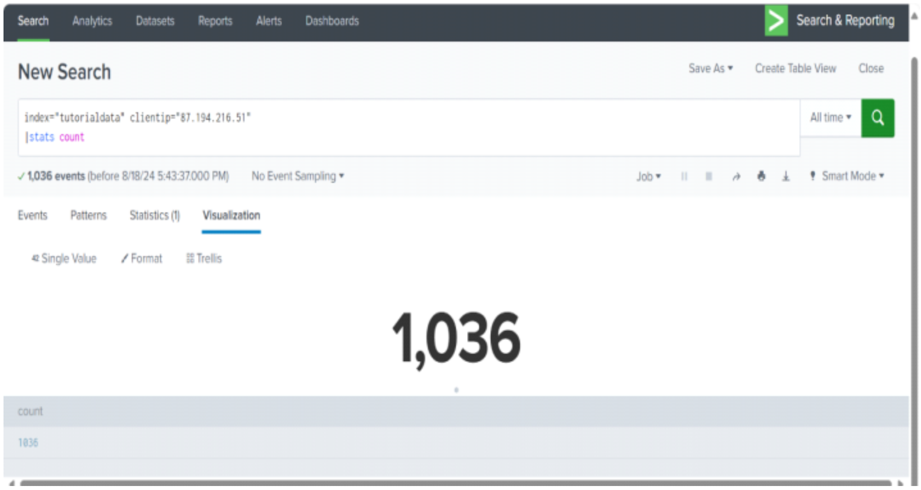
Creating a Splunk Dynamic Dashboard

Saturday, August 17, 2024 1:54 AM

Dynamic form-based dashboards in Splunk enable users to update and interact with dashboard data in real-time without leaving the page. This functionality is achieved by incorporating various input fields—such as time pickers, radio buttons, textboxes, checkboxes, and dropdowns—into the dashboard. These inputs allow users to refine and change the displayed data instantly based on their selections.

<u>How to create</u>

- Access Splunk Dashboard and input the query into the search bar



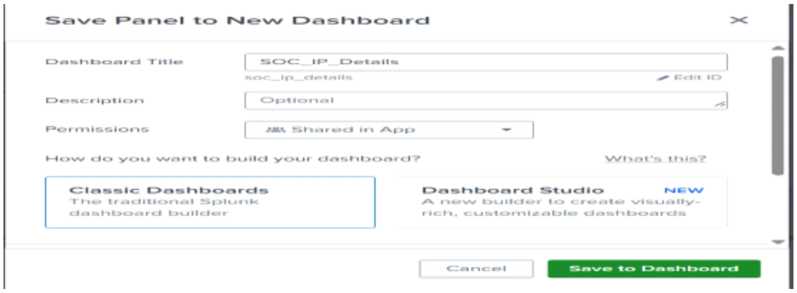
```
index="tutorialdata" clientip="87.194.216.51"
|stats count
```

✓ 1,036 events (before 8/18/24 5:43:37.000 PM) No Event Sampling ▾

1,036

count
1036

- Using the save as button, save the single line visualization data as a new dashboard. Give the dashboard a name, choose the appropriate app, set the permissions, choose dashboard Type:



Save Panel to New Dashboard

Dashboard Title: SOC_IP_Details
soc_ip_details

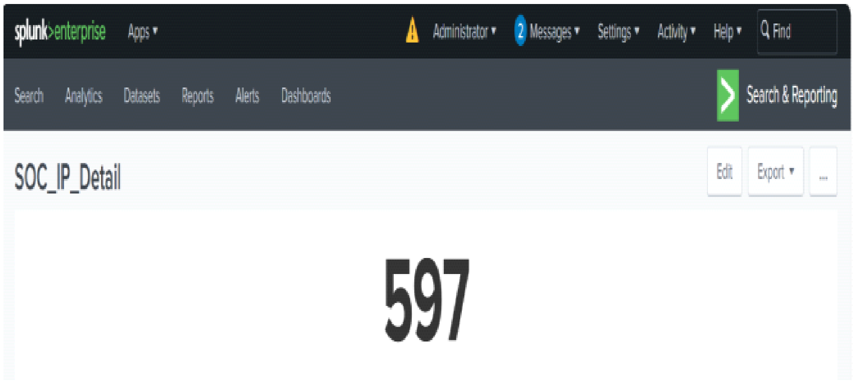
Description: Optional

Permissions: Shared in App

How do you want to build your dashboard?

Classic Dashboards
The traditional Splunk dashboard builder

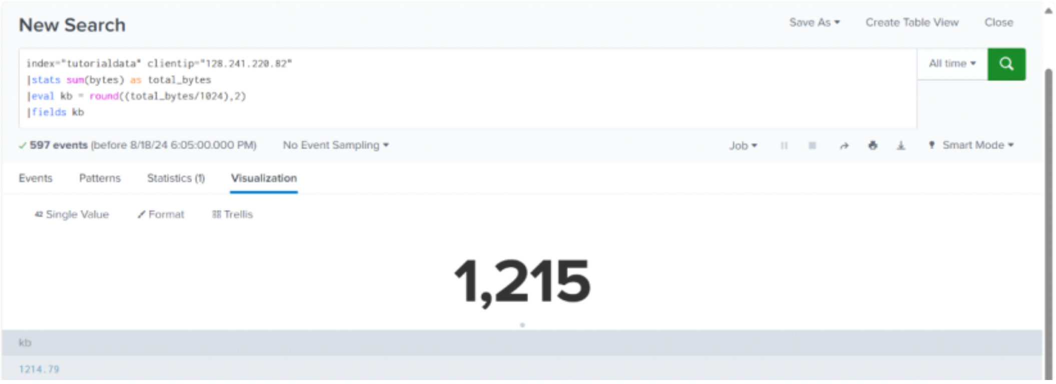
Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards



SOC_IP_Detail

597

- Input two more queries identifying the bytes of IP address (in KB) and the time chart (can use the line char visualizationt). Save data as Existing dashboard already created

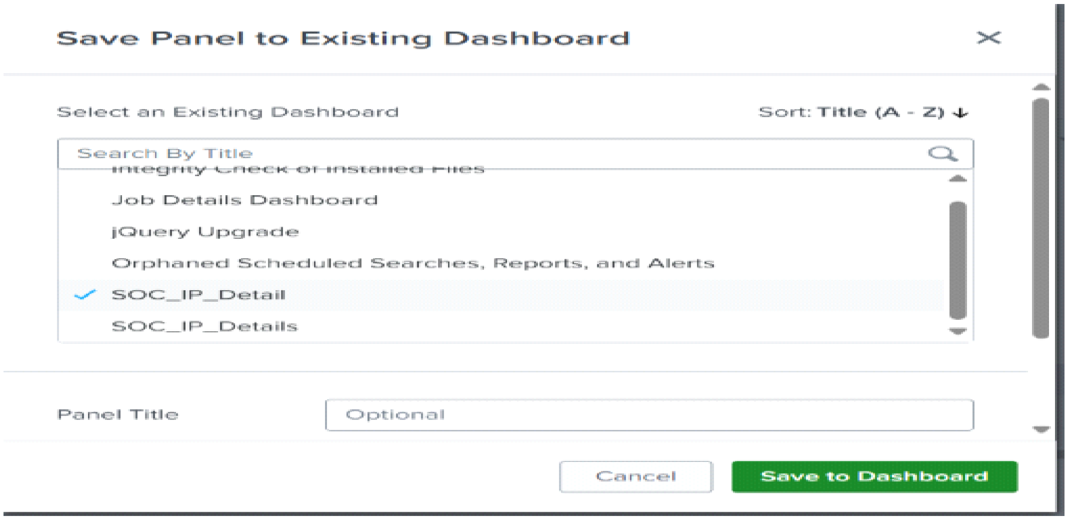


New Search

```
index="tutorialdata" clientip="128.241.220.82"
|stats sum(bytes) as total_bytes
|eval kb = round((total_bytes/1024),2)
|fields kb
```

✓ 597 events (before 8/18/24 6:05:00.000 PM)

kb
1214.79



Save Panel to Existing Dashboard

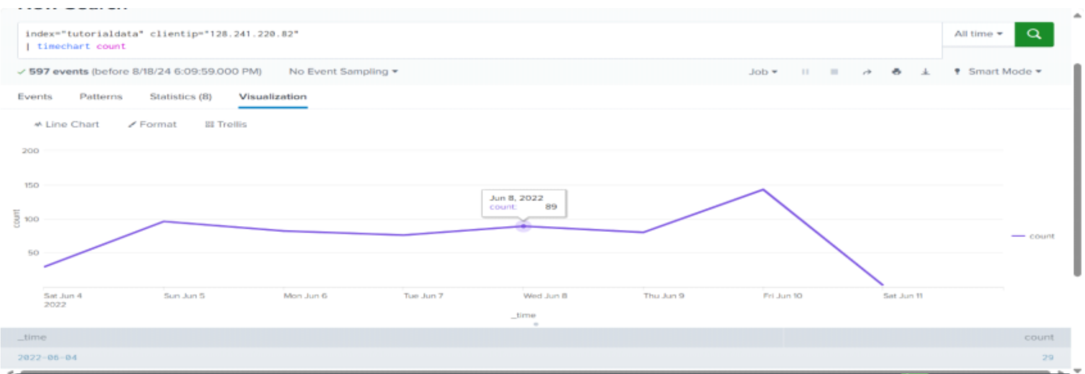
Select an Existing Dashboard

Sort: Title (A - Z) ↓

Search By Title

- Integrity Check of Installed Files
- Job Details Dashboard
- jQuery Upgrade
- Orphaned Scheduled Searches, Reports, and Alerts
- ✓ SOC_IP_Detail
- SOC_IP_Details

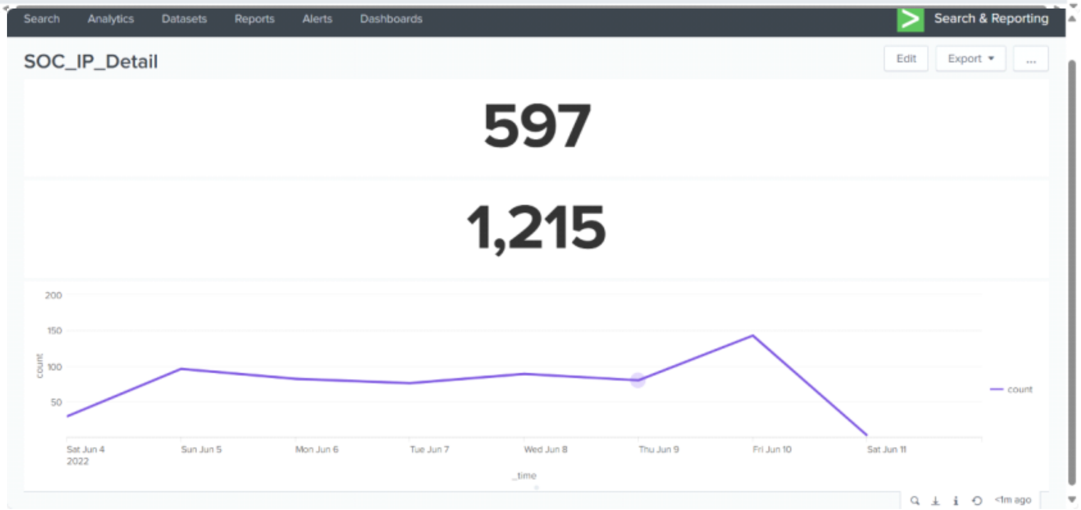
Panel Title: Optional



```
index="tutorialdata" clientip="128.241.220.82"
| timechart count
```

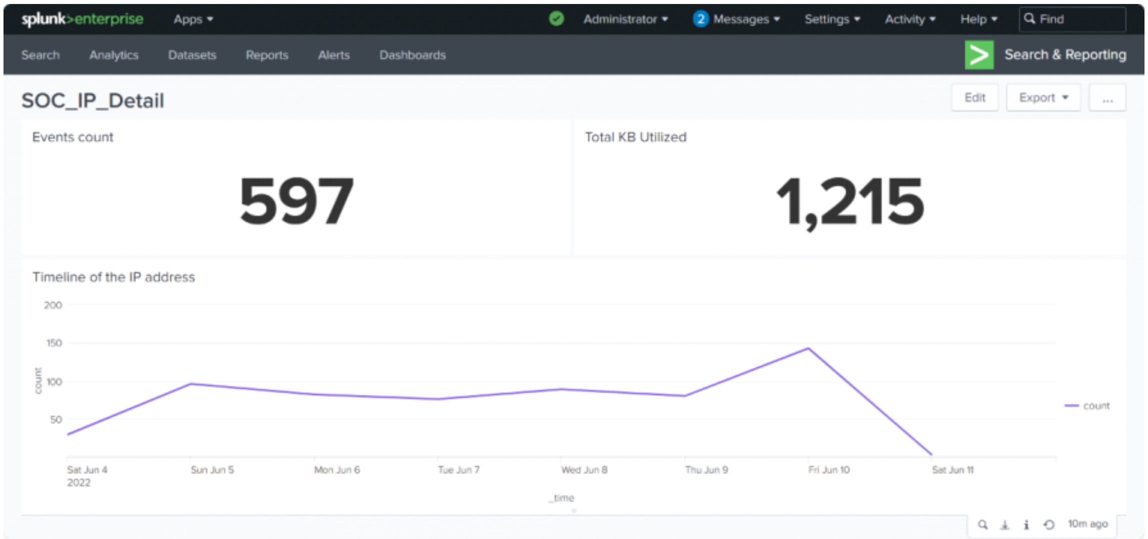
✓ 597 events (before 8/18/24 6:09:59.000 PM)

_time	count
2022-06-04	29



SOC_IP_Detail

► Edit the Dashboard: Once the dashboard is created, click Edit (add title, organize data) then save



SOC_IP_Detail

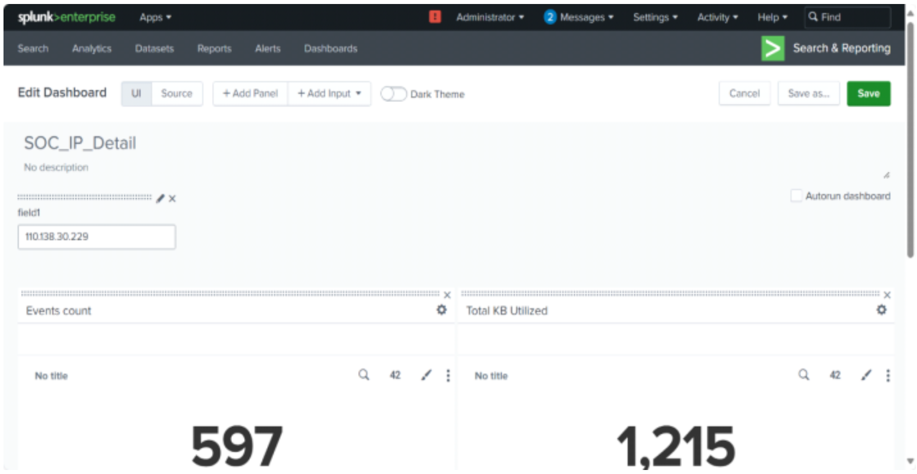
Events count: 597

Total KB Utilized: 1,215

- ► Add Input Fields: Click on Add Input in the dashboard editor toolbar. Add text, on the field bar, add the IP address

  Note: You can also add various input fields such as:

  Time Picker: Allows users to select a time range.
  Dropdown: Provides a list of options to choose from.
  Radio Button: Offers a set of radio buttons for selection.
  Checkbox: Allows multiple selections.
  Text Box: Lets users enter custom text.



SOC_IP_Detail

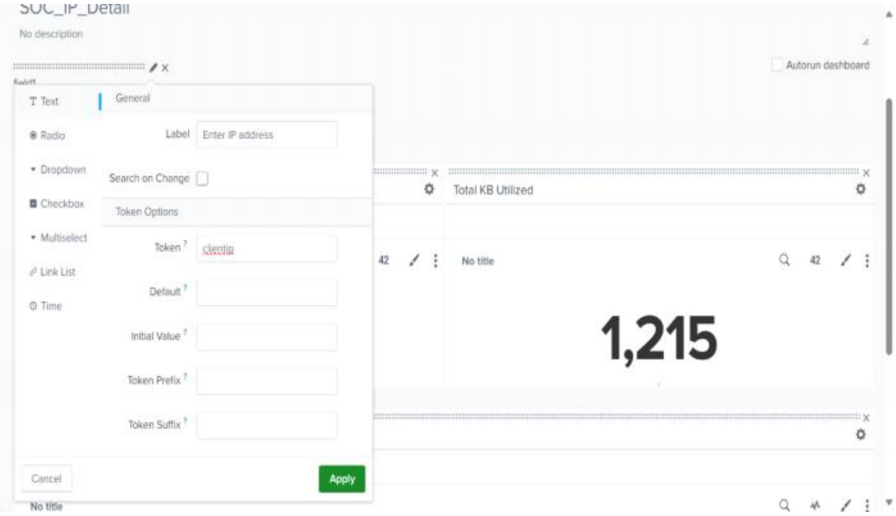
No description

field1: 110.138.30.229

Events count: 597

Total KB Utilized: 1,215

- ► Configure Input Settings: After adding the input fields, configure them by clicking on the pencil button and defining the available options: Label, Token (used for referencing in searches), default values etc



Label: Enter IP address

Search on Change □

Token: clientip

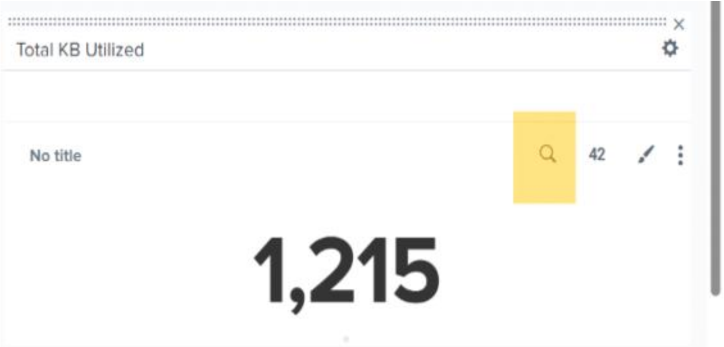
Default:

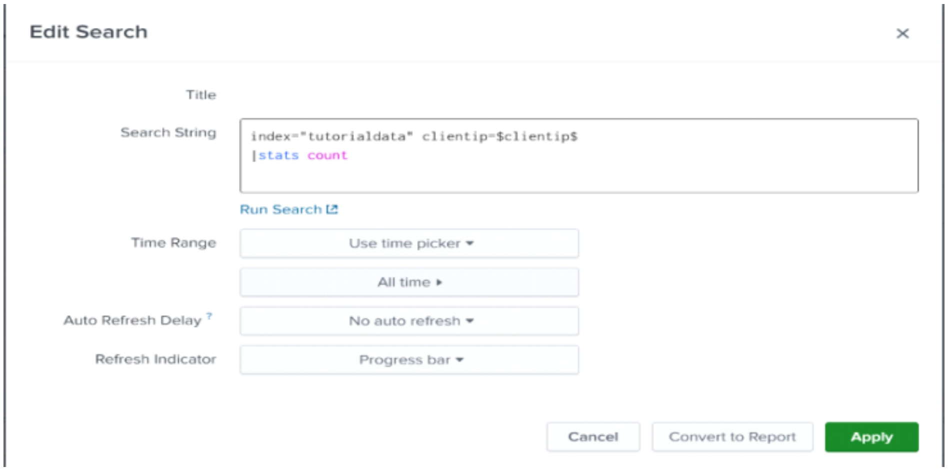
Initial Value:

Token Prefix:

Token Suffix:

- Link Inputs to searches by editing the existing panels that will display the search results.
- Reference Input Tokens in Search Queries: Modify the search queries in the panels to include the tokens from the input fields (using the $$ symbol inbetween the symbol input the token name)





Title

Search String

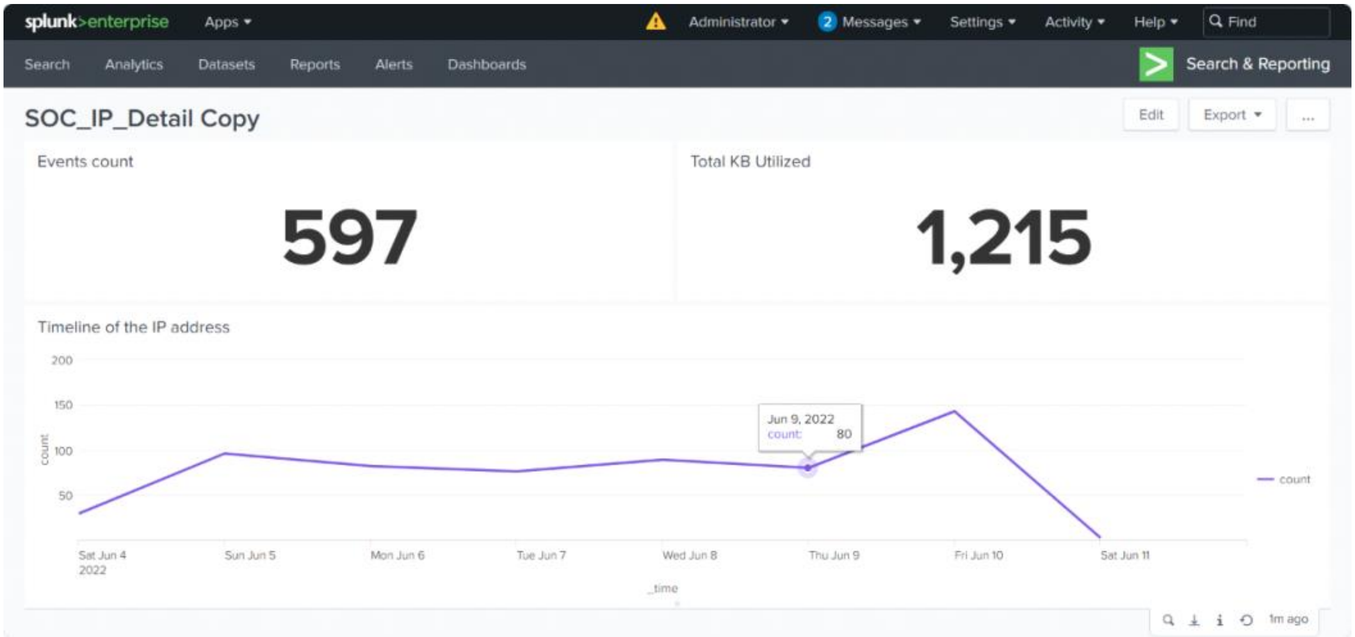
```
index="tutorialdata" clientip=$clientip$
|stats count
```

Time Range: Use time picker ▾

All time ▸

Auto Refresh Delay: No auto refresh ▾

Refresh Indicator: Progress bar ▾



SOC_IP_Detail Copy

Events count

597

Total KB Utilized

1,215

Timeline of the IP address

- ► Save Your Dashboard