Splunk Searches

Cybersecurity

SIEM Day 2

Class Objectives

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

- Explore and select Splunk add-ons and apps based on project needs.
- Upload logs into a Splunk repository.
- Create complex SPL queries to analyze specific security situations.

Today we will use a powerful **big data tool** offered by the software company Splunk.

Introducing Splunk

Splunk is...

a software tool that searches, analyzes, and monitors big data with an easy-to-use interface.

Splunk can...

capture large amounts of incoming data, and create visualizations, reports, and alerts.

Splunk has...

a base product designed to conduct basic tasks such as searching and reporting.

Introducing Splunk

While our focus this week is on Splunk's benefits to infosec industry, Splunk is useful for a variety of industries, such as:

01

Finance

02

Utilities

03

Healthcare

Finance

For example, financial organizations can use Splunk to analyze mortgage rates to determine future rate changes.

Utilities

For example, gas companies can use Splunk to monitor customer use levels.

Healthcare

For example, medical researchers can use Splunk to create reports and metrics for analyzing successes of medical trials.

Apps, Add-Ons, and Suites

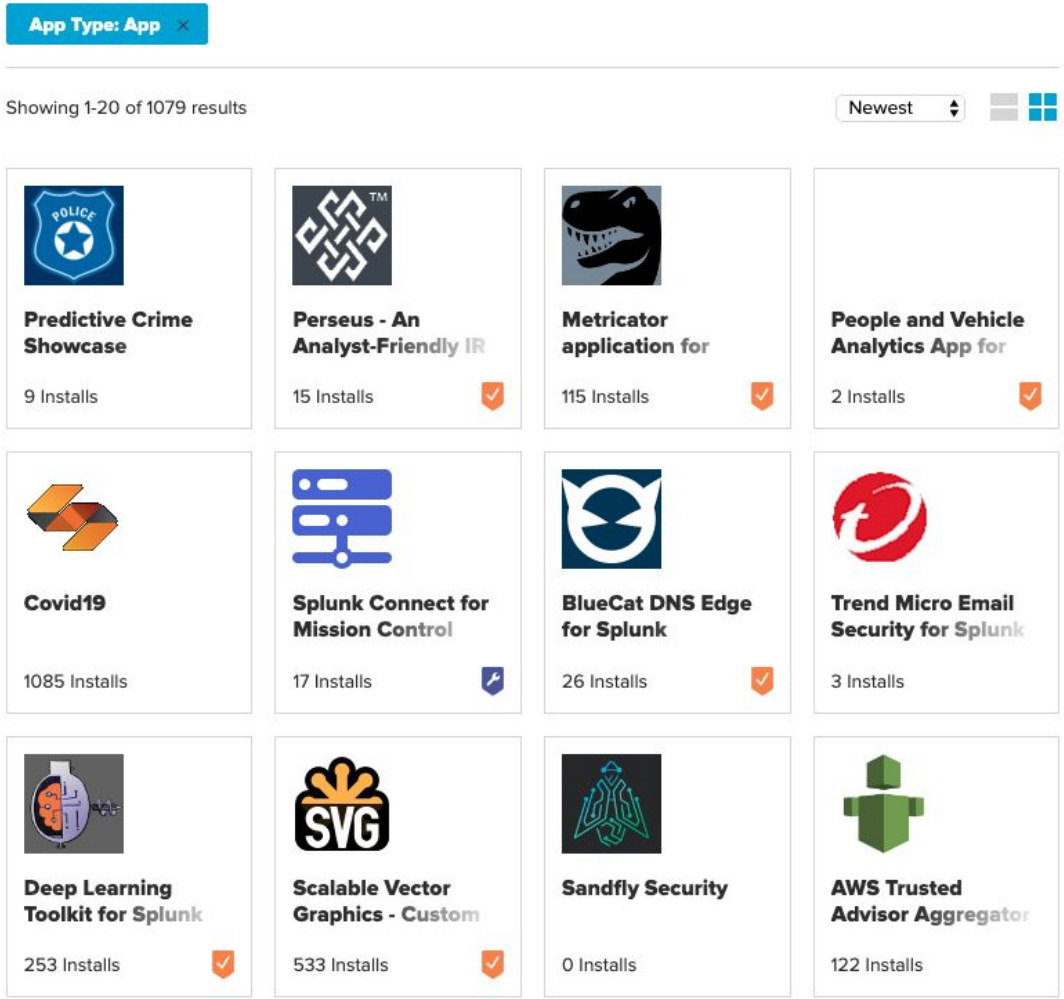
Splunk can be used for these industry-specific tasks by adding the following to the base product: Splunk apps, Splunk add-ons, and Splunk suites.

(splunk.com)

Splunk Apps

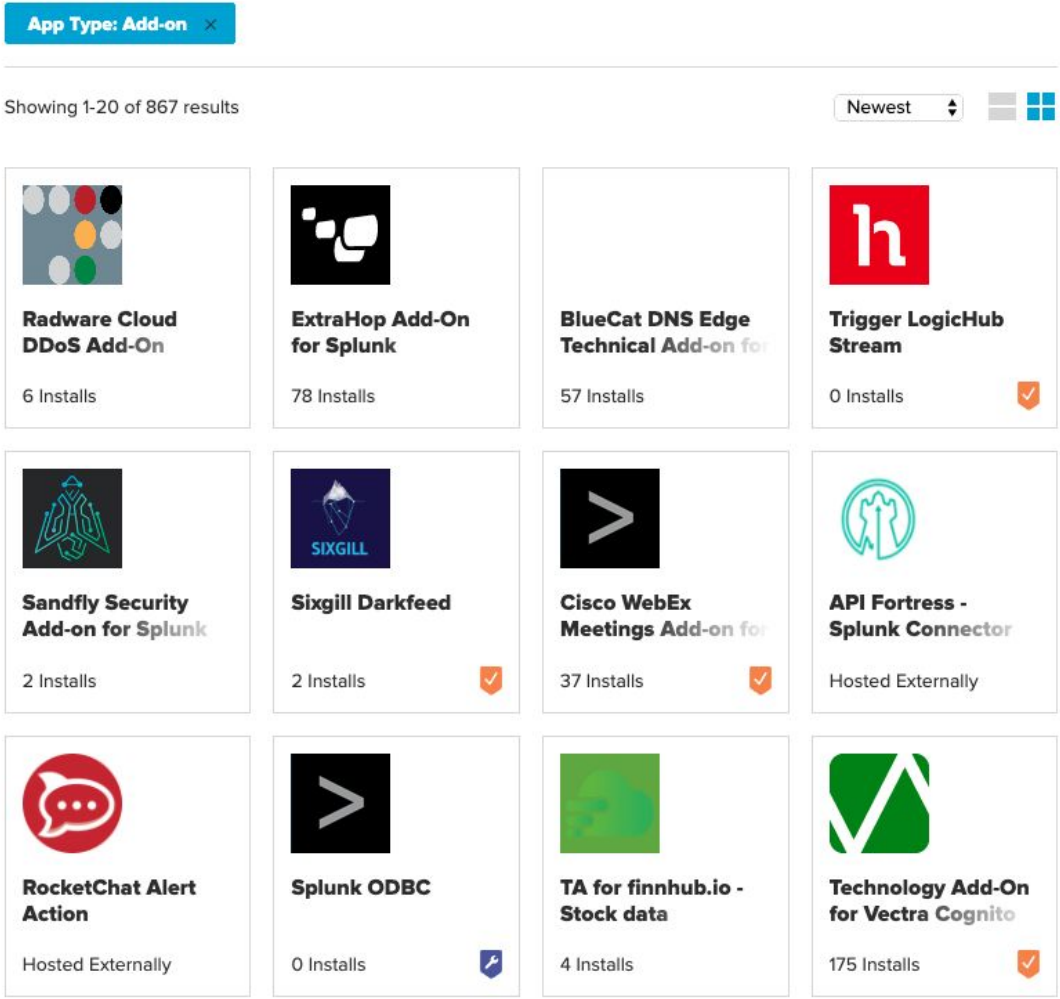
are applications that users can add to their Splunk base product. Apps have custom searches and features, and their own interface.

(splunkbase.splunk.com)



Splunk Add-ons

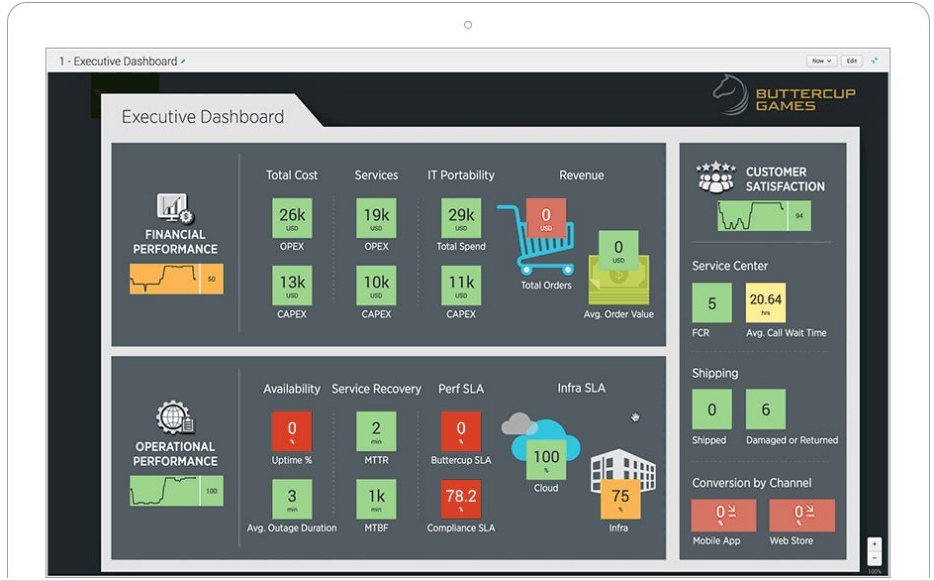
are smaller components that provide additional functionality, without their own interface.



(splunkbase.splunk.com)

Splunk Suites

are collections of apps with a single focus, such as an industry or technology.



Splunk IT Service Intelligence (ITSI)

Simplify operations, prioritize problem resolution and align IT with the business using a monitoring and analytics solution tailored for today's environments.

Get Predictive Analytics ›

VictorOps

Empower your on-call teams to find and fix problems faster with automated and insightful incident response routing, collaboration and reviews.

Make On-Call Suck Less ›

Splunk Insights for AWS Cloud Monitoring

Don't lose sight or control of your data. Enjoy end-to-end security, operational and cost-management insights for your AWS workloads.

See Through the Cloud ›

Splunk App for Infrastructure

Unify and correlate logs and metrics on one solution. Get free comprehensive infrastructure monitoring, alerting and investigation with your Splunk Enterprise license.

Install to Insights in Minutes ›

(Source)

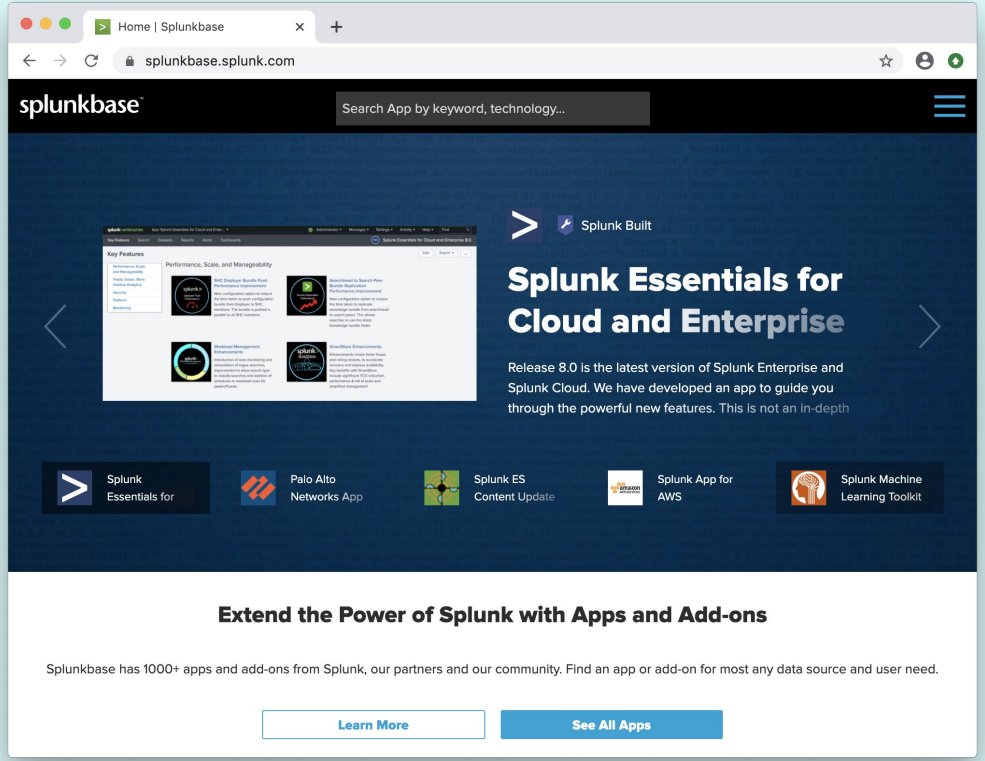
Splunk Add-ons and Apps

We will explore various Splunk apps and add-ons with the following scenario:

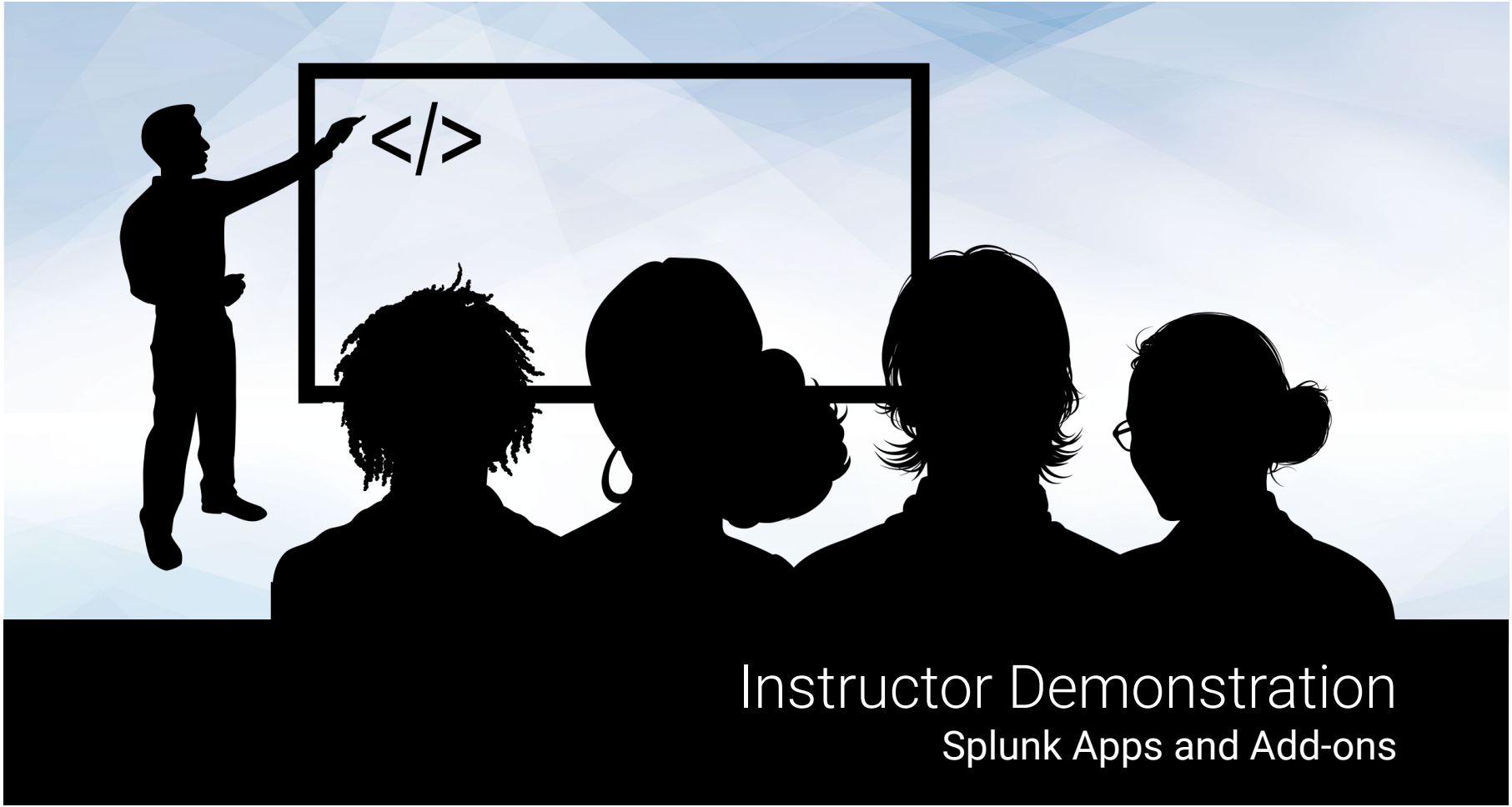
Your manager has notified you that your organization has purchased a web application filter by the vendor F5.

V

Your manager would like you to find the appropriate Splunk app to assist with monitoring this product.

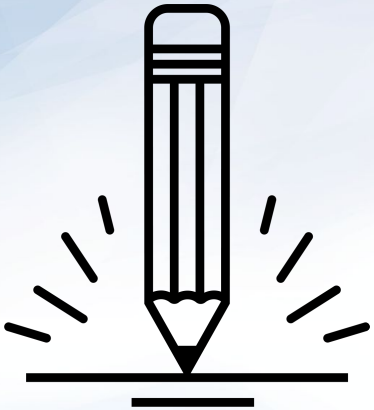


(splunkbase.splunk.com)



Instructor Demonstration

Splunk Apps and Add-ons



Activity: Splunk Features

In this activity, you will analyze add-ons and apps to determine which will work with your security products.

Suggested Time:
7 Minutes

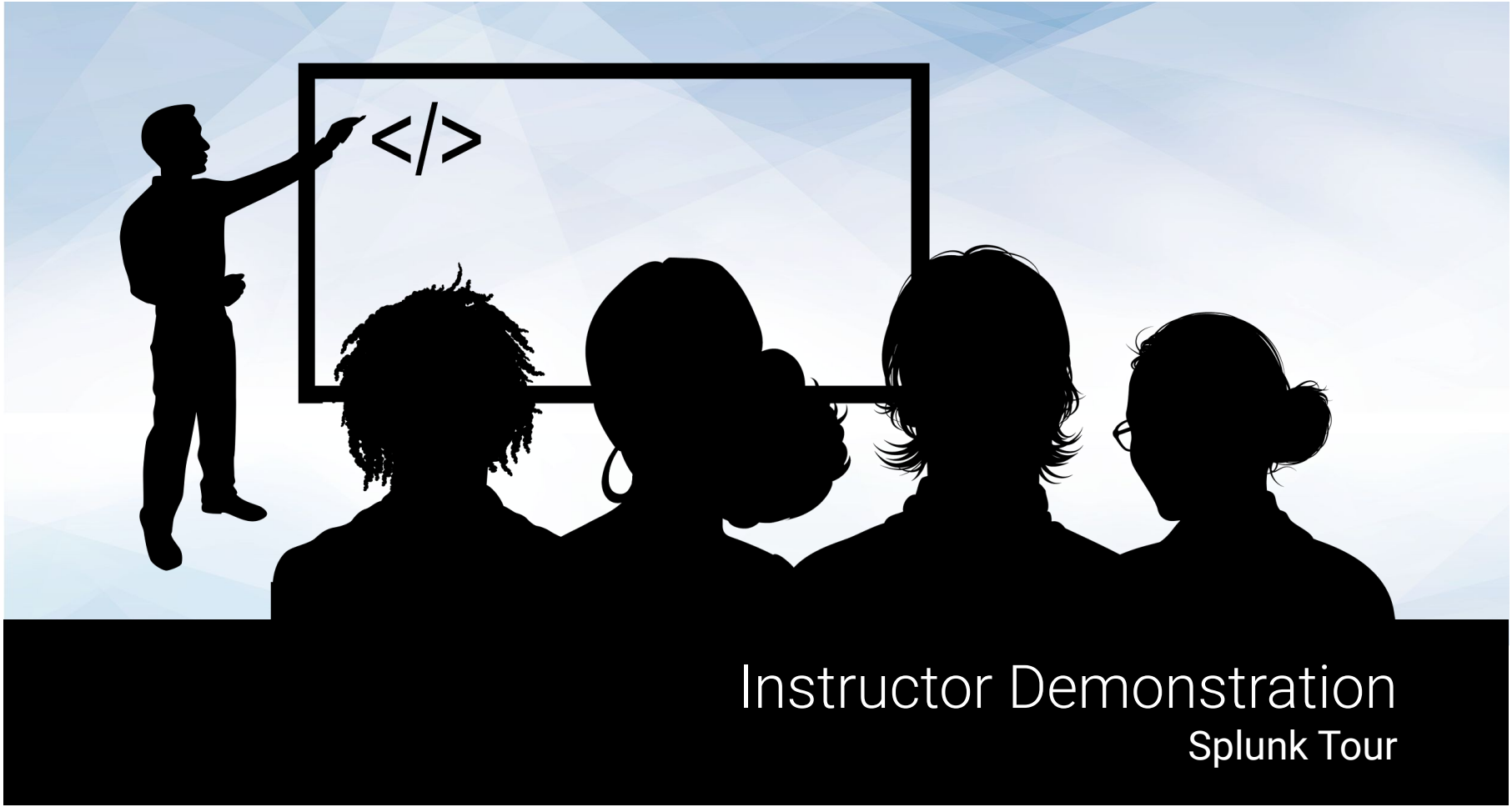
Time’s Up! Let’s Review.

Tour of Splunk

Splunk Setup

The best way to learn how to use the Splunk product is to dive right in and start using the application.

In the following guided tour, we'll explore the Splunk setup, interface, and features.



Instructor Demonstration

Splunk Tour

Adding Data

To use the various search capabilities of Splunk, we need to first add the data to search against.

01 Indexer

- When Splunk receives incoming data, it transforms the incoming data into **events**.
- Splunk adds these events into repositories called **indexes**.
- **Indexers** are used to add events to indexes and search through the data.

02 Search head

- The **search head** is Splunk's GUI that we use to conduct searches.
- It manages search requests to the indexer and provides the search results back to the user.

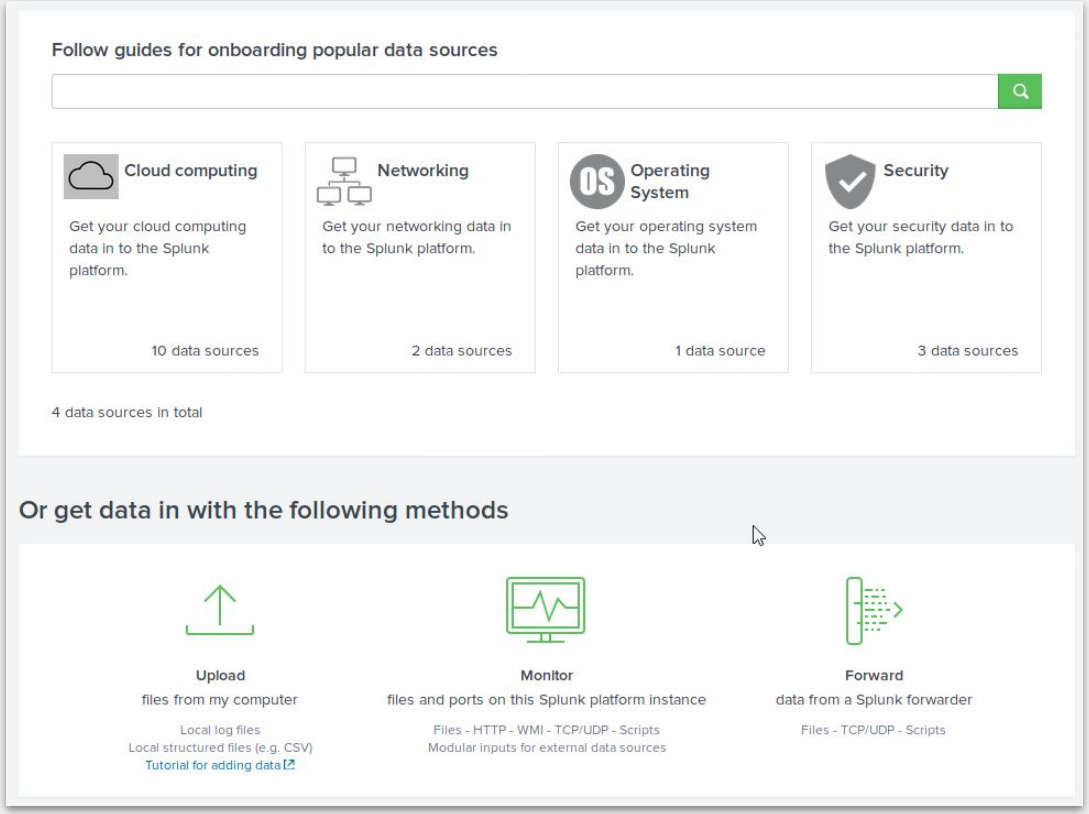
Searching in Splunk

In order to add data to Splunk on the **Add Data** page, we use one of the following paths:

From the Welcome page, go to **Explore Splunk Enterprise** and select **Add Data**.

V

From within the Search and Reporting app, select **Settings** > **Add Data**.



Adding Data

01 Add Data by Data Source

We can upload data based on the source.

- For example, a Splunk user may want to add Palo Alto Firewall logs into Splunk.
- The Palo Alto option under Networking is an example of a data type.
- Based on the option selected, an add-on may be provided or settings may be configured.

02 Adding Data by Method

Or we can use one of these three methods to add data:

- Monitor
- Forward
- Upload

Add Data Methods

Adding data by method allows you to add data by one of the following methods:

01

Monitor: Monitor logs from a system, device, or application that Splunk has direct access to.

This is commonly used by businesses to monitor their production environment.

02

Forward: Install a program called a forwarder on the system from which logs are collected.

Forwarders forward logs from a device into the Splunk system.

03

Upload: Manually upload logs directly into your Splunk repository.

We will primarily focus on this process during class.

Uploading Data into Splunk

In this demonstration, we will use the following scenario to upload data into Splunk:

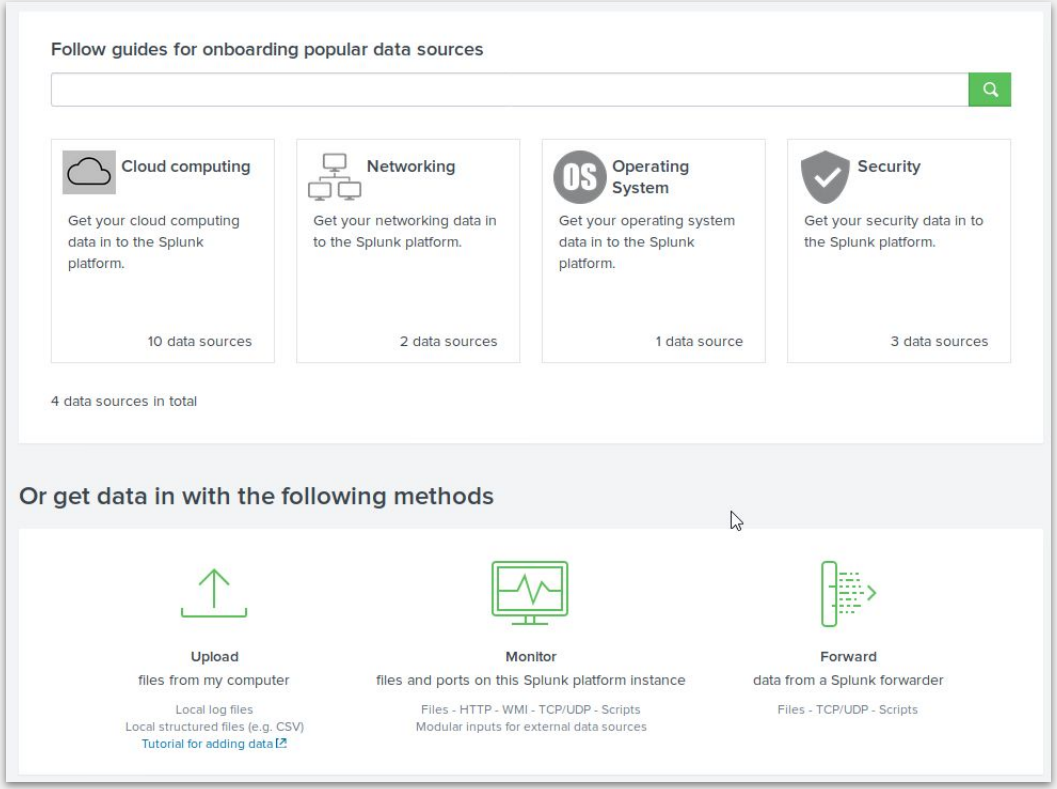
Our manager reported suspicious login activity on our Linux servers.

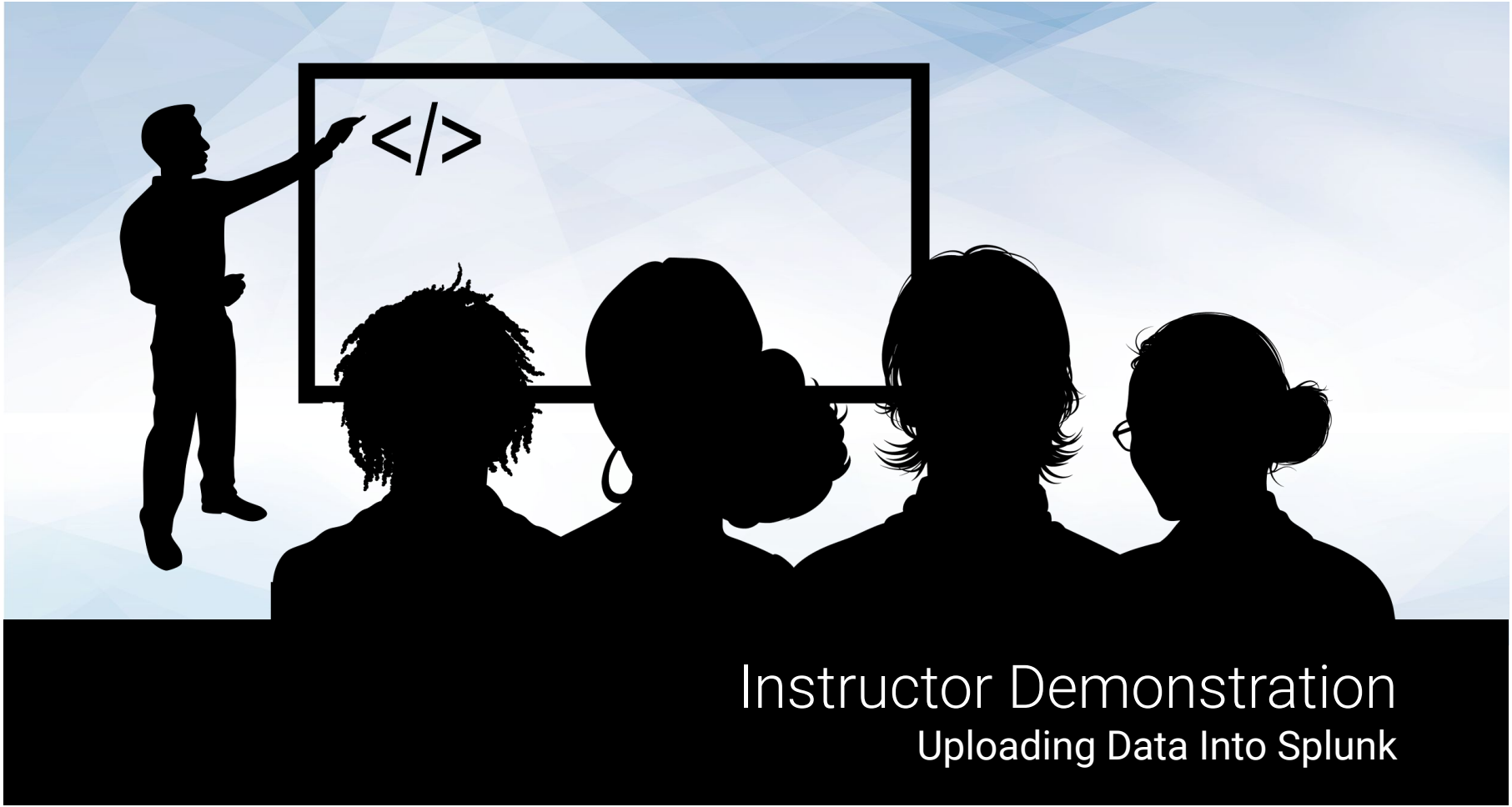
V

We've been provided the login activity from the servers.

V

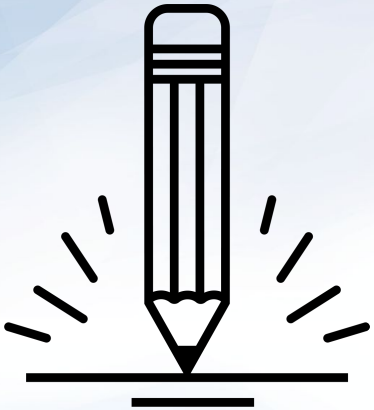
We must upload the activity data into Splunk so it can be analyzed.





Instructor Demonstration

Uploading Data Into Splunk



Activity: Uploading Data Into Splunk

In this activity, you will upload several log files that will be used later to analyze security events.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

Searching with Splunk

Searching in Splunk allows users to query uploaded and monitored data.

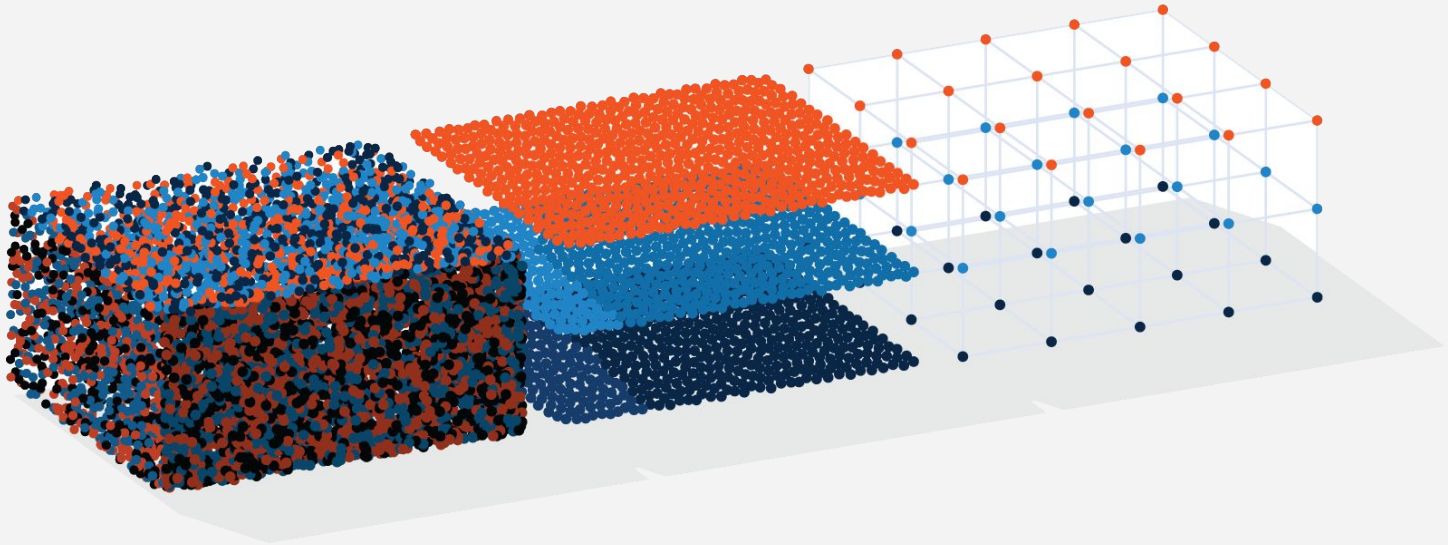
Splunk queries can be customized to look only for specific data or to manipulate how the data is displayed.

Searching in Splunk

We can use Splunk queries to find specific, helpful information about a security event.

For example

- Determine the **primary IP** that is being attacked during a DDOS attack.
- Determine the **user ID** being used in a brute force attack.



Searching Splunk

Splunk searching is almost always a time-based search.

Splunk searching is almost always a time-based search. When we search for events, we must designate a time range or real-time period.

01

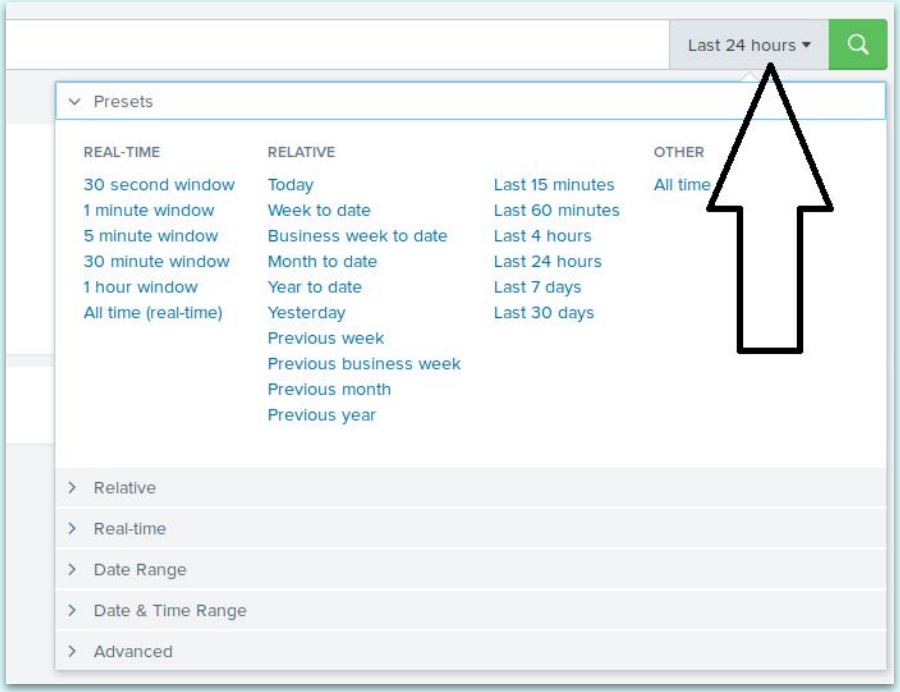
Real-time search
Returns a window of real-time data as it is happening and continues to update as the events occur.

02

Relative search
Returns data by date, date range, time, or time range. Results won't change, even if more events occur.

03

All time search
Returns all available data based on the search.



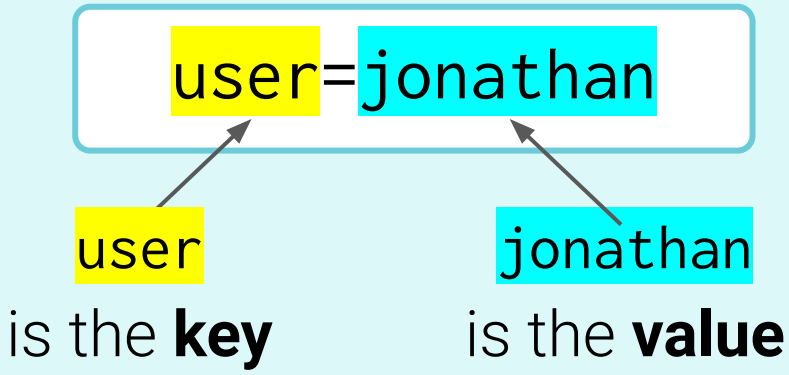
Splunk queries are designed using a coding language called **Splunk processing language (SPL).**

Key-Value Pairs

Key-value pairs are the most common method used to search for data.

For example:

If you want to find a user named **`jonathan`** in your search results, you would design the following search:



`user=jonathan`

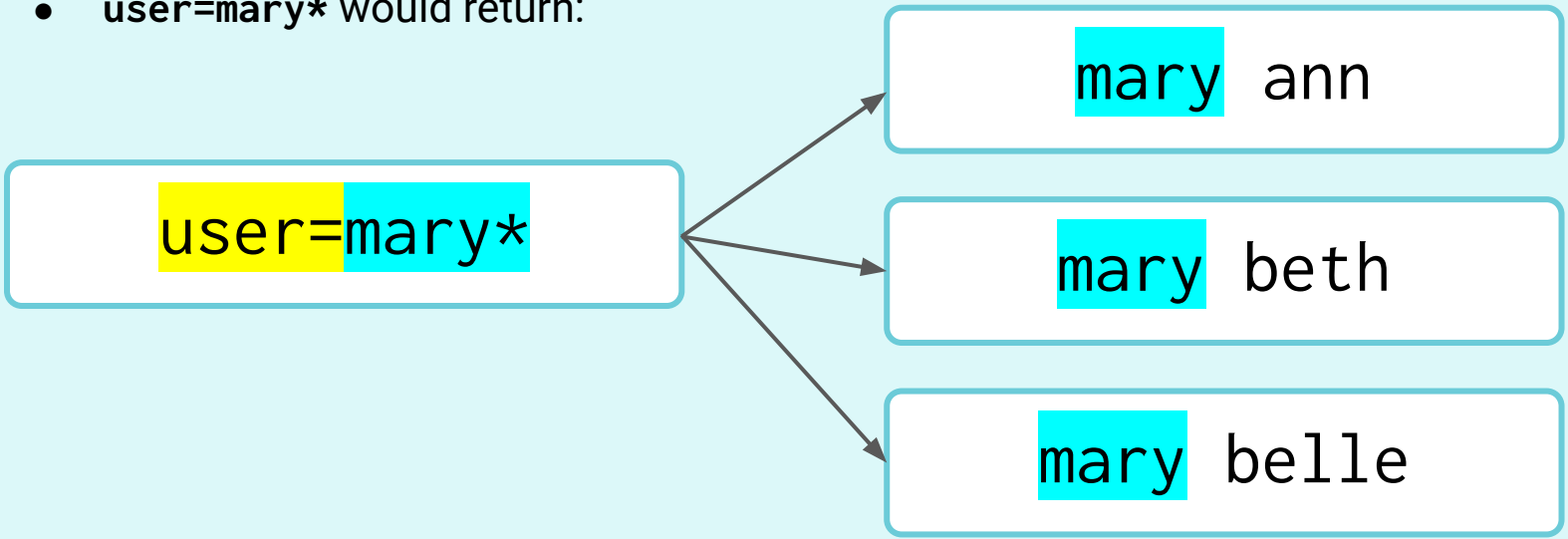
is the **key-value pair**

Wildcards

Similar to other programming languages, SPL uses **wildcards**. When used with the wildcard symbol (*) the search results return the search term followed by any character or string in place of the wildcard symbol.

For example:

- `user=mary*` would return:



Boolean Expressions

SPL uses the boolean expressions **AND**, **OR**, and **NOT** to assist in searching for specific data.

Expression	Use	Example
AND	Combines two key-value searches.	`user=jonathan AND activity=login`
OR	Looks for multiple instances of a key-value pair.	`user=jonathan OR user=beth`
NOT	Excludes certain values from search results.	`user=jonathan NOT activity=logout`

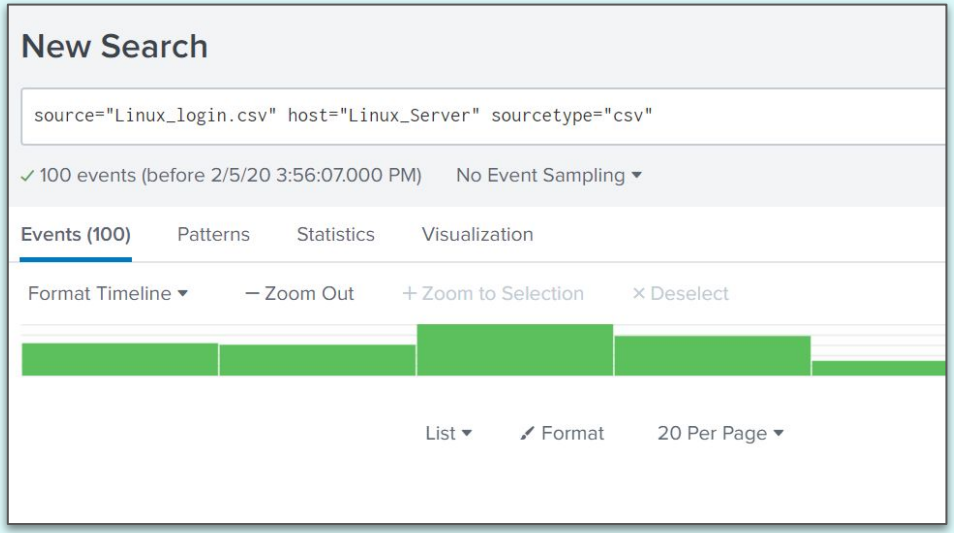
Search Demonstration

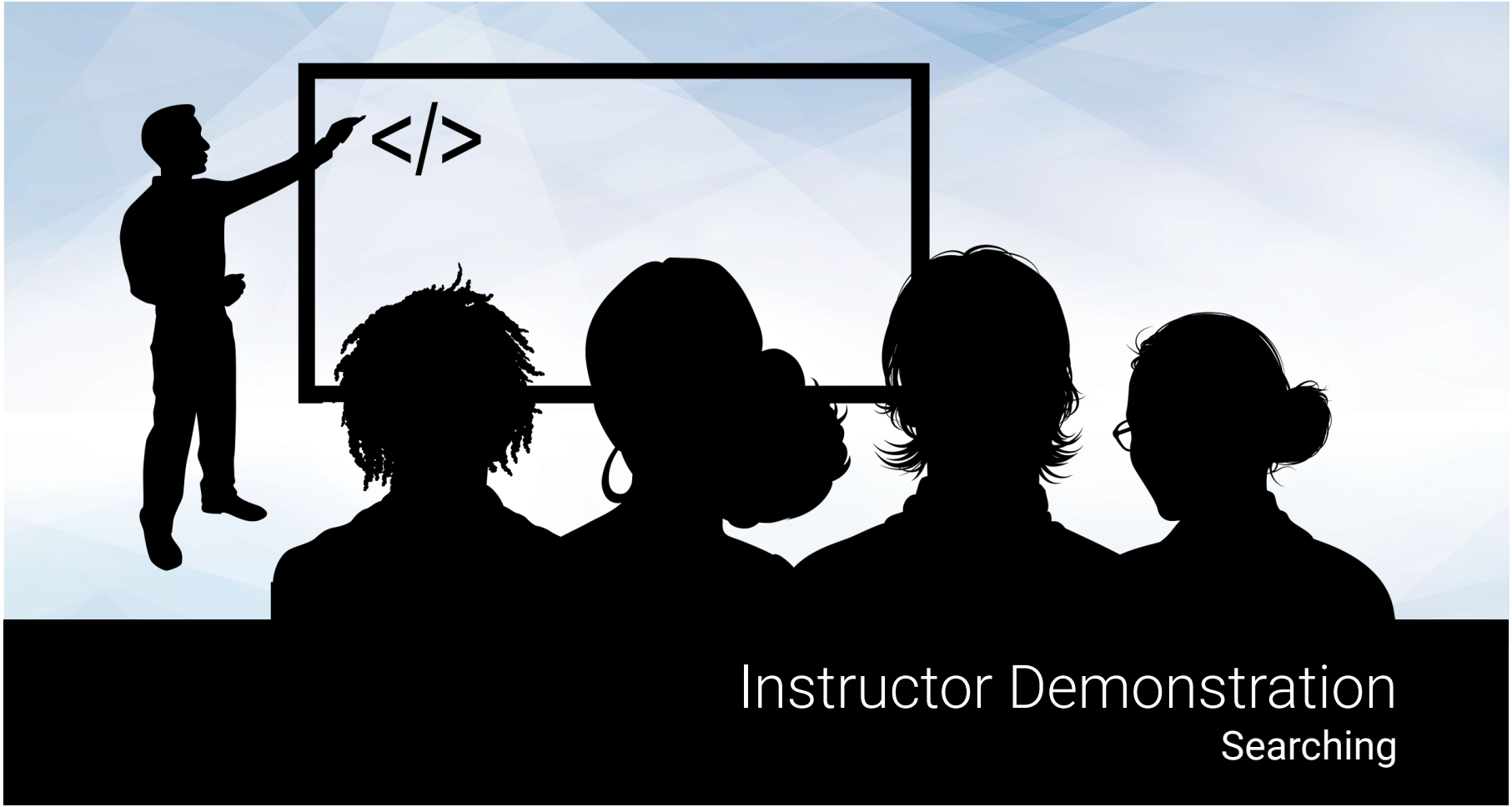
In the next demonstration, we will use the following scenario:

Your manager reported some suspicious login activity on your Linux servers.

They would like you to create a query to look at these login activities, specifically for logins coming from the source IP of `10.11.36.17`.

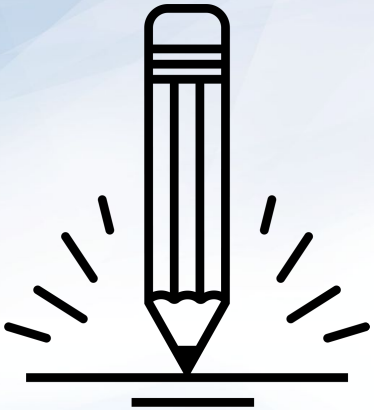
They believe this IP is from a machine infected with malware.





Instructor Demonstration

Searching



Activity: SPL Search

In this activity, you must design SPL searches to run against the vulnerability scanning log file, **`nessus.txt`**.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

So far, we've been manually typing out the keys and values for our SPL queries.

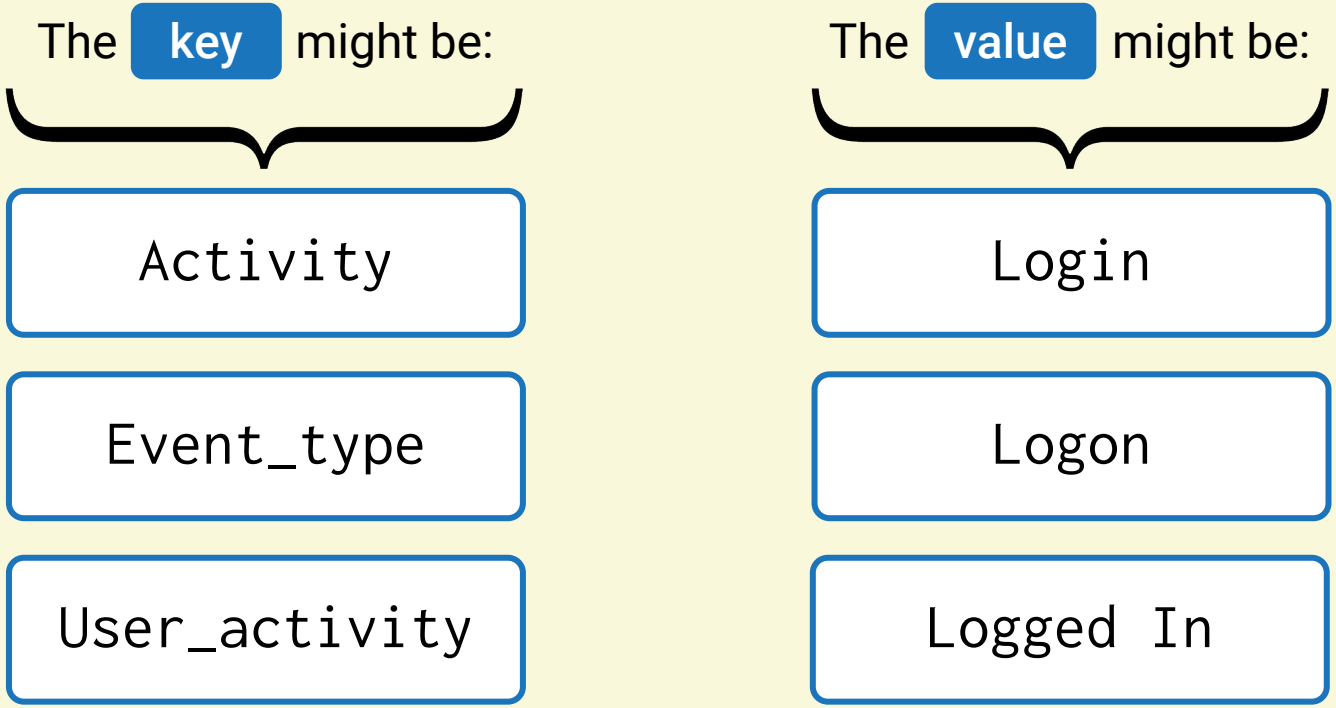
The more complex the queries become, the more time-consuming this task will be.

(Source)

Keys and values may vary depending on server and application.

Complexities of SPL Queries

For example, if we need to find users that logged into a machine:



Search Fields

When files are uploaded and parsed, the data is separated into fields, as shown on the left side of Splunk's search page.

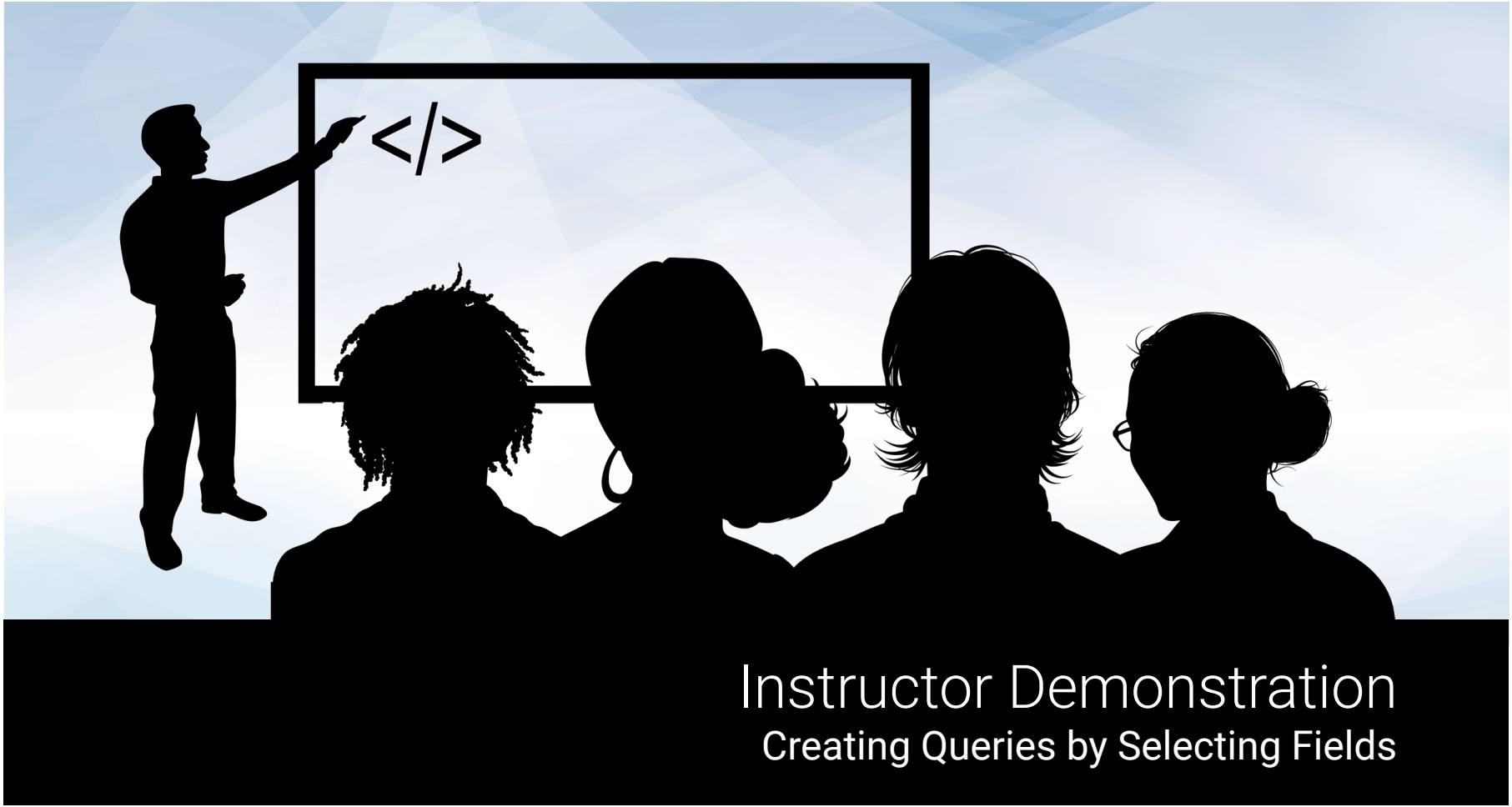
Fields are divided into:

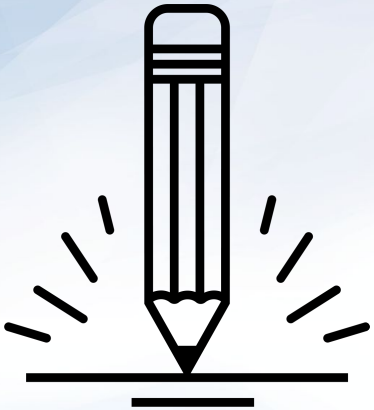
Selected fields

that appear in every log event.

Interesting fields

that appear in at least 20% of log events.


Instructor Demonstration
Creating Queries by Selecting Fields



Activity: Searching Fields with Splunk

In this activity, you will create complex SPL queries by selecting fields in your Splunk search.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

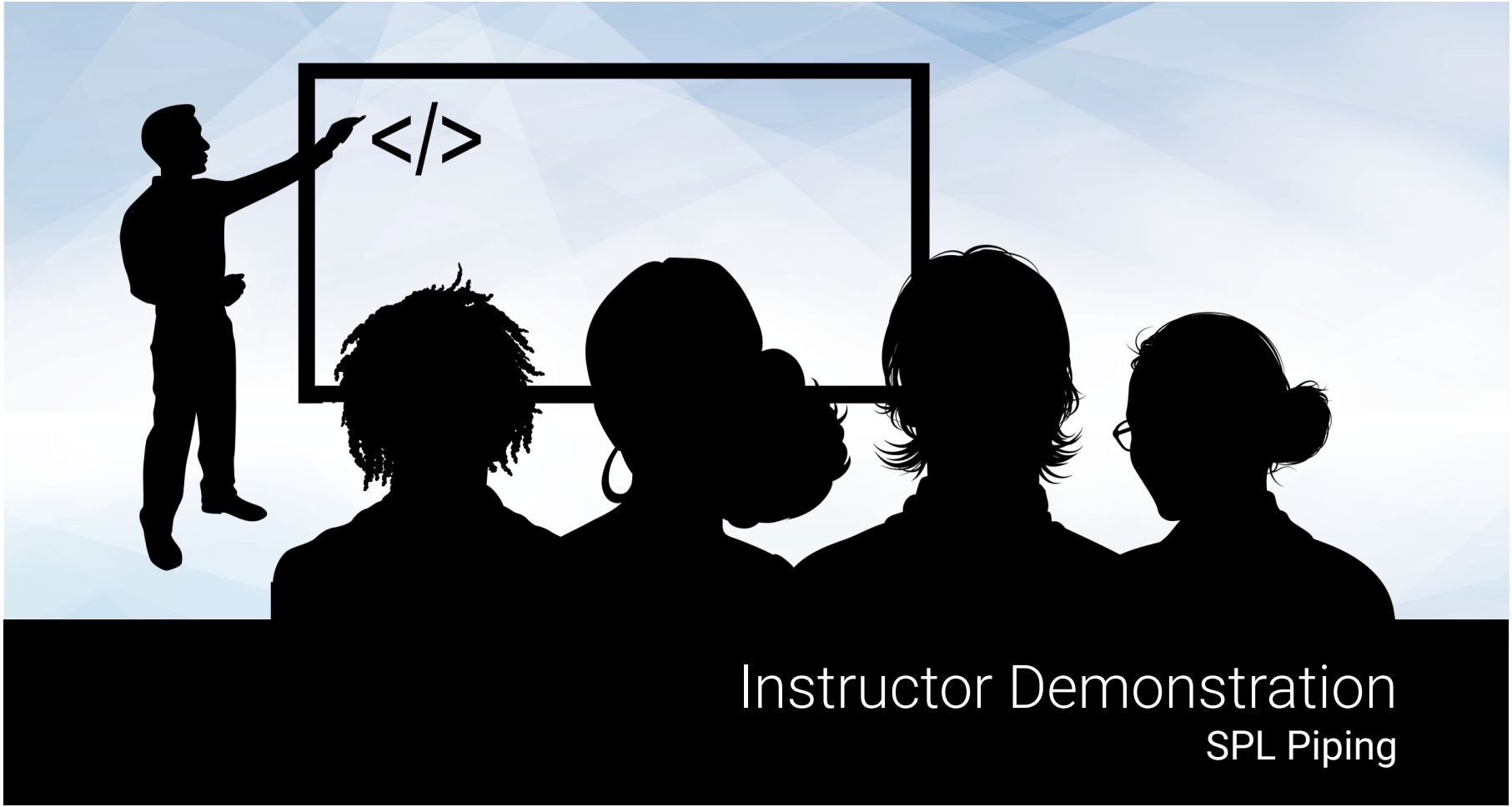
SPL Piping

We can add **piping** to our SPL queries to modify or adjust the display of the results, or to create custom reports.

```
source="Linux_login.csv" host="Linux_Server__" sourcetype="csv" | head 20 | sort src_ip
```

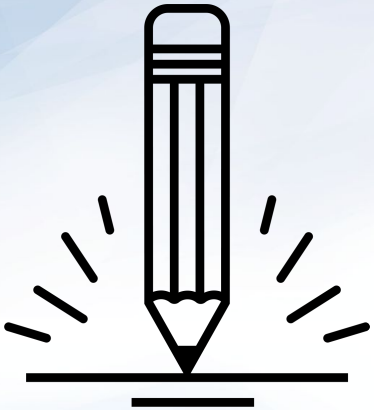
SPL piping uses the | symbol in the search queries.

Piping works in Splunk as it does in Linux. The data is modified from left to right as it flows through the pipeline.



Instructor Demonstration

SPL Piping



Activity: Advanced Searches with Piping

In this activity, you will run several advanced searches to find out if a specific user is being targeted by an attacker.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.


The End