Splunk Dashboards and Visualizations

Cybersecurity

SIEM Day 4

Class Objectives

By the end of class, you will be able to:

- Create visualizations of single and multiple value searches.
- Use the `geostats` and `iplocation` commands to add location-based visualizations to searches.
- Combine multiple visualizations in a single dashboard.
- Modify dashboards with time range input and drilldown capabilities.

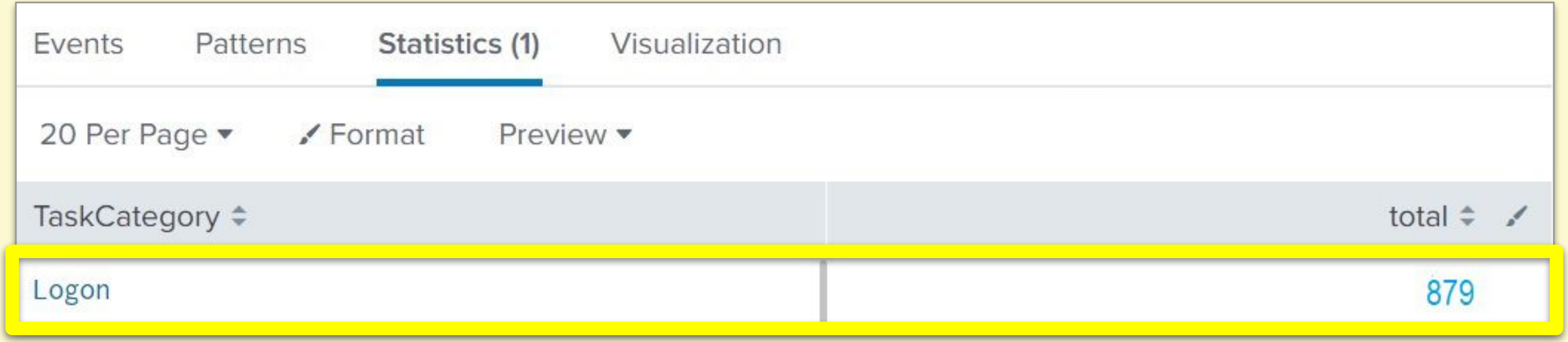
splunk® > visualizations

Today, we will expand our Splunk capabilities to include adding contextualized and informative visuals.

We will use these to analyze and research system and security issues.

Contextualizing Data

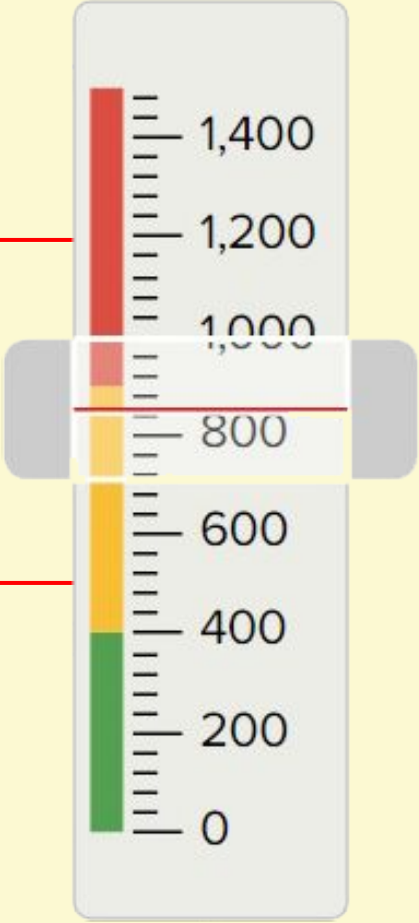
The following table shows the the number of logins per minute into a web application:



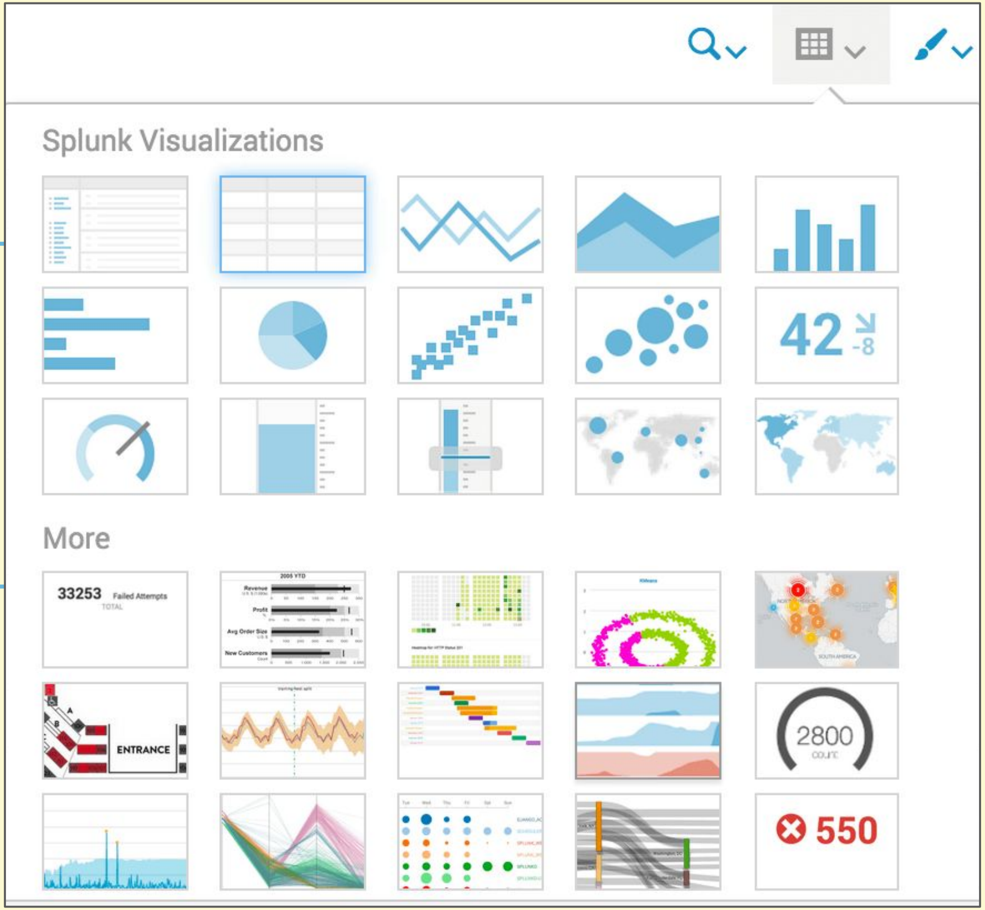
TaskCategory	total
Logon	879

Number of logins per minute

The **gauge visualization** contextualizes that number by including the severity of the login count.



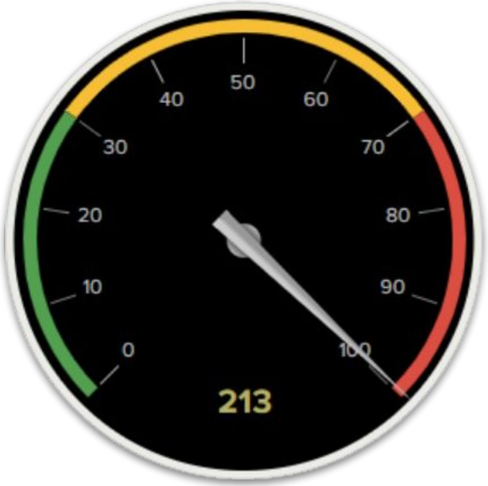
Splunk uses **visualizations** to make complex data easier to understand and analyze.



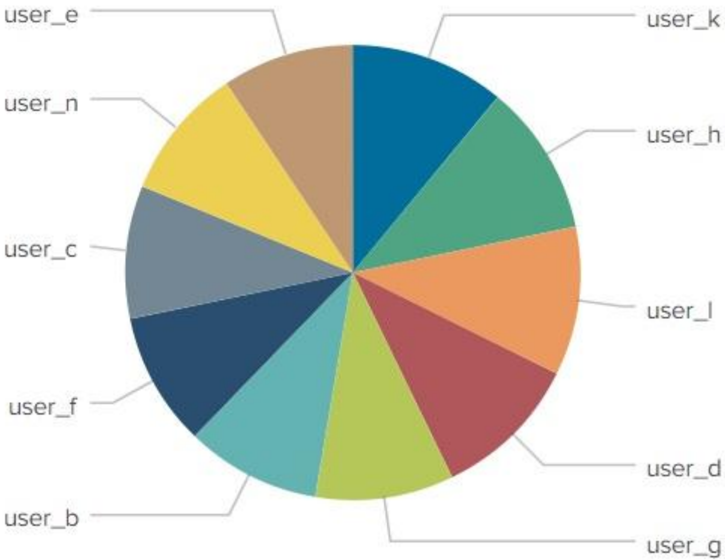
Splunk Visualizations

Splunk visualizations can display single values, such as total count of attacks, and multiple values, such as a chart of attacks correlated by attack type.

Single Value Visualizations



Multiple Value Visualizations

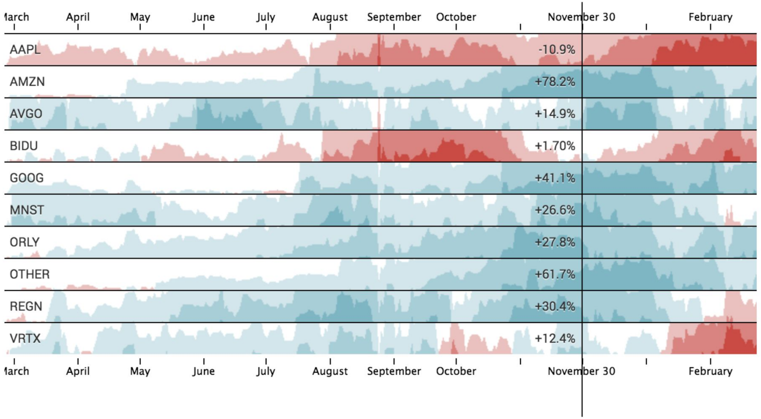


Splunk Visualizations

~~These range from simple bar and column charts to complex horizon charts and punchcards.~~

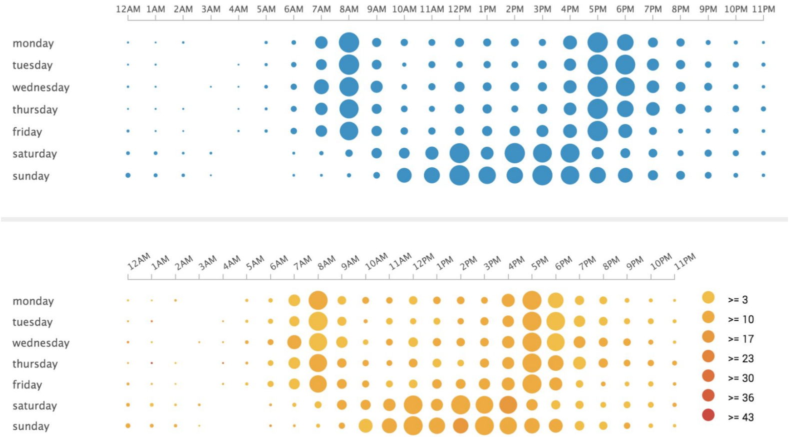
Splunk visualizations allow interactivity and offer more in-depth details.

Horizon chart



[(Horizon Chart)](#)

Punchcard



[(Punchcard)](#)

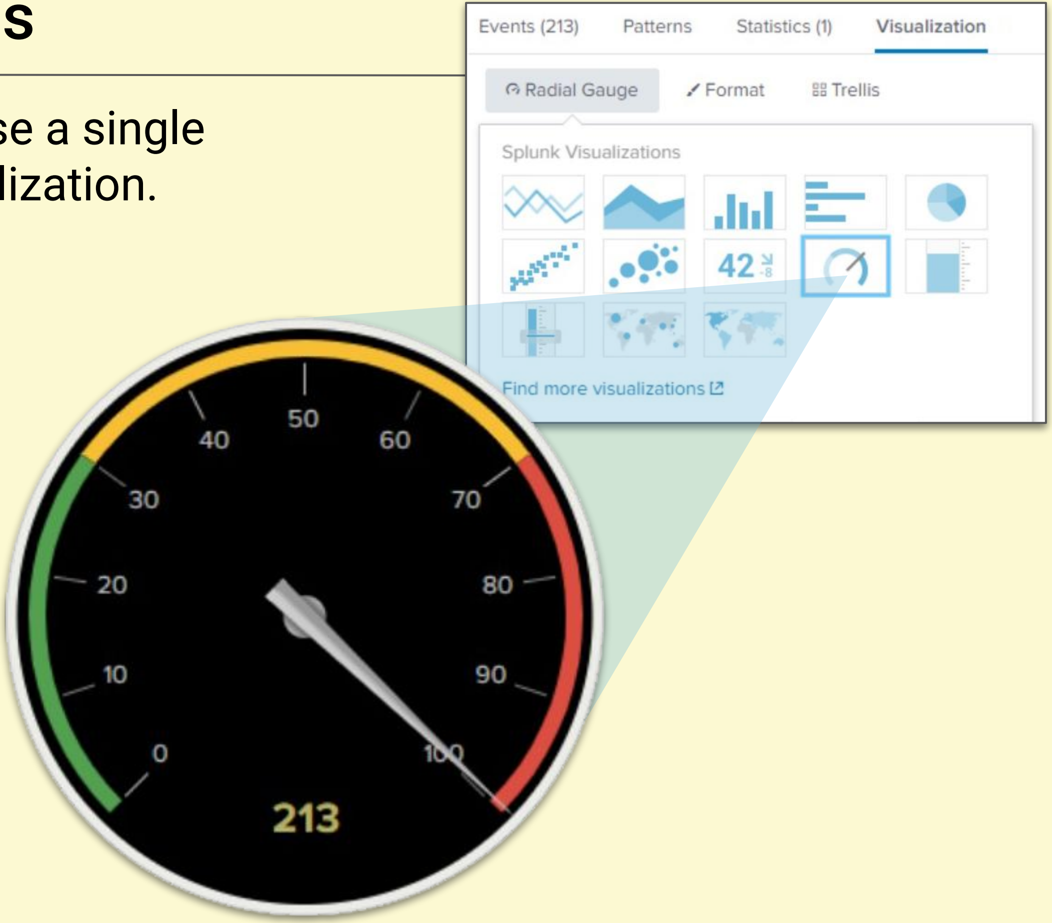
Single Value Visualizations

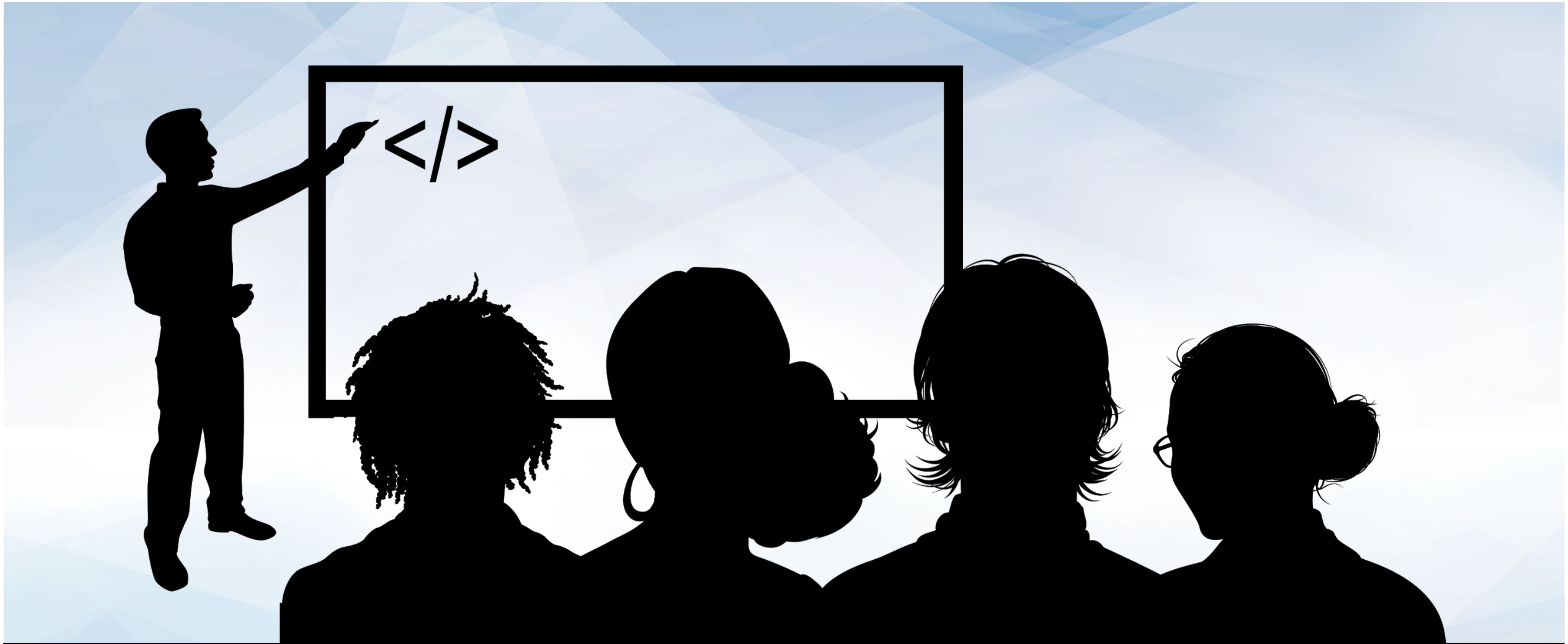
In the first demonstration, we will use a single value to create a **radial gauge** visualization.

Radial gauges are similar to the RPM dial found in the dashboard of a car.

RPM (revolutions per minute) is a single value visualized in the dial.

The dial includes a red section that indicates when the level is too high.





Instructor Demonstration

Single Value Visualization

Activity: Single Value Visualizations

In this activity, you will design a single value radial gauge to assist with monitoring attacks against your website.

Suggested Time:
15 Minutes

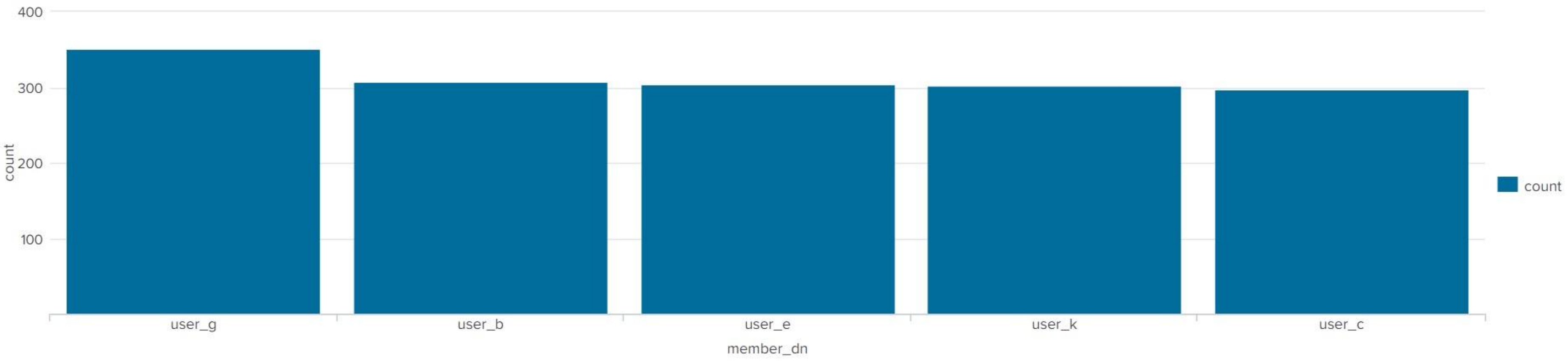
Time’s Up! Let’s Review.

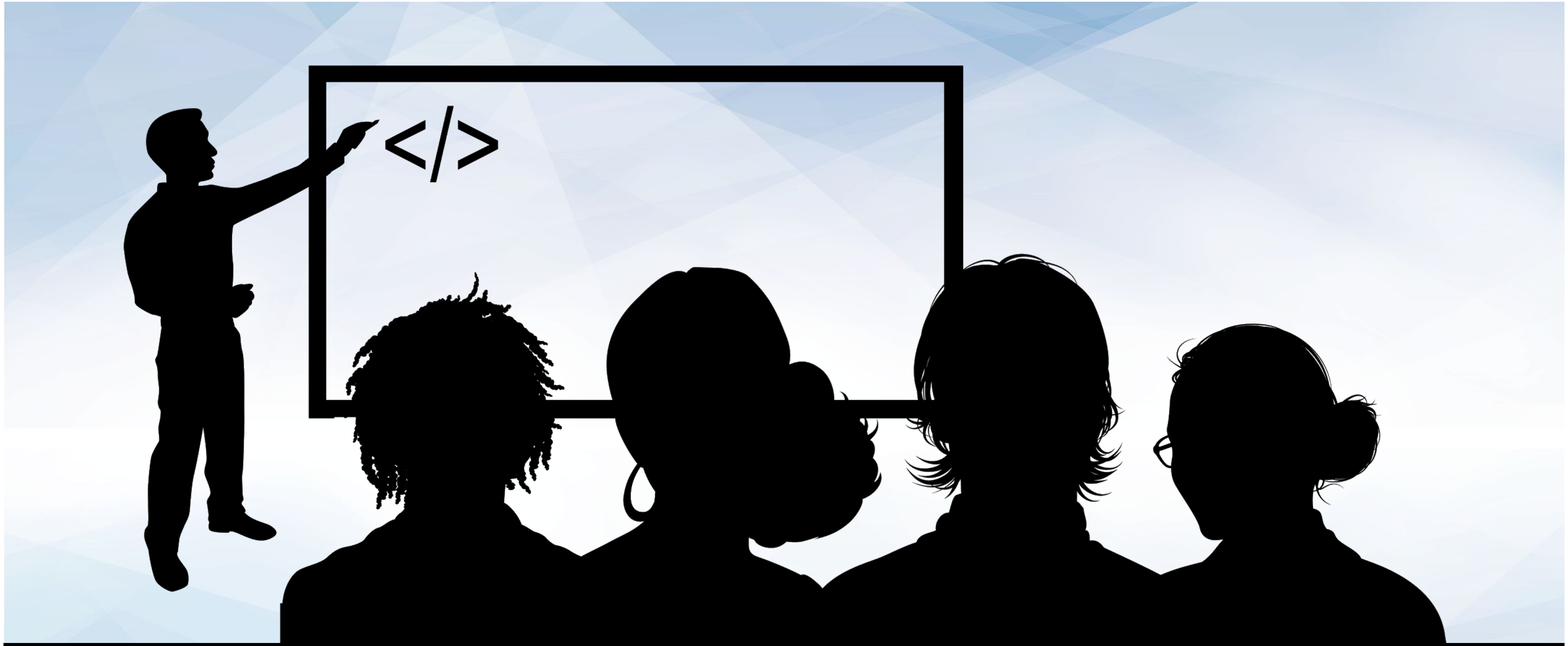
Now, we will visualize multiple values.

Multiple Values Visualization

Suppose a business is experiencing brute force attacks against a web application. They want want to visualize the list of users being attacked and the number of attacks experienced by each user.

We can convert Splunk stat spreadsheets into more informative and interactive visualizations:





Instructor Demonstration

Multiple Value Visualization

Activity: Multiple Value Visualizations

In this activity, you will design a multiple value visualization to display the URL paths being targeted by the POST requests.

Suggested Time:
15 Minutes

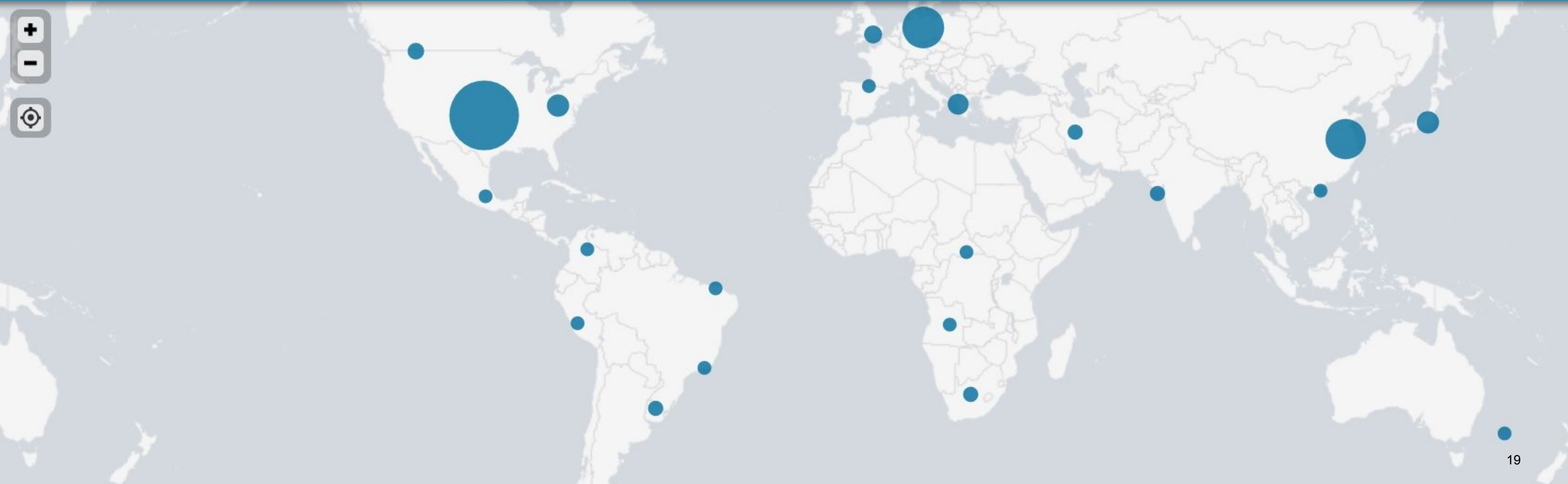
Time’s Up! Let’s Review.

Geographic Map Visualization

Organizations can monitor **where** users access their application from to help determine the source of security issues.

For example

A business knows that their application customers are primarily located in the United States. If they find out a significant number of users have started accessing their application from somewhere else, they will take this as a cue to investigate the activity.



Geographic Map Visualization

To create these maps and gain more insight into the locations of activity, we will use the following commands:

01

The `iplocation` command

will output the city and country data of an IP field, such as `src_ip` or `dest_ip`.

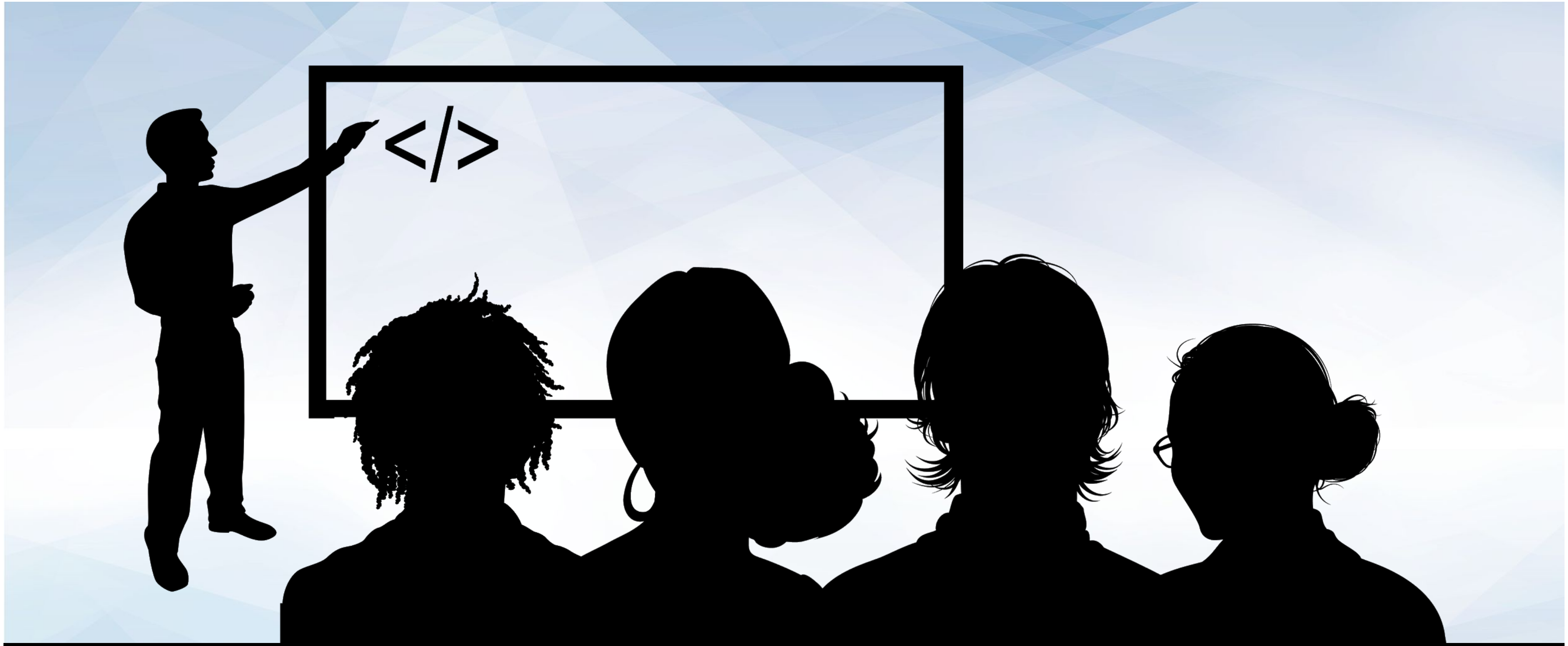
```
sourcetype="stream:http" | iplocation src_ip
```

02

The `geostats` command

uses the location data found with the `iplocation` command to map latitude and longitude data for each event.

```
sourcetype="stream:http" | iplocation src_ip | geostats count
```



Instructor Demonstration

Geographic Map Visualization

Activity: Geographic Map Visualizations

In this activity, you will design a geographic map visualization to help your SOC team understand where attacks are originating.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

splunk®> dashboards

While the visualizations we’ve covered so far are useful on their own, they are even more effective when grouped and displayed together.

Dashboards

For example, an organization that is monitoring a website may want to view all of the following at the same time:

01 The volume of **successful logins** on the website.

02 The volume of **unsuccessful logins** on the website.

03 A **geographic map** illustrating where the activity is coming from.

04 A **pie chart** displaying the specific pages of the website that are being accessed.

Dashboards

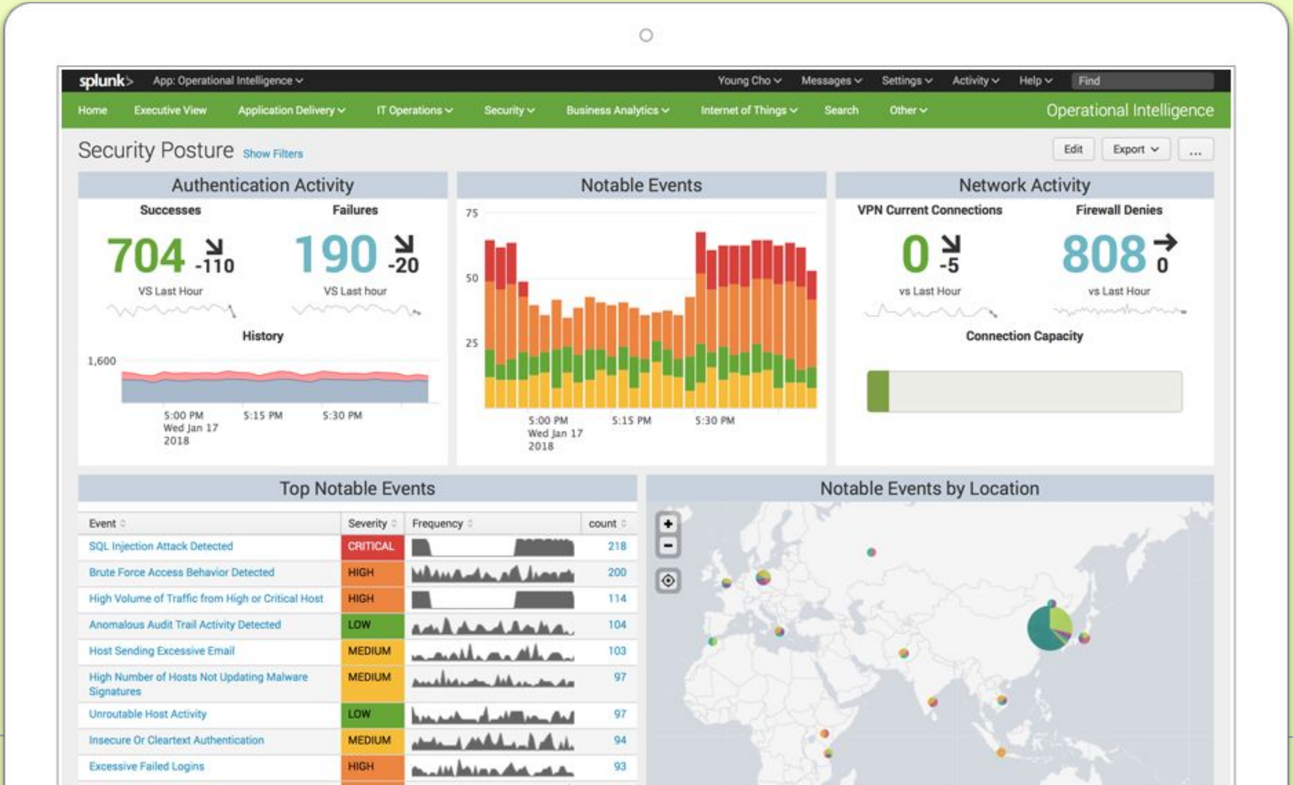
Viewing all this information together can provide a security analyst with a complete picture of the state of their web application.

(Source)

Dashboards are a collection of multiple visualizations in a single location.

Dashboards

The **visualizations** are placed in different sections, called panels.



Top Notable Events

Event	Severity	Frequency	count
SQL Injection Attack Detected	CRITICAL		218
Brute Force Access Behavior Detected	HIGH		200
High Volume of Traffic from High or Critical Host	HIGH		114
Anomalous Audit Trail Activity Detected	LOW		104
Host Sending Excessive Email	MEDIUM		103
High Number of Hosts Not Updating Malware Signatures	MEDIUM		97
Unroutable Host Activity	LOW		97
Insecure Or Cleartext Authentication	MEDIUM		94
Excessive Failed Logins	HIGH		93

(Splunk.com)

SOCs often have dashboards displayed on multiple screens in their operations room to provide availability and functionality across their staff.

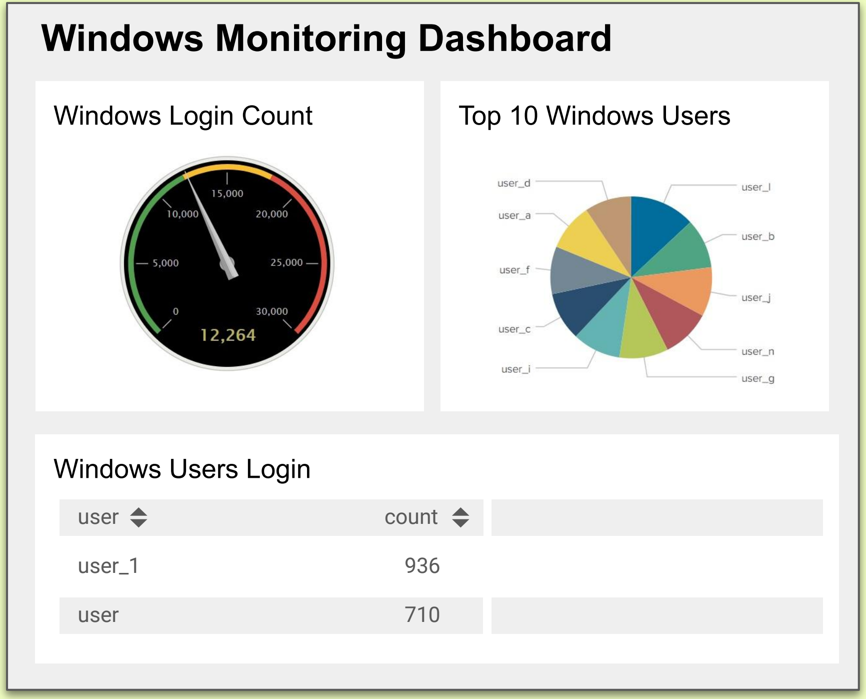
Dashboard Demo Scenario

As a SOC manager, you would like to create a single three-panel dashboard to monitor your Windows server. You want the panels to include:

01 A radial gauge of successful logins.

02 A pie chart of users logging in.

03 A statistical chart of the data in the pie chart.



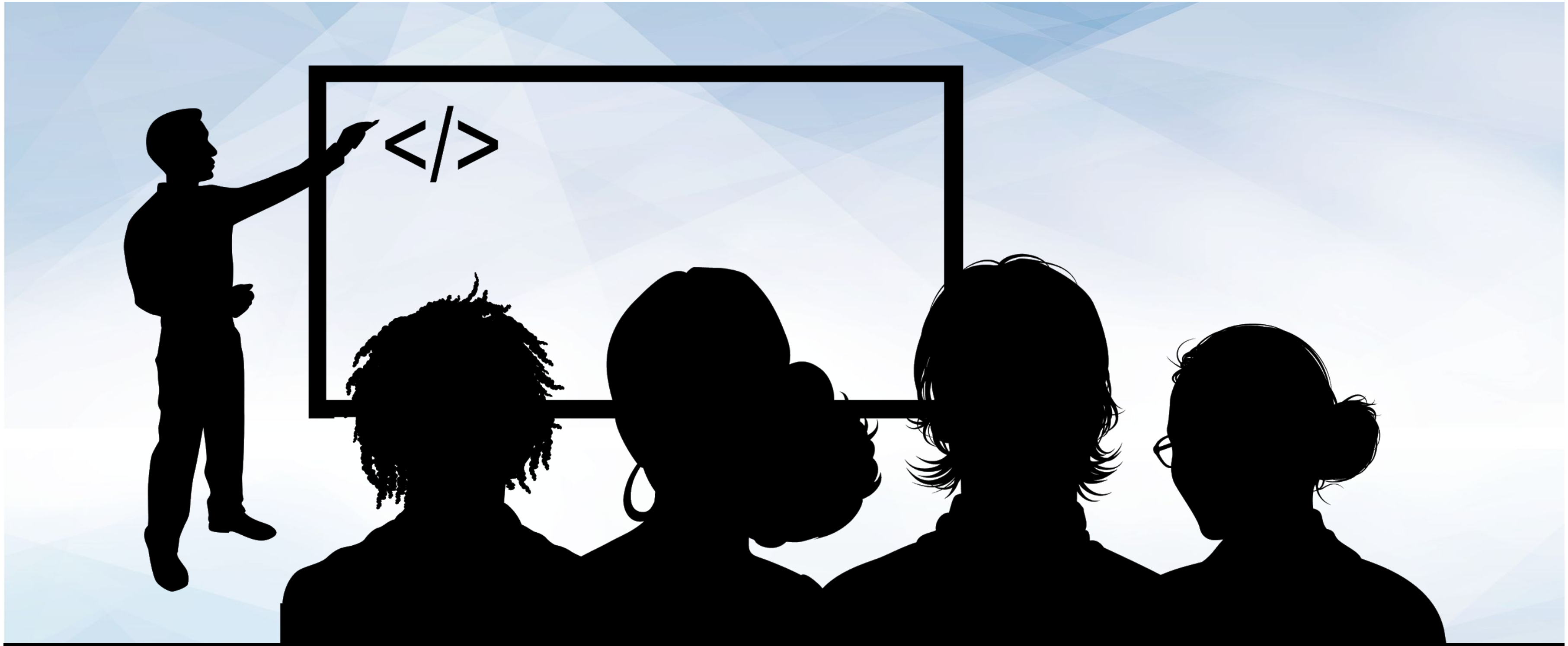
Windows Monitoring Dashboard

Windows Login Count

Top 10 Windows Users

Windows Users Login

user	count
user_1	936
user	710



Instructor Demonstration

Creating Dashboards

Activity: Creating Dashboards

In this activity, you will design a dashboard to view all of the visualizations we’ve made, in a single location.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Next, we'll take these dashboards a step further by adding drill downs and interactivity.

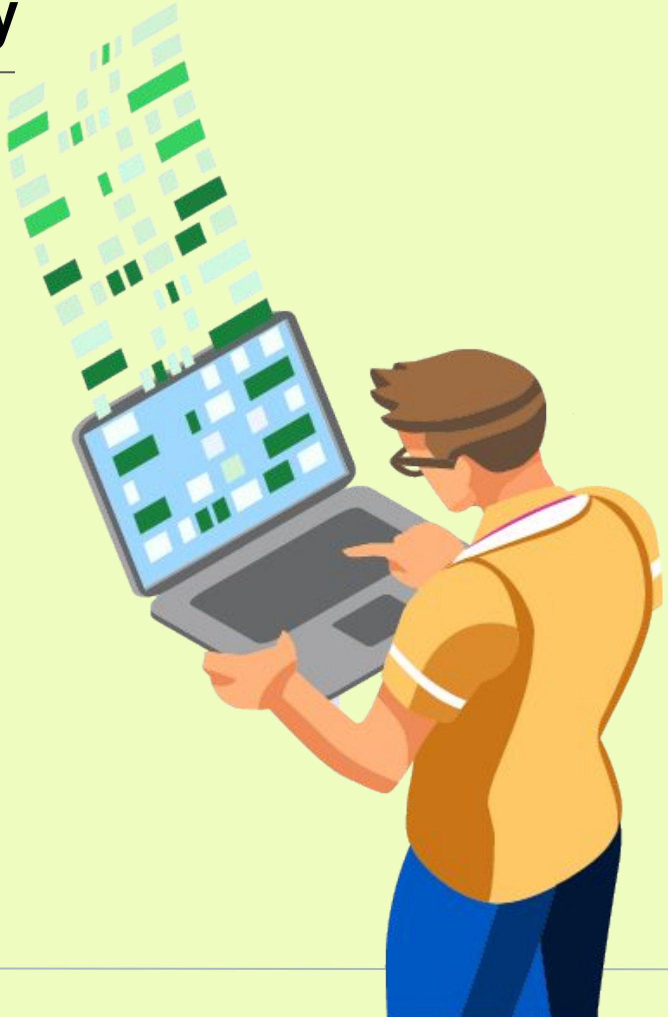
Dashboard Drilldowns and Interactivity

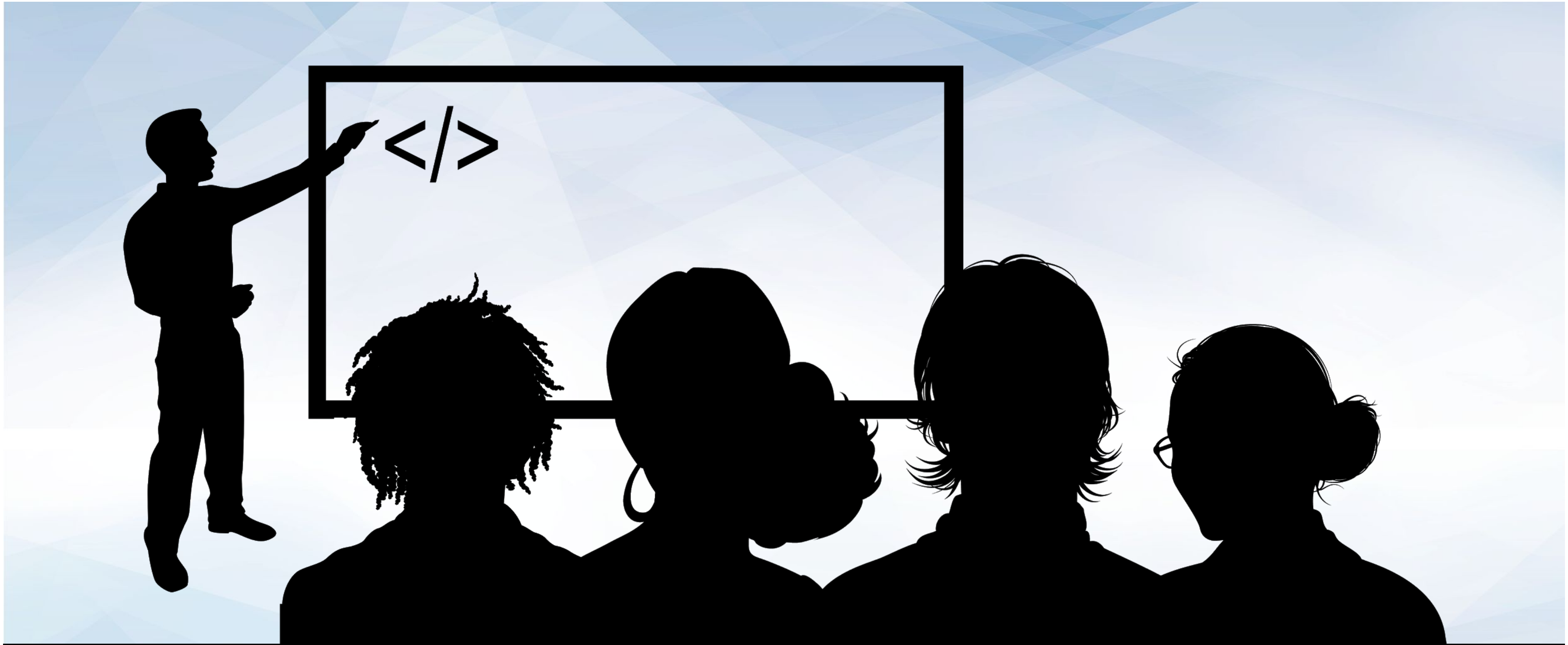
We will walk through how to configure these features by using the dashboard and scenario from the last demonstration.

As a SOC manager, you created a three-panel dashboard to monitor your Windows server.

You will expand the functionality of this dashboard by:

- Modifying the date and time ranges being analyzed directly on the dashboard.
- Adding a drilldown into the visualizations to assist with further analysis.





Instructor Demonstration

Dashboard Drilldowns and Interactivity

Activity: Advanced Dashboards

In this activity, you will enhance your dashboard by adding drilldowns and interactivity features.

Suggested Time:
0:15

Time’s Up! Let’s Review.

The End