**Nwachukwu Edumanichukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 1 Lab – Advanced Dashboarding and Alerting**

In this first lab, we will begin exploring various tool to build dashboards and alerting. More specifically, we will use Splunk and Grafana to build charts, graphs, tables, and other visualizations. We will then go through process of using our queries to build automated alerts. Splunk has three data sets that contain attack data. We will be using the Boss of the SOC V3 data to create a dashboard. We will also be using the Grafana test data set to draw charts.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

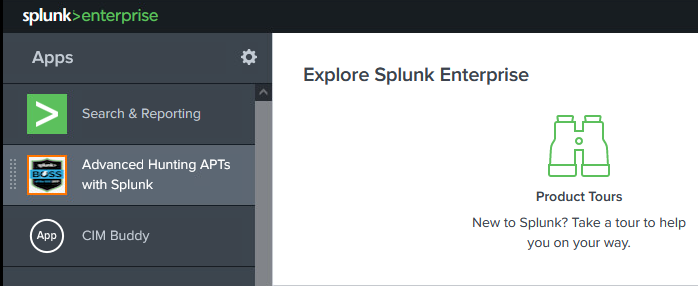
Accessing the Lab

This lab is hosted in the universities IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. You should use the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log into this interface with your Bellevue student ID and password.

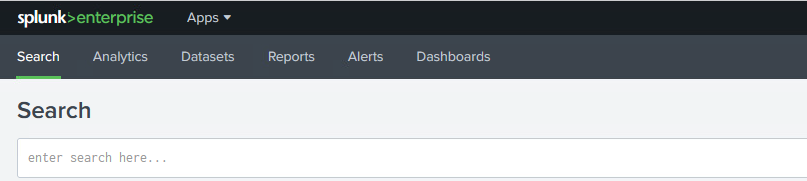
Part 1 - Dashboarding and Alerting with Splunk

Splunk is a scalable platform for ingesting, parsing, indexing, and analyzing machine generated data. Though originally built primarily as an analytics platform, the core functionality of the platform made it ideal for working as a SIEM and providing other security functions. In Part 1 of this lab, you will utilize the visualization functionality to build a simple dashboard and setup a single alert.

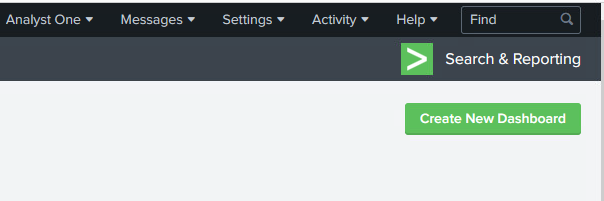
1. Access Splunk by opening a browser and navigating to <https://10.98.100.11:8000/>. You may get a warning related to the certificate not being trusted. Accept the warning and proceed to Splunk.
2. Login to Splunk using the username analyst# and password An@lyst#!! where # is your assigned student/analyst number.
3. Click on spunk>enterprise on the upper left of the web page and then click Search & Reporting.



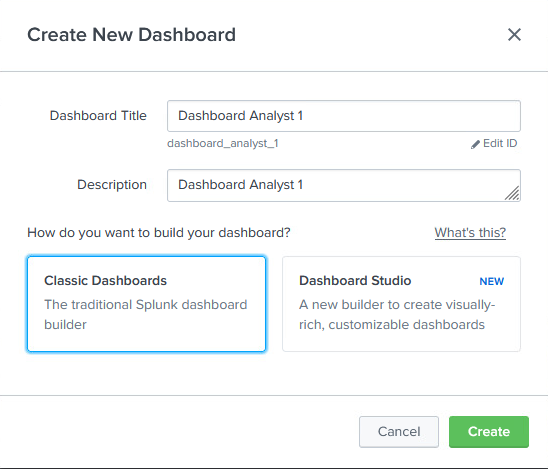
1. On the upper menu click Dashboards



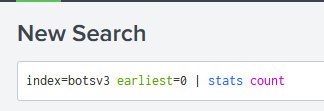
1. In the upper right-hand corner of the page, click the Create New Dashboard.



1. Use “Dashboard Analyst #” where # is your analyst number. Use the same text for the description. Select Classic Dashboards and then click Create.



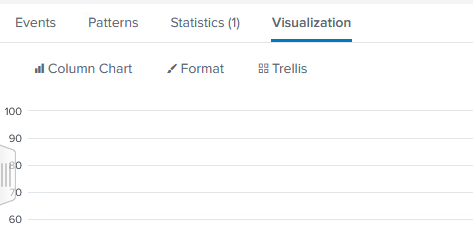
1. Switch back to search and enter the following query in the New Search text field: index=botsv3 earliest=0 | stats count. This query will tell us which kinds of logs are in the Boss of the SOC dataset.

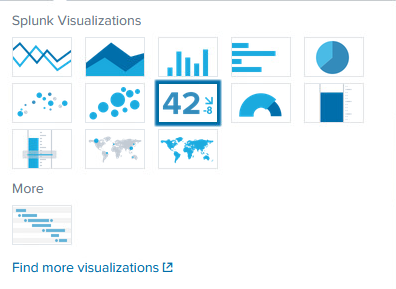


**How many total events are part of the BOTSv3 dataset?**

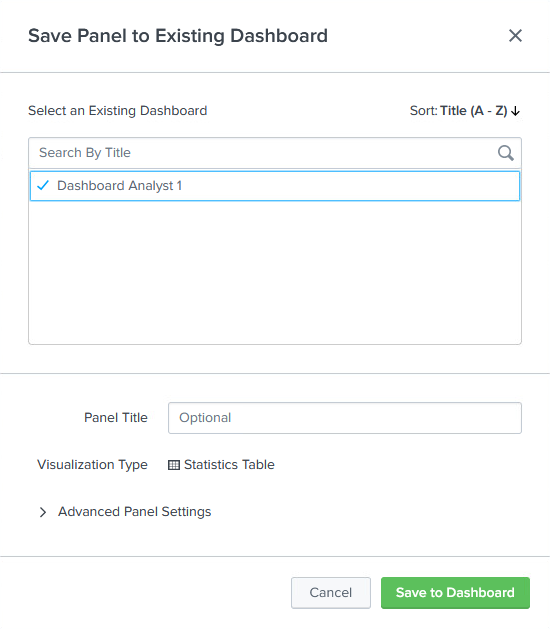
**2,842,010 events**

1. Select Visualization and then Column Chart. Change the visualization type to Single Value.

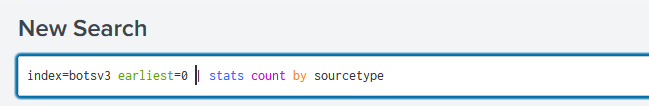




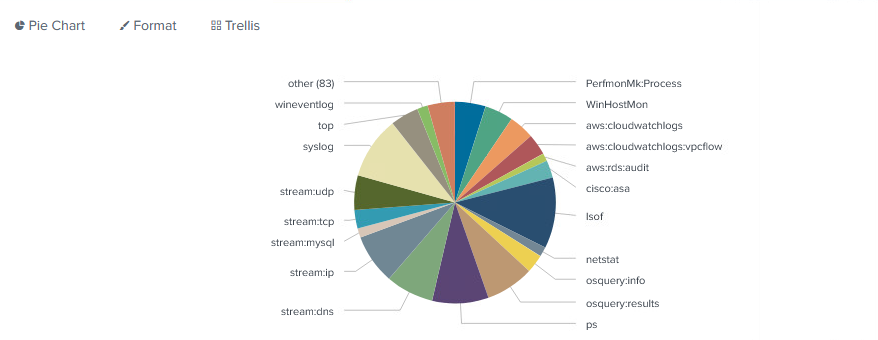
1. In the upper left-hand corner of the web page, select “Save As” and then “Existing Dashboard.” Select “Dashboard Analyst #” and then click the “Save to Dashboard.” Click View Dashboard. Eventually you will see your dashboard with the total number of events displayed as a single value.



1. Click on Search again and type “index=botsv3 earliest=0 | status count by sourcetype”. This will show us the different logs types that are part of the index.

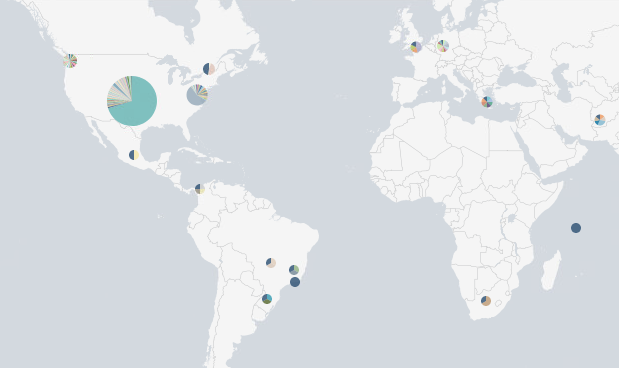


1. Click on Statistics and then “Save As”, then select “Existing Dashboard”, “Dashboard Analyst #”, and then Save to Dashboard. Click “View Dashboard” to see the Statics Table added to the dashboard.
2. Click back to search and enter the same query: index=botsv3 earliest=0 | stats count by sourcetype. Click Visualization and then switch the visualization type to Pie Chart. Click Save As, Existing Dashboard, Analyst Dashboard # as before. Click View Dashboard or X to return to search.



1. Click back to Search and enter the following query: index=botsv3 earliest=0 sourcetype=stream:ip | iplocation src\_ip | geostats count by src\_ip latfield=lat longfield=lon globallimt=150. When you search, the Visualization of a Cluster Map should automatically show. If it doesn’t, click Visualization and select cluster map. Save this map to your existing dashboard.

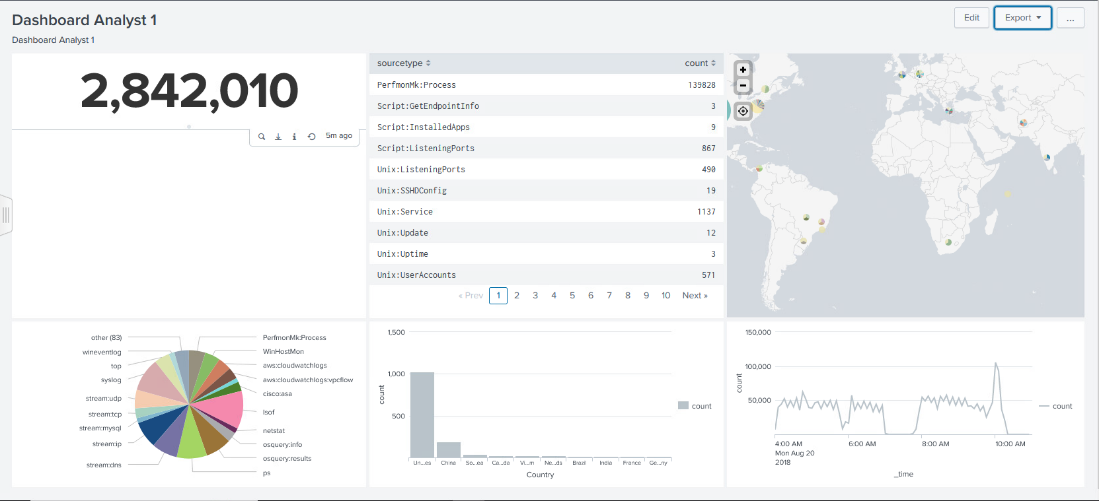




**Which countries on the map have the most network traffic as the source?**

**United States of America**

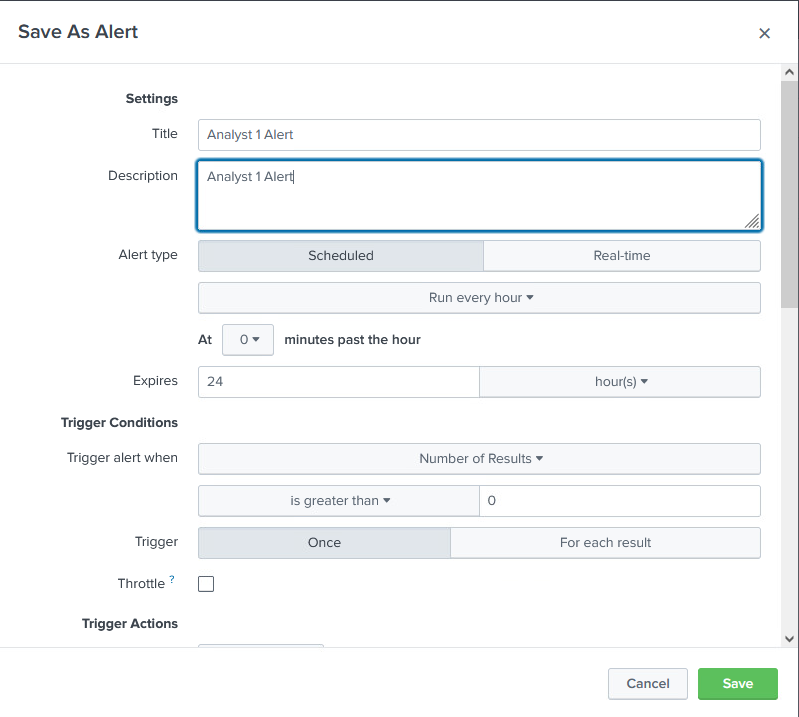
1. Click back to Search and enter the following query: index=botsv3 earliest=0 sourcetype=stream:ip | iplocation src\_ip | stats count by Country | sort –count | head 10. Click Visualization and select Column Chart. Save this column chart to your dashboard.
2. Add one more visualization to your dashboard using the query and visualization of your choosing.
3. When you are finished you should have six panels on your dashboard. When on your dashboard page, click Edit and move the panels to make the interface look nice. You can also edit the look of the visualization by clicking the paintbrush on each panel. In the dashboard below, the panels were organized into two rows of three and the stats tables we changed to only display 10 rows per page.



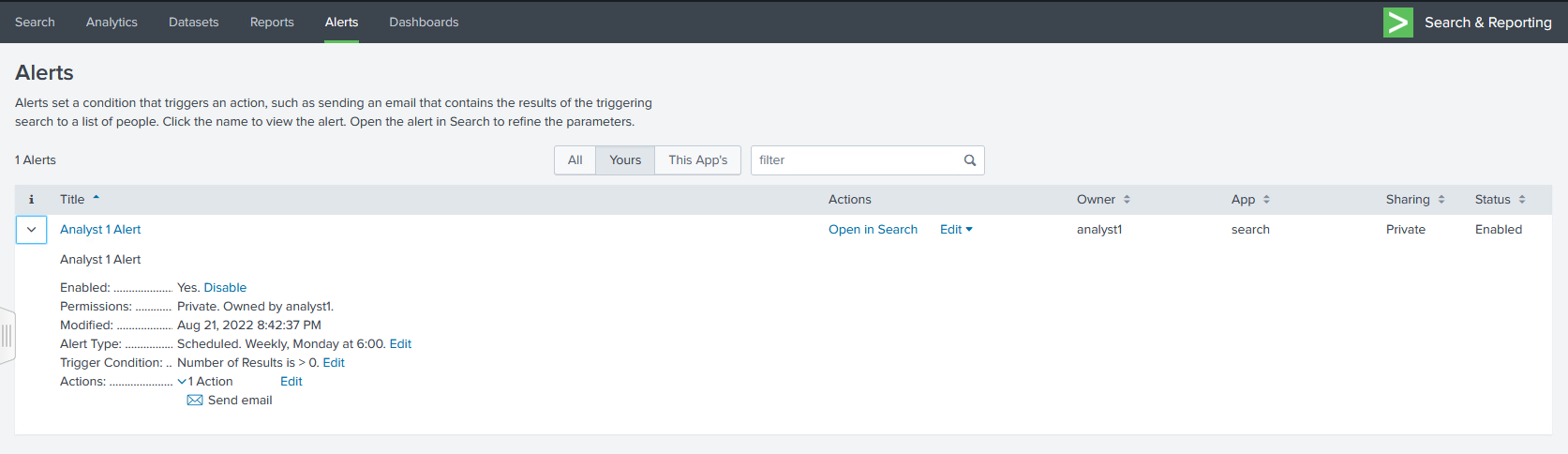
**Paste a screenshot of your own dashboard below****. A screenshot of a computer

Description automatically generated with medium confidence**

1. On the upper menu click Search and enter the query: index=botsv3. Make sure the time is set to “Last 24 hours”. Notice that there 0 events displayed. This is test data and let’s say we want to receive an alert if any more data is added to the botsv3 index. Click Save As and then Alert.
2. On the Save As Alert. Use the following values for the Alert and click save. If this alert were to trigger (any events added to the index) it would send an email to analyst#@bbtrust.com.
   1. Title: Analyst # Alert
   2. Description: Analyst # Alert
   3. Alert Type: Scheduled
   4. At \_ minutes past the hour: 0
   5. Expires: 24 hours
   6. Trigger Conditions: Number of Results
   7. Is great than: 0
   8. Trigger: Once
   9. Trigger Actions: Send Email
   10. To: [analyst#@bbtrust.com](mailto:analyst#@bbtrust.com)
   11. Priority: Normal
   12. Subject: default (Splunk Alert: $name$)
   13. Message: default (The alert condition for ‘$name$’ was triggered
   14. Include: Defaults Checked
   15. Type: HTML & Plain Text



1. Click on the Alerts Menu and select Yours, then expand the Analyst # Alert.



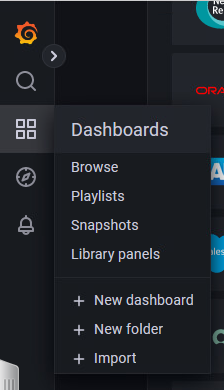
**Paste a screenshot of your own alert belowA screenshot of a computer

Description automatically generated with medium confidence**

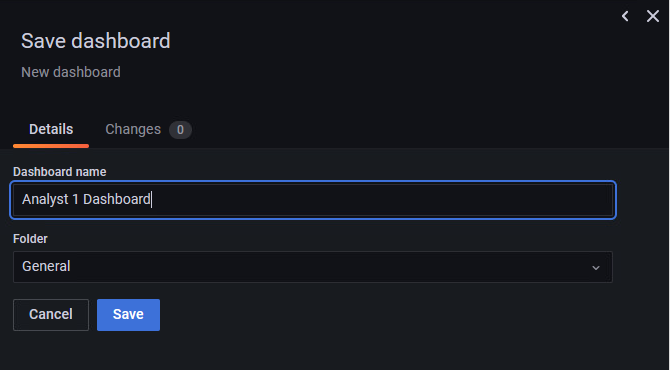
Part 2 – Dashboarding and Alerting with Grafana

Grafana is open-source and freely available platform the provides analytics and interactive visual charts and graphs that can be used to build detailed dashboards. It does not index or store its own data but can use data source plugins to access data from various other data stores. It has an interactive query builder and supports alerting when certain trigger conditions are met. This lab will have you use Grafana to build a simple dashboard based on data available in the test data set. You will also build a single alert based on that test data.

1. Access Grafana by opening a browser and navigating to <https://10.98.100.11:3002/>. You may get a warning related to the certificate not being trusted. Accept the warning and proceed to Grafana. Log in using the username analyst# and password An@lyst#!!, where # is your student/analyst number.
2. Grafana is a tool meant exclusively for dashboarding. While this lab utilizes the test data set built into the tool, it can also be used to connect to other data sources such as Loki, Graphite, Prometheus, Elasticsearch, MySQL, PostgreSQL, Microsoft SQL Server, Splunk. Salesforce, etc. Start by clicking the on the four squares icon on the left menu, then click New dashboard.

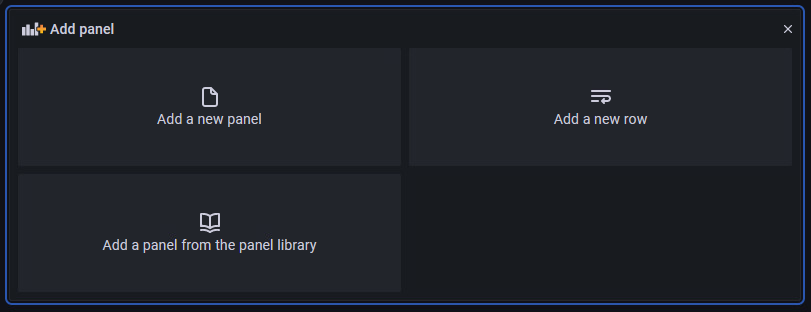


1. Start by saving the dashboard by clicking the Save icon in the upper left-hand corner of the web page. Name the dashboard Analyst # Dashboard.Save it in the General Folder.

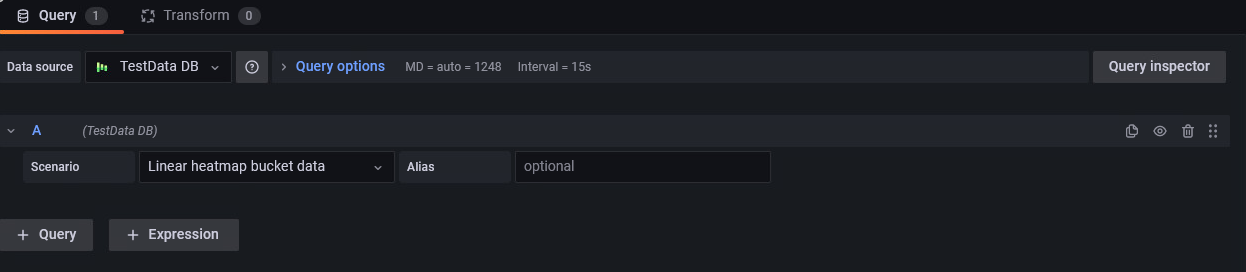


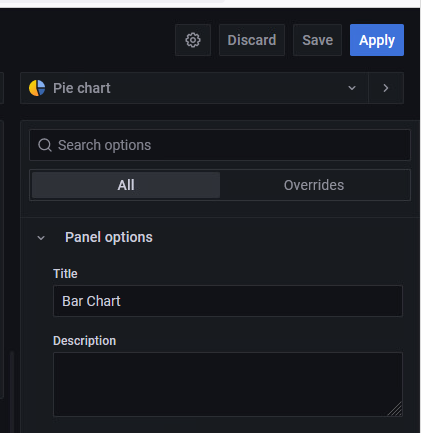
1. Click the Add Panel bar chart icon on the top right of the screen to create a new panel.

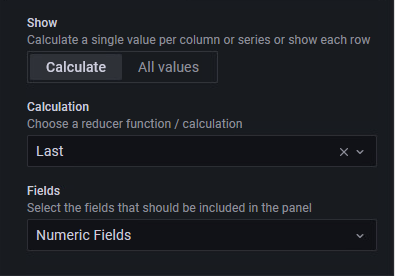




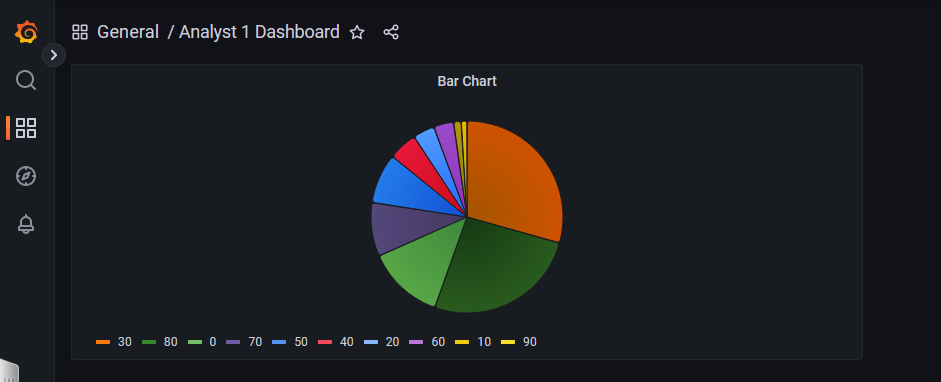
1. Click the Add Panel button within the new panel that was added. You should see a line chart with several controls. Under the Query make sure TestData DB is selected as the data source and the Scenario under data set A is set to “Linear heatmap bucket data. In the upper right-hand corner of the screen, change the time series to Pie chart. Change the Panel Title to Bar Chart. Change the Calculation option to last and in the Fields drop down select Numeric Fields.



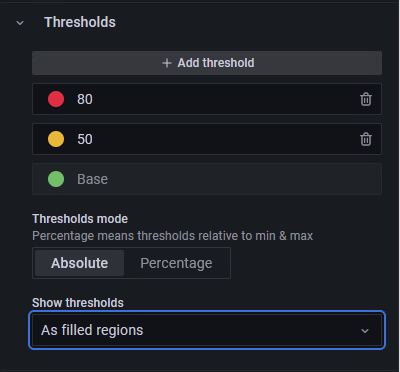




1. Click Save in the upper right-hand corner, then Save again on the dialog that appears. Then click the back arrow in the upper left-hand corner of the page to go back to the Analyst # Dashboard. You should now see a bar chart on the upper left of your dashboard.



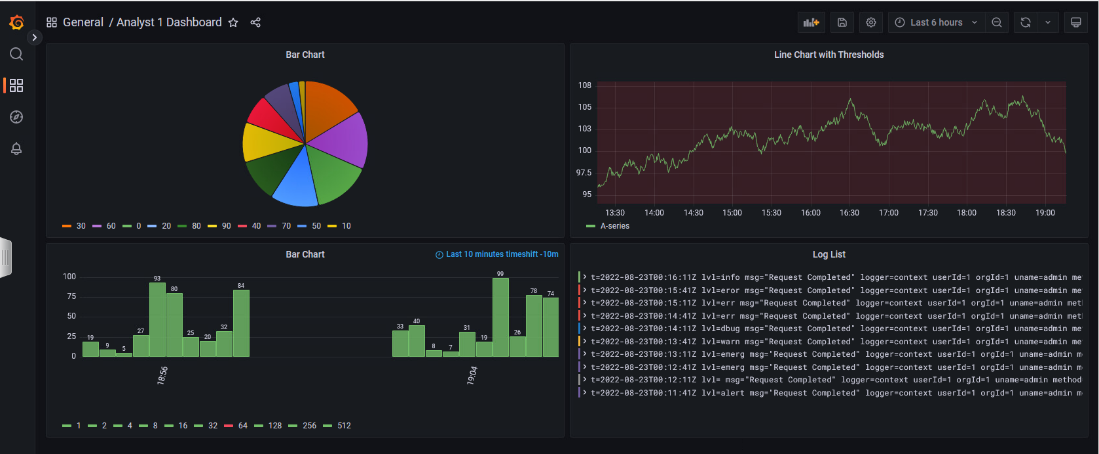
1. Click the Add Panel button again and then Add a new panel in the new panel that appears. You should see again a line chart based on the Random Walk data. Keep the defaults for the query and chart type. Edit the Thresholds for the time series data options on the left. Under the thresholds options add the following values:
   1. + Add Threshold: 80 – Red
   2. + Add Threshold: 50 – Yellow
   3. Threshold mode: Absolute
   4. Show Thresholds: As filled regions



1. Give the panel the title “Line Chart with Thresholds” and then save the panel. Use the arrow to go back to the Analyst # Dashboard. Move the panels so they are right next to each other.



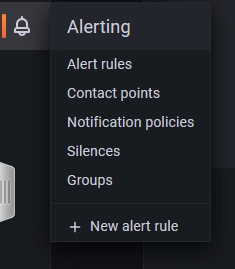
1. Based on what you have learned about Grafana, add two more panels with visualizations of your choosing to the dashboard. Take a screenshot of the panel and paste the results below. An example completed panel is also shown below.



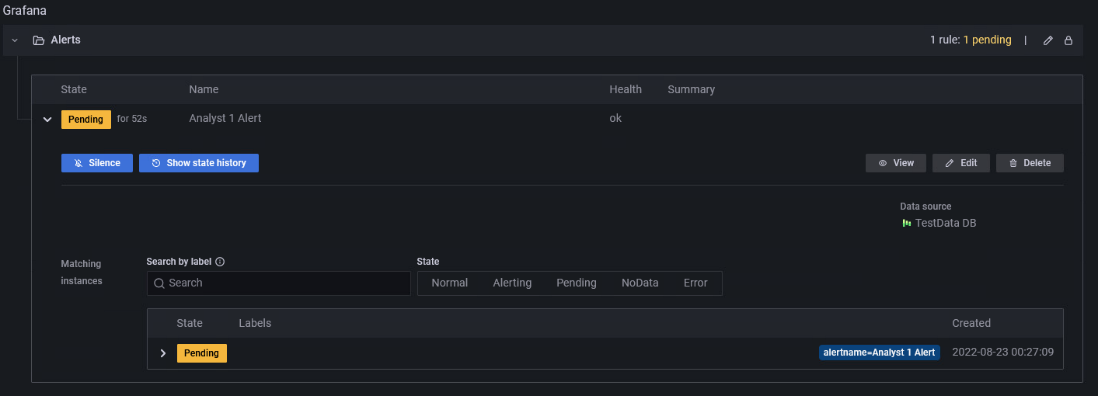
**Paste a screenshot of your own dashboard below:A screenshot of a graph

Description automatically generated with low confidence**

1. On the left side of the screen/menu, click on the alarm bell icon and then + New alert rule.



1. Make sure the following values are set on the Create alert rule:
   1. Alert Type: Grafana managed alert
   2. Time series A:
      1. Select the time dropdown next to TestDataDB and click Last 1 hour
   3. Expression B:
      1. Operation: Classic Condition
      2. Conditions:
         1. WHEN: max()
         2. OF: A
         3. IS ABOVE: 50
   4. Click Run queries to see a preview of the alert threshold based on the alert.
   5. Click Preview alerts to see the current condition for the alert (should read either Normal or Alerting)
   6. Rule Name: Analyst # Alert
   7. Folder: Alerts
   8. Group: Alerts
   9. Click save and exit
2. Click on the alert bell icon on the left side of the screen. Select Alert rules. Expand the Alerts folder and then expand the alert rule to view the details. Take a screenshot of the alert details and paste it below. An example is also included.



**Paste a screenshot of your own alert below.A screenshot of a computer

Description automatically generated with medium confidence**

1. Answer the following questions in 3-4 sentences.

**Give an example of a useful chart or visualization for SOC or CSIRT purposes.**

Incident Response Timeline

**Give an example of a useful dashboard (set of related charts and visualizations).**

Unified Dashboard Framework

**What advantages do dashboards and visualizations have over raw logs?**

It provides increased visibility, saves time, enables more collaboration, and improves decision making.

**In which situations, from a CSIRT or SOC perspective would it be appropriate to create an alert.**

When there is a potential security threat, a new vulnerability, or a new threat actor.