

Cybersecurity

Splunk Dashboards and Visualizations

Lesson 20.1

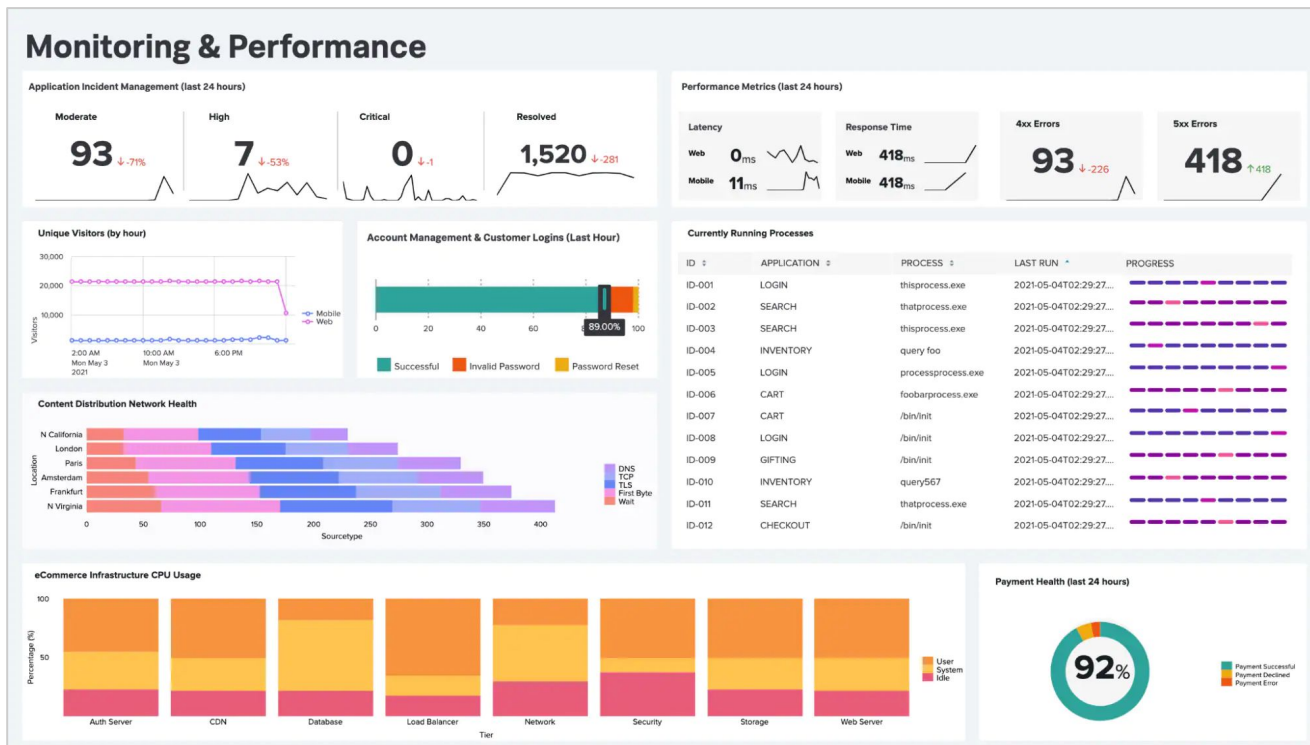


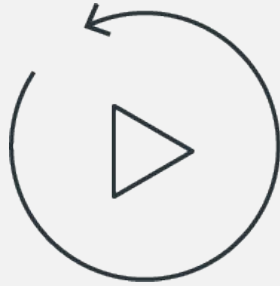
Class Objectives

By the end of class, you'll be able to:

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

Today, we'll learn how security professionals use Splunk's visualization capabilities to identify and mitigate security issues.





Let's recap



Recap: Splunk

Let's first review the last class:

1

Splunk uses the Statistics feature to display specific values from search results in an easy-to-read spreadsheet.

2

The `eval` command is used to design new fields or modify existing fields.

3

Splunk uses reports to save searches and run them at designated times.

4

Splunk alerts are designed to send automatic notifications when a specific condition, known as a trigger condition, is met.

Recap: Alerts

Designing poor alerts can cause two types of issues:

01

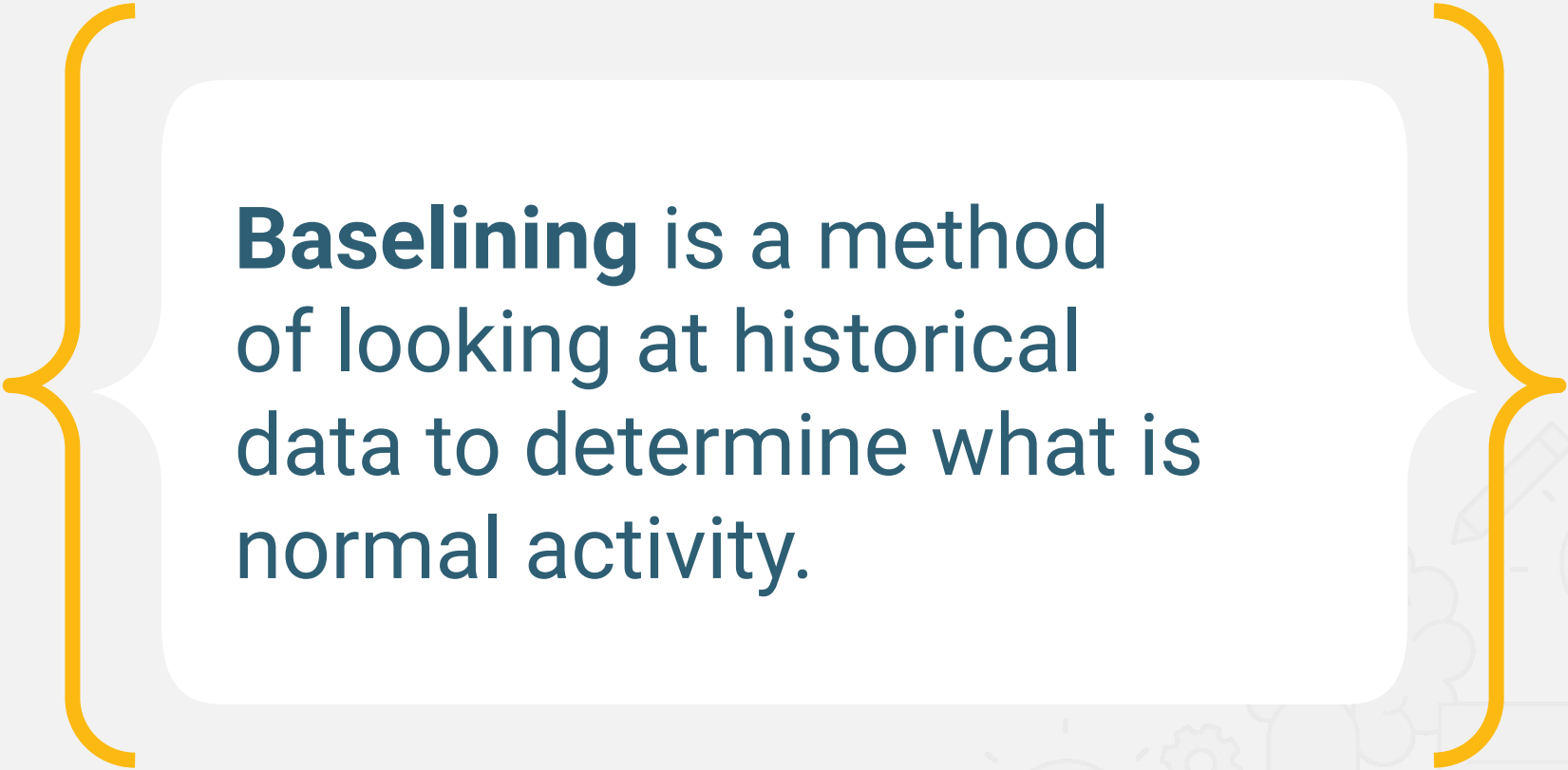
False positives

When conditions are met and an alert is triggered, but the security situation being monitored did not actually occur

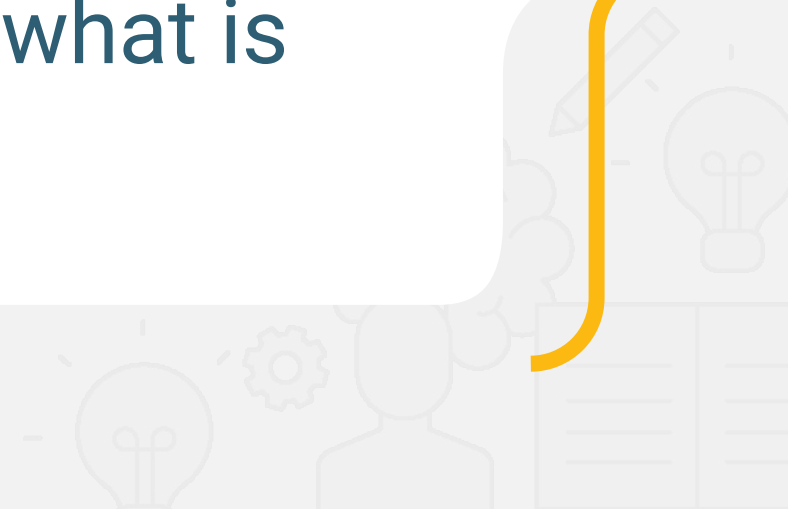
02

False negatives

When the condition is met and an alert is not triggered, meaning the security situation occurred undetected



Baselining is a method of looking at historical data to determine what is normal activity.



Recap: Baselineing

Security professionals use **baselineing** to determine a threshold: the condition or level that, when met, triggers an alert.

Setting the threshold **too high**
risks missing an alert.

Setting the threshold **too low**
creates too many false positives.





Security professionals may encounter the challenge of **alert fatigue**.

This occurs when they receive so many alerts that they cannot adequately respond to each one.



Introduction to **Visualizations**

Introduction to Visualizations

Today, we'll use Splunk to create contextualized and informative visuals.

We'll use these to analyze and research system and security issues.



Contextualizing Data

Example: Table showing the number of logins to a web application per minute

Events Patterns **Statistics (1)** Visualization

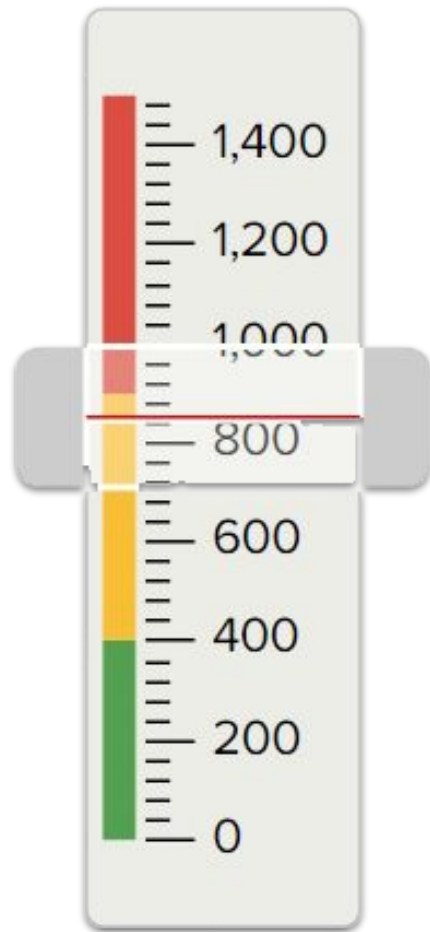
20 Per Page ▼ ✎ Format Preview ▼

TaskCategory ▴ ▾	total ▴ ▾ ✎
Logon	879

Number of logins per minute

Contextualizing Data

The **gauge visualization** contextualizes the number 879 by highlighting the severity of the login count.



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



More

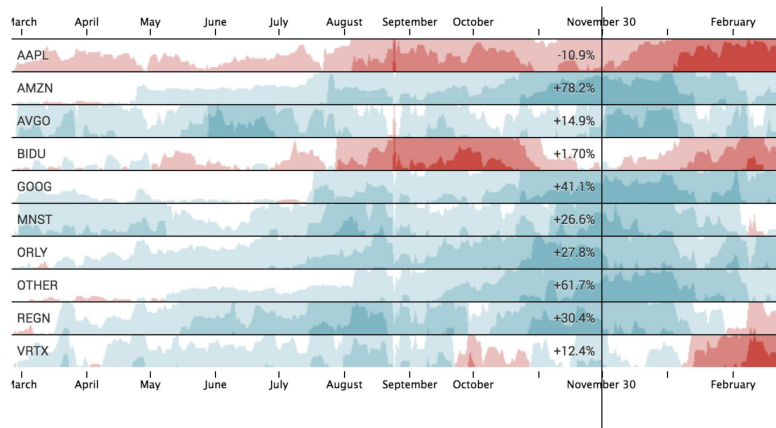


Splunk Visualizations

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

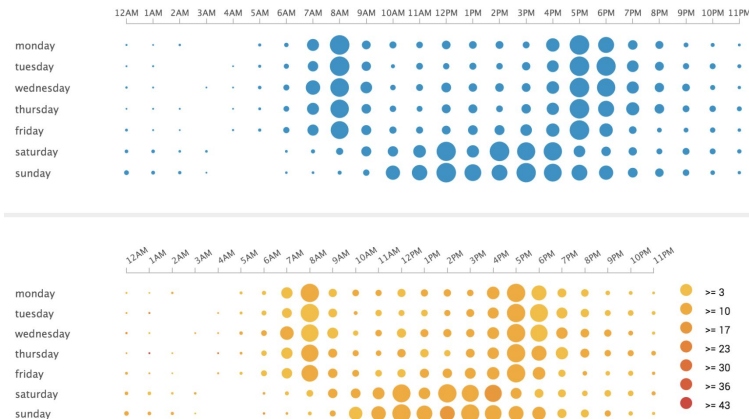
These visualizations range from simple bar and column charts to more complex horizon charts and punch cards.

Horizon chart



(Horizon Chart)

Punch card



(Punchcard)

Splunk Visualizations

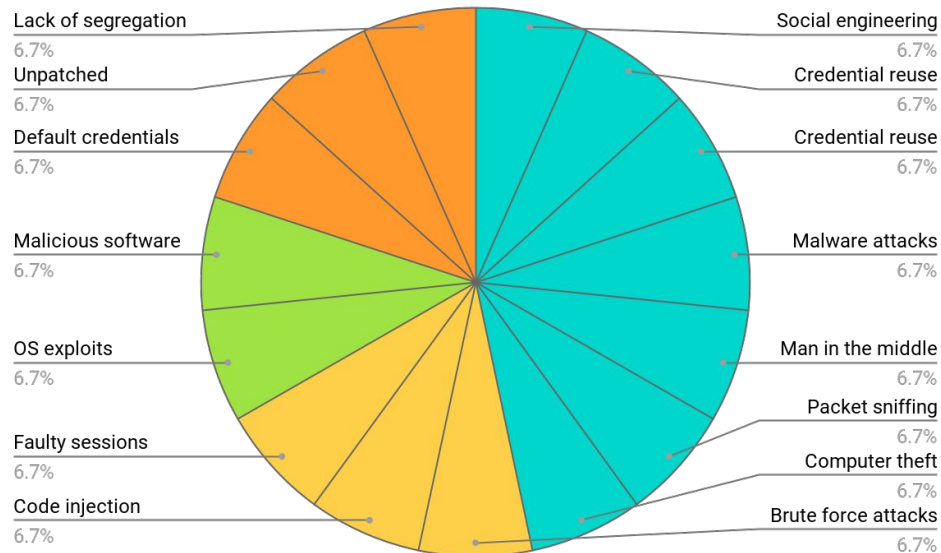
Splunk visualizations can display single values, such as total attacks, or multiple values, such as attacks correlated by attack type.

Single-value visualizations



Multiple-value visualizations

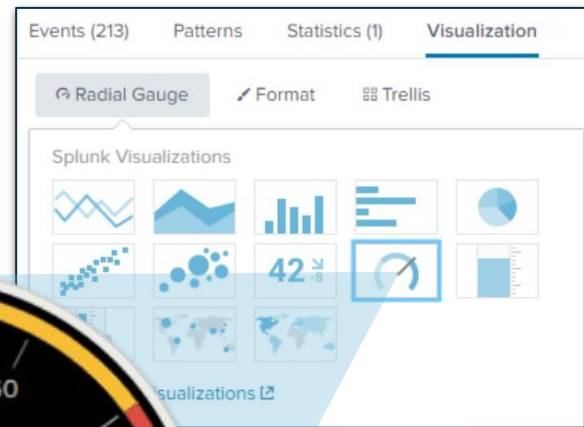
- Database attacks
- Server attacks
- Web attacks
- User attacks



Single-value Visualizations

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

- Radial gauges are similar to the RPM dial in a car dashboard.
- 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'll design a single-value radial gauge to help monitor attacks against your website.

Suggested Time:
15 Minutes





Time's up!
Let's review



Questions?





Multiple-value **Visualizations**

Multiple-value Visualizations

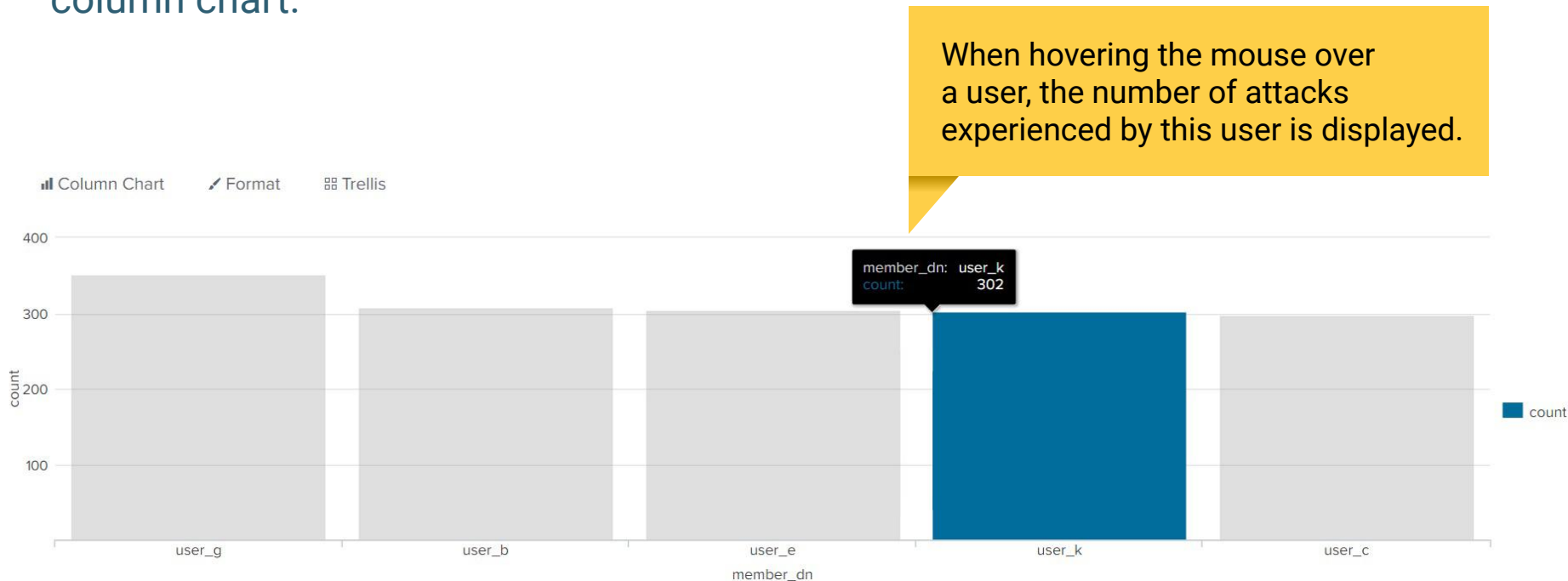
Suppose a business is experiencing brute-force attacks against a web application.

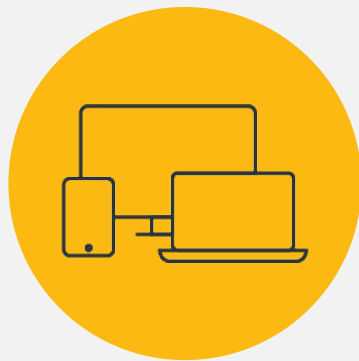
The SOC manager wants to visualize the list of users being attacked and the number of attacks experienced by each user.



Multiple-value Visualizations

We can convert Splunk stat spreadsheets into more informative and interactive visualizations. The data found in the spreadsheet can be displayed in a column chart.





Instructor **Demonstration**

Multiple-value Visualization



Activity:

Multiple-value Visualizations

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

Suggested Time:
15 Minutes





Time's up!
Let's review



Questions?

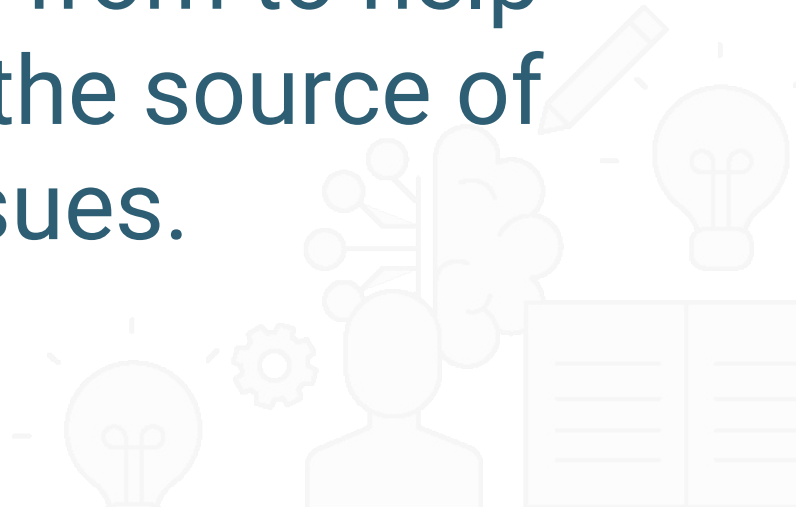




Geographic Map **Visualizations**



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



Geographic Map Visualization

Example:

A business knows that its application customers are primarily located in the United States. A significant number of users accessing the application from another place is a cue to investigate the activity.



Geographic Map Visualization

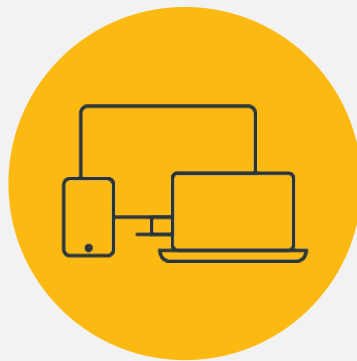
To create these maps and gain insight into the locations of activity, we'll use the following commands:

The **iplocation** command outputs the city and country data of an IP field, such as **src_ip** or **dest_ip**.

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

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 Visualization

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

Suggested Time:
15 Minutes





Time's up!
Let's review



Questions?





Break
15 mins



Splunk Dashboards

Splunk Dashboards

So far, we've covered the following visualizations:

Single value



Multiple values



Geographic maps



Splunk Dashboards

While each of these visualizations is useful on its own, they are even more effective when grouped and displayed together.

Single value



Multiple values



Geographic maps



Splunk Dashboards

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

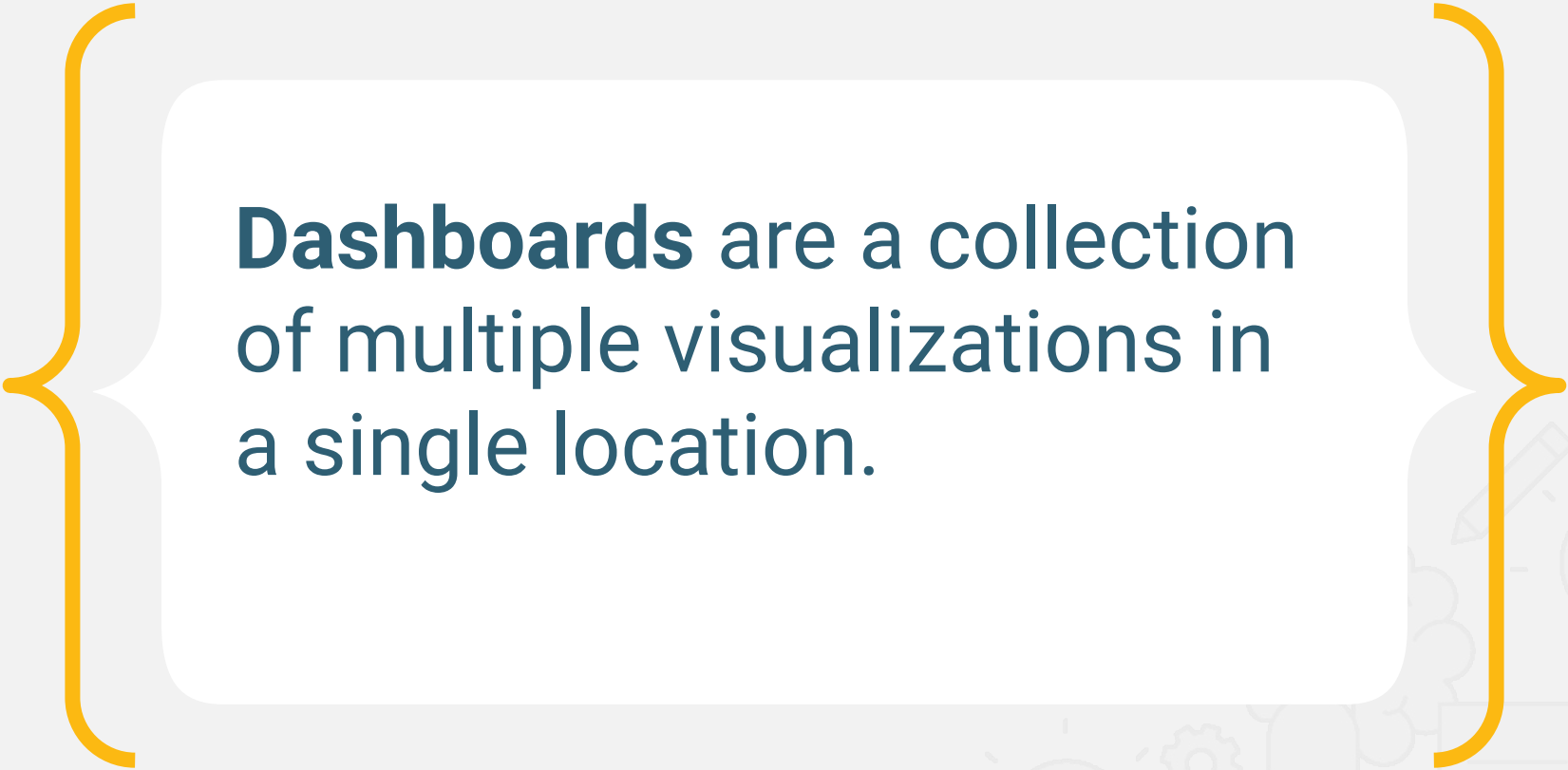
A geographic map illustrating where the activity is coming from

04


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

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





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

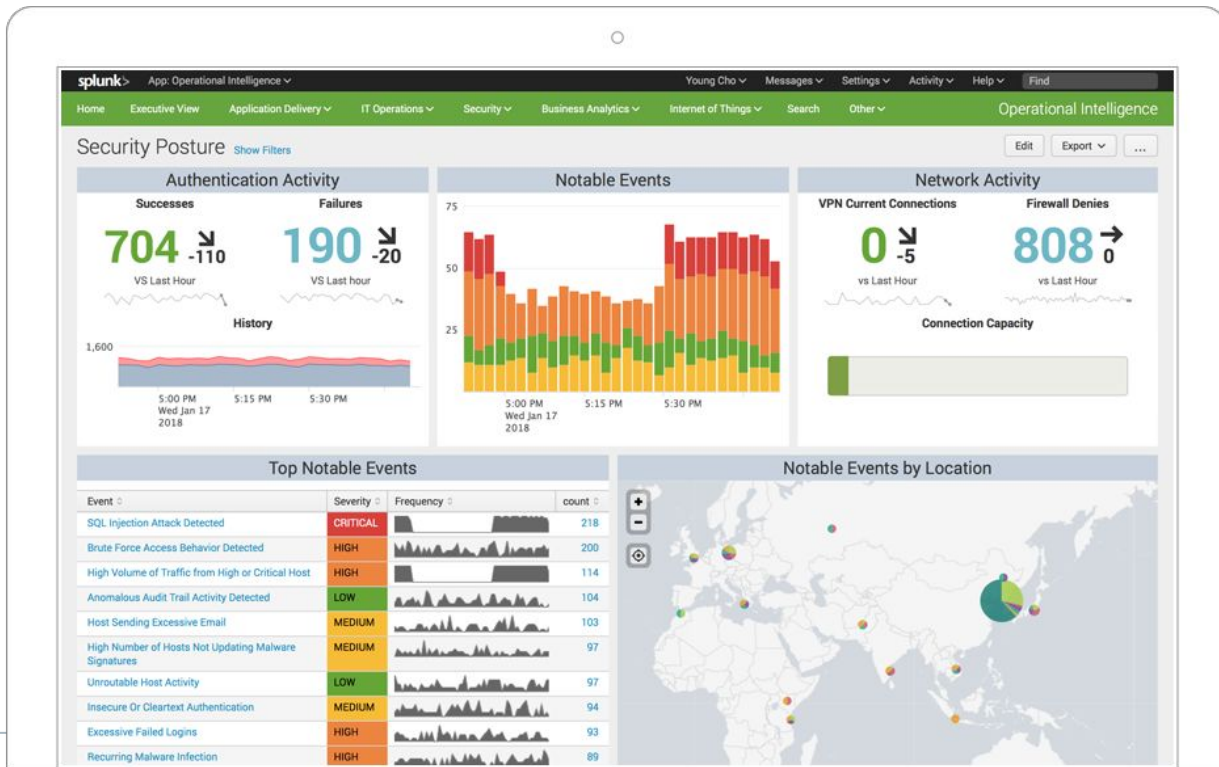


Dashboards

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

Panels can contain:

- Single-value visualizations
- Multiple-value visualizations
- Geographic maps
- Statistical charts



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

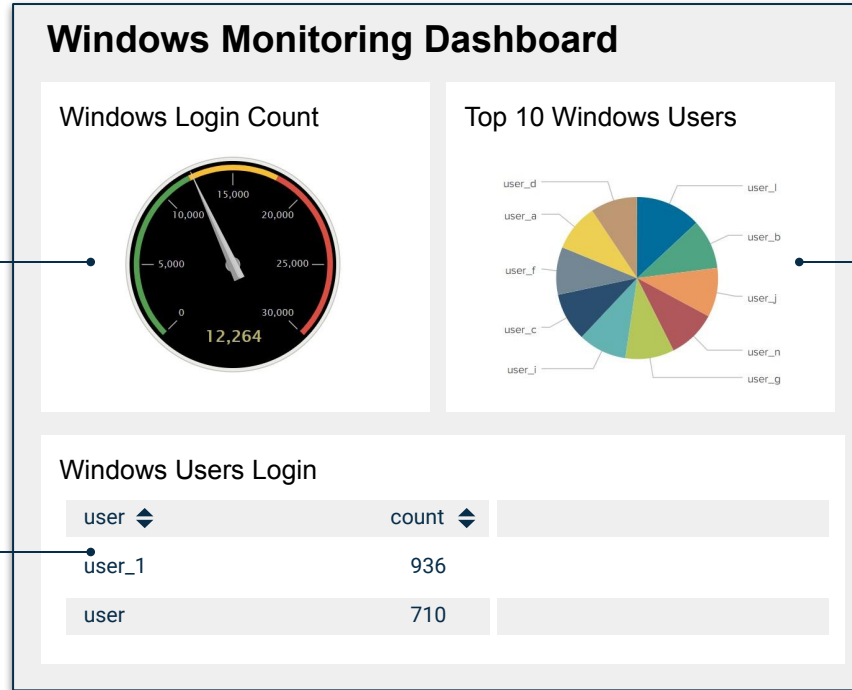


Dashboard Demo Scenario

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

A **radial gauge** of successful logins

A **statistical chart** of the data in the pie chart



A **pie chart** of users logging in



Instructor **Demonstration**

Creating Dashboards



Activity:

Creating Dashboards

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

Suggested Time:
15 Minutes





Time's up!
Let's review



Questions?



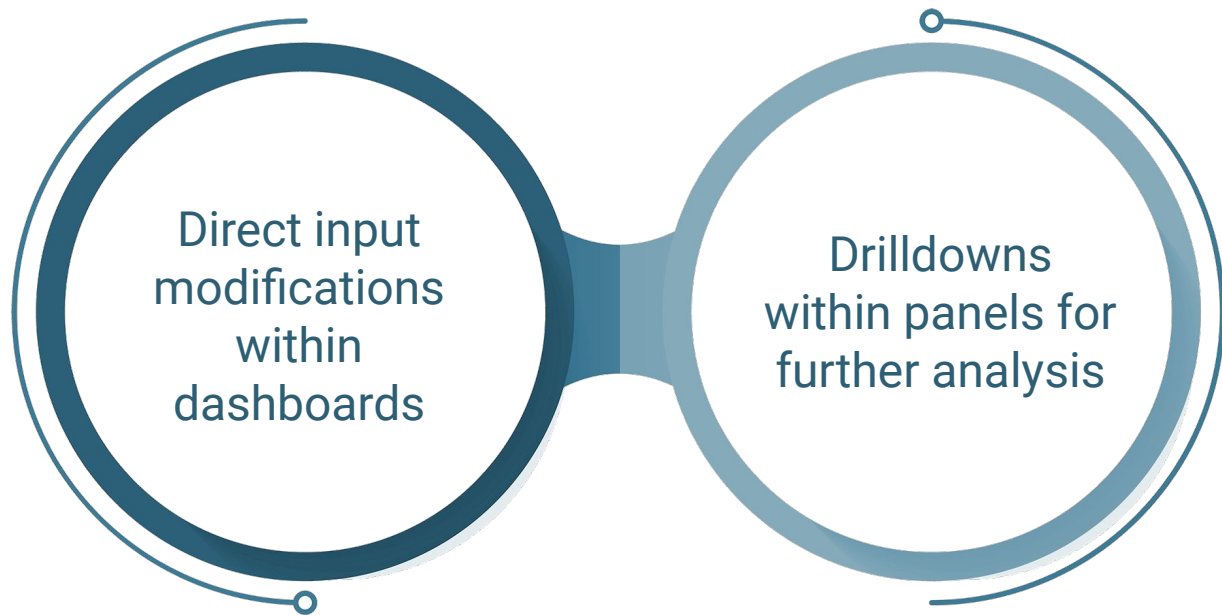


Drilldowns and Dashboard Interactivity

Drilldowns and Dashboard Interactivity

Similar to many other applications in Splunk, dashboards have advanced features that can help information security professionals research security issues.

These include:



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

Drilldowns and Dashboard Interactivity

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

You will expand the functionality of this dashboard by:

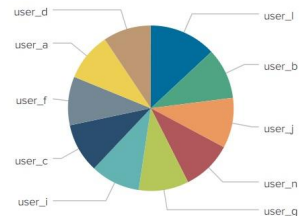
- Modifying the date and time ranges being analyzed directly on the dashboard
- Adding a drilldown into the visualizations to assist with further analysis

Windows Monitoring Dashboard

Windows Login Count



Top 10 Windows Users



Windows Users Login

user	count	
user_1	936	
user	710	



Instructor **Demonstration**

Drilldowns and Dashboard Interactivity



Activity:

Advanced Dashboards

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

Suggested Time:
15 Minutes





Time's up!
Let's review



Questions?





The End