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.

Write complex SPL queries to analyze specific security situations.


Recap

Recap

Before we introduce Splunk and its capabilities, let's review last class's concepts:

Organizations use **continuous monitoring** to monitor risks to the confidentiality, integrity, and availability of their technical assets.

Organizations use **logs** that contain **log entries** to monitor against these risks.

Organizations **aggregate**, **parse**, and **normalize** multiple logs so they can be analyzed together.

Organizations correlate these logs with **correlation rules** to alert when a security event or suspicious activity is detected.

SIEM software is a security tool that can assist with all of the above processes.

We also learned about the many SIEM vendors available, each with different features, strengths, and weaknesses.

In The Next Two Modules…

We will:

- Focus on one of the most popular SIEM vendors, Splunk.
- Learn about Splunk and its features.
- Complete hands-on activities within Splunk that mirror those security professionals perform every day.

Splunk Capabilities

Splunk is the vendor name of a **big data software** solution, and the SIEM tool is just one of the thousands of features Splunk provides.

Splunk Capabilities

Splunk is…

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

Splunk can…

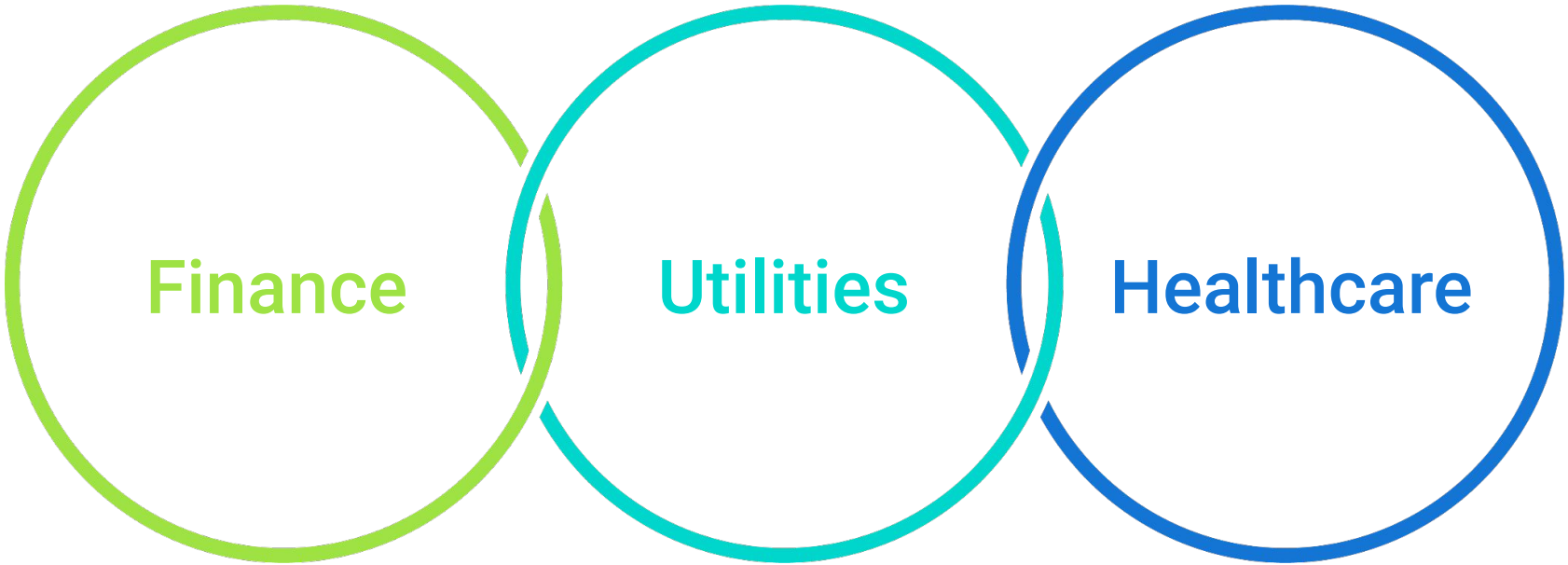
Capture large amounts of incoming data, which can be used to create visualizations, reports, and alerts.

Splunk has…

A base product that is designed to conduct basic tasks such as searching and reporting.

Splunk Capabilities

This week, we're focusing on Splunk's benefits to the InfoSec industry, but Splunk is useful for a variety of industries, such as:



Finance

Financial organizations can use Splunk to analyze mortgage rates and determine future rate changes.

Utilities

Gas companies can use Splunk to monitor customer use levels.

Healthcare

Medical researchers can use Splunk to create reports and metrics for analyzing the success of medical trials.

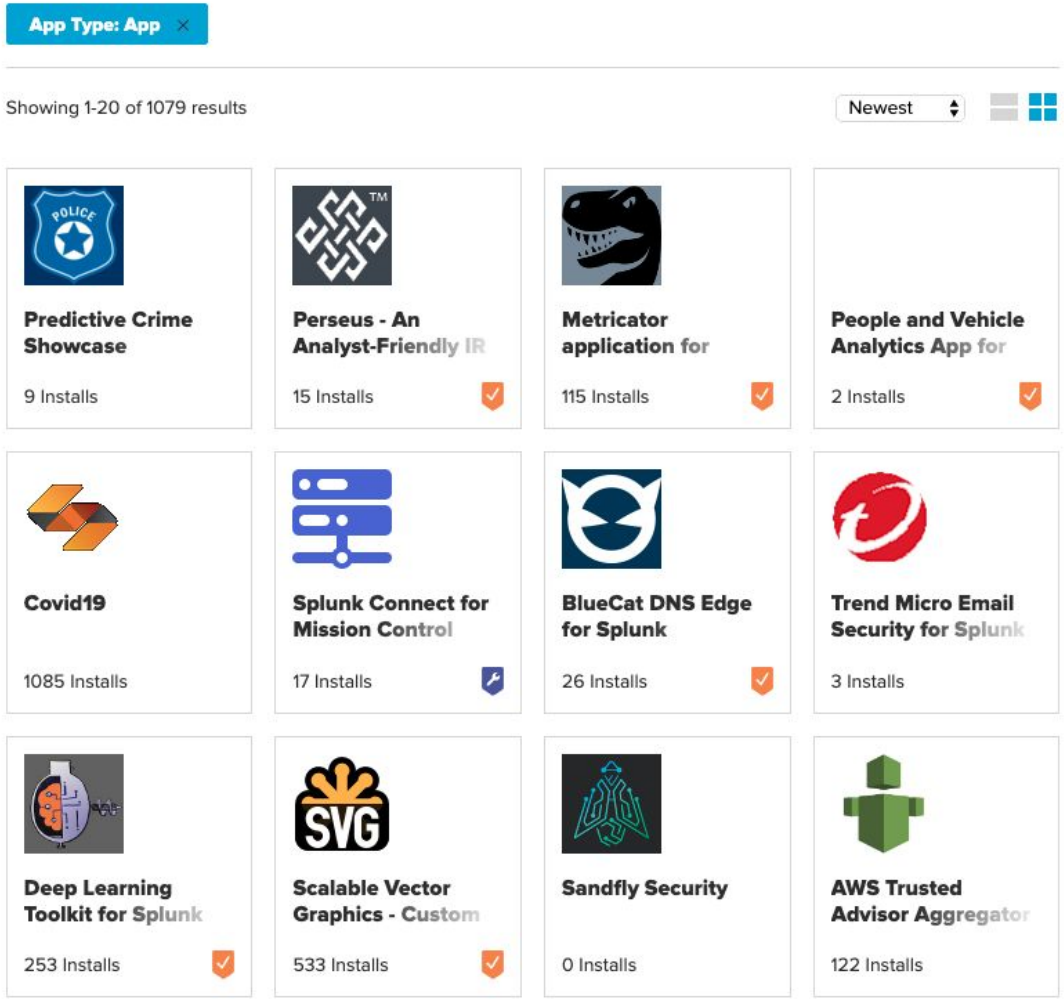
Apps, Add-Ons, and Suites

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

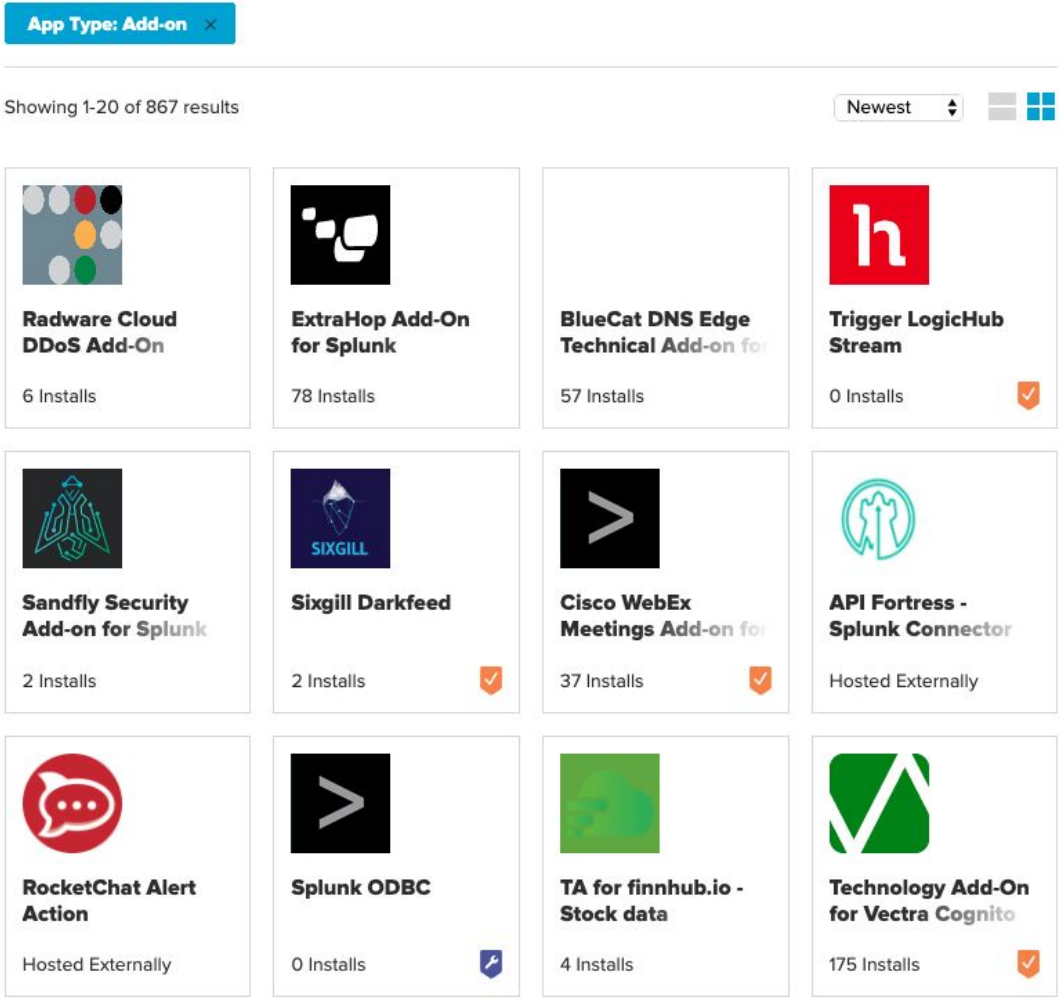
Applications that users can add to their Splunk base product. Apps have custom searches and features and their own interfaces.



(splunkbase.splunk.com)

Splunk Add-ons

Smaller components that provide additional functionality without their own interfaces.



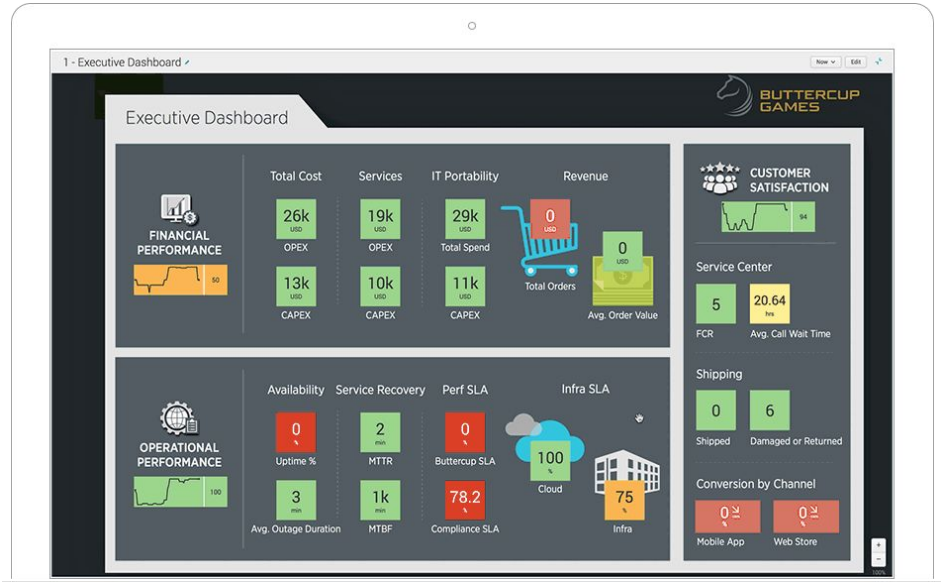
(splunkbase.splunk.com)

Splunk Suites

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

We will not review Splunk suites in this class.

(Source)



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 ›

Apps, Add-Ons, and Suites

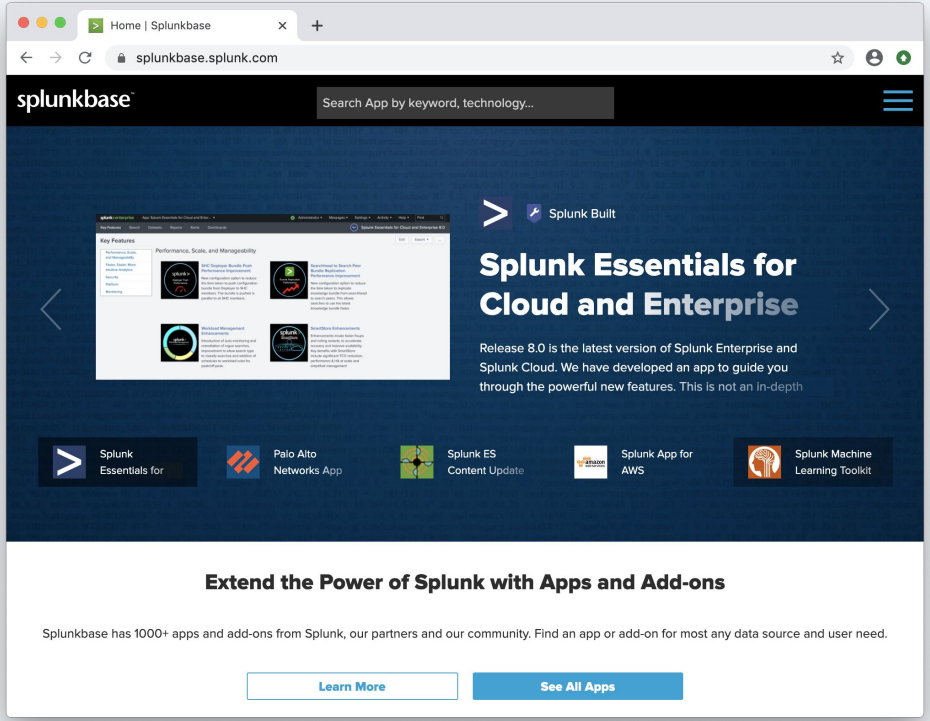
Splunk has so many of these apps and add-ons that they are broken up by type:

Technology	Vendor	Industry
There are apps and add-ons specific to cloud servers.	There are apps and add-ons specific to the security vendor Rapid7.	There are apps and add-ons specific to manufacturing organizations.

Splunk Add-ons and Apps

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

- Your manager has notified you that the organization has purchased a web application filter by the vendor F5.
- Your manager would like you to find the appropriate Splunk app to assist with monitoring this product.



(splunkbase.splunk.com)

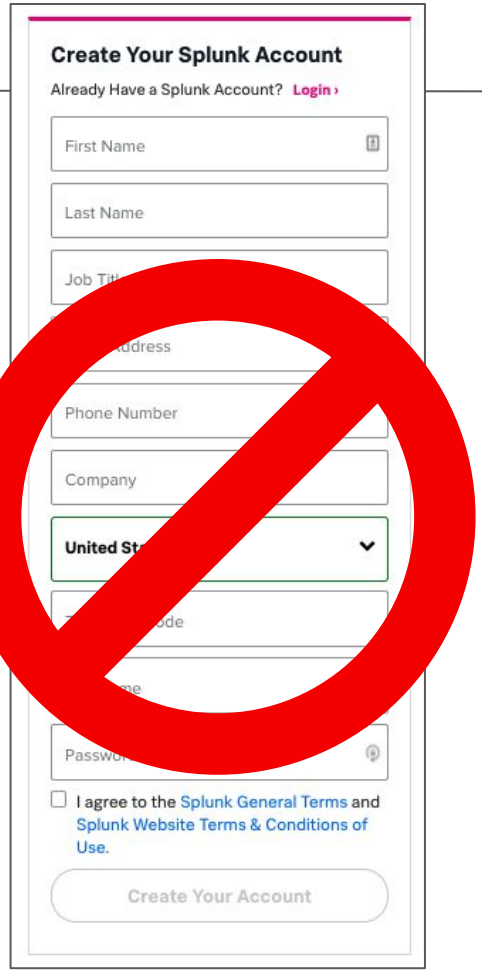
Instructor Demonstration

Splunk Apps and Add-ons

Splunk Account

Do not sign up for a Splunk account at this time.

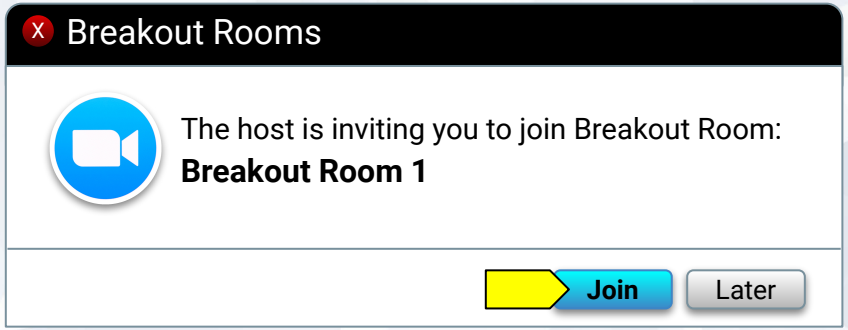
There is a 7-day trial window that we will start next week, so that we have access to Splunk for as long as the curriculum requires it.



Questions?

Activity: Splunk Features

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



Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

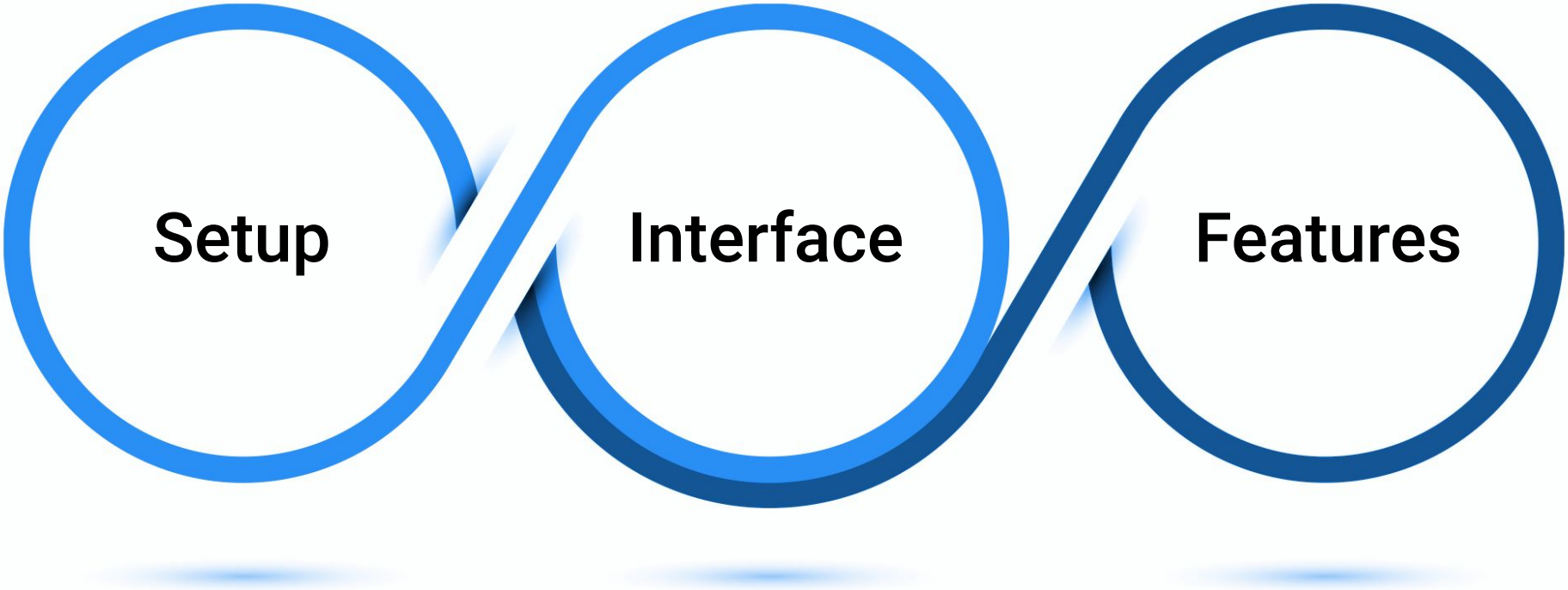
Tour of Splunk

Tour of Splunk

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

Tour of Splunk

In the following walkthrough, we'll explore the Splunk:



Instructor Demonstration

Splunk Tour

Questions?

Adding Data into Splunk

Before we add data, it is important to have a general understanding of Splunk's architecture and how it handles incoming data.

Splunk Architecture Basics

Splunk architecture contains two primary components:

01 The 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 The search head

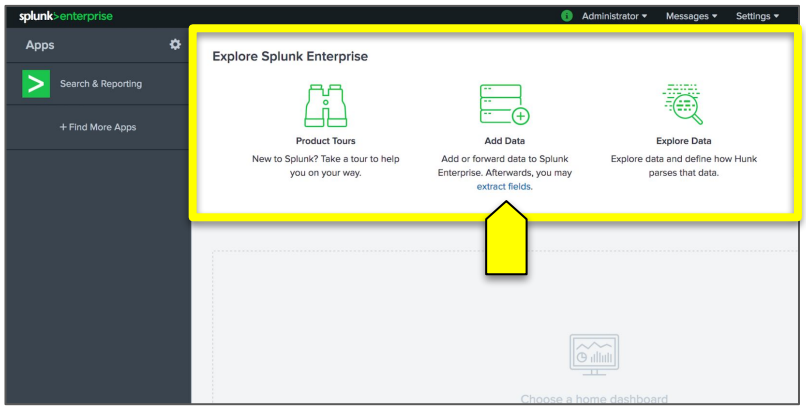
- The **search head** is Splunk's GUI that we use to conduct searches.
- It manages search requests to the indexer and provides the search results back to the user.

Splunk Data Addition Methods

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

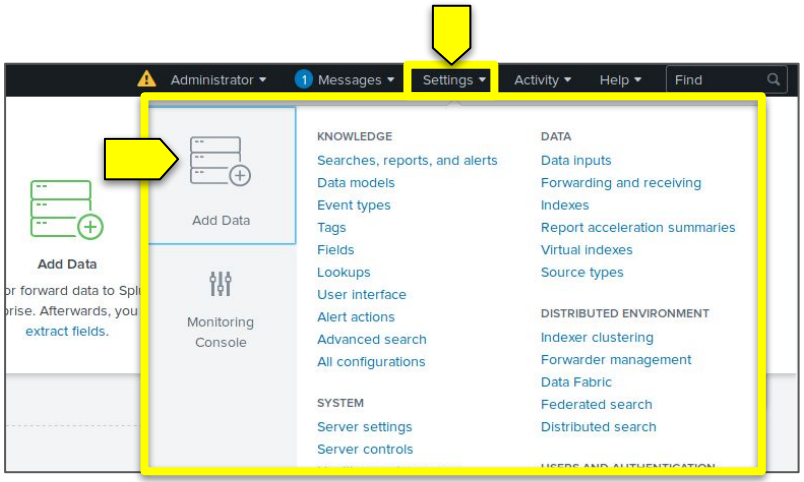
From the Welcome page

Go to **"Explore Splunk Enterprise"** and select **"Add Data."**



From the Search & Reporting app

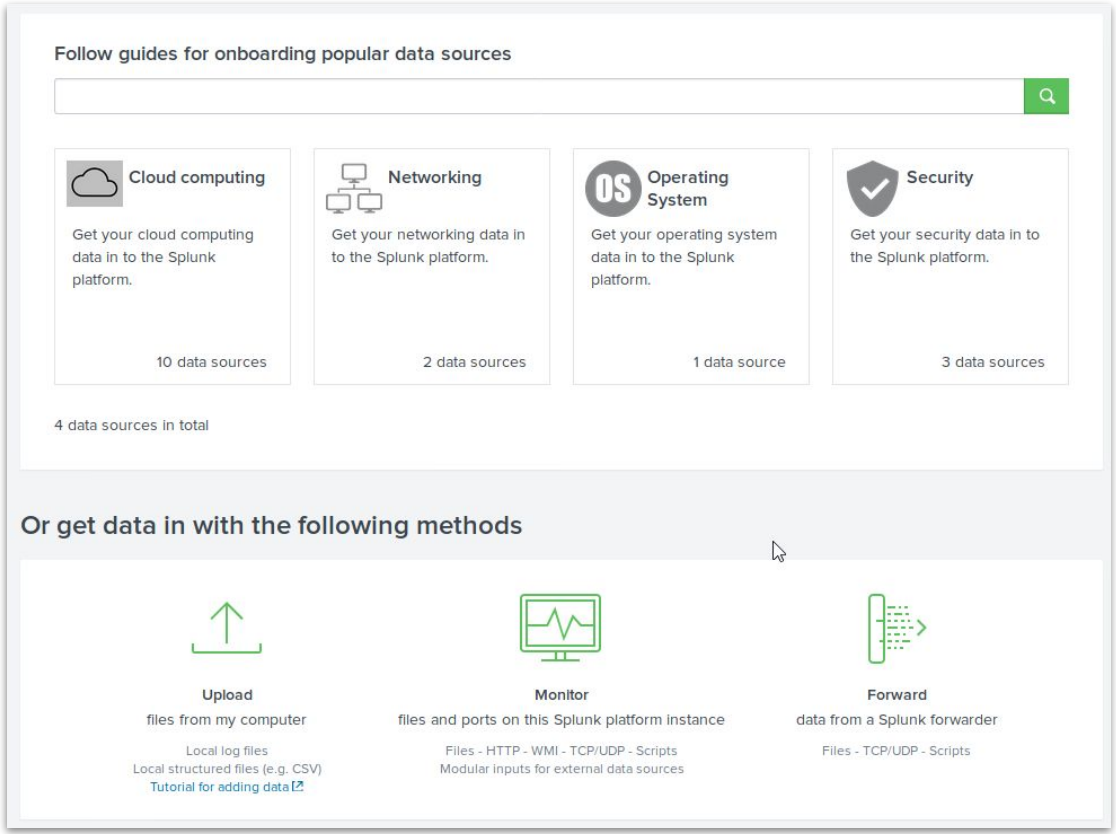
Select **"Settings"** and then **"Add Data."**



Splunk Data Addition Methods

The Add Data page prompts you to add data either by:

- Data source
- A specific method



Adding Data: Data Source

Adding data by data source allows us to upload various types of data.

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 configured.

Adding Data: Specific Method

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

Monitor

Splunk monitors logs from a system, device, or application that it has direct access to.

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

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.

Upload

Manually upload logs directly into your Splunk repository.

While monitoring and forwarding are important to understand conceptually, we will primarily use the upload process for the remainder of this class.

Uploading Data into Splunk

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

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

They have provided you with the login activity from your Linux servers.

You must upload them into Splunk so they can be analyzed.

Instructor Demonstration

Data Upload

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:

15 Minutes

Time’s Up! Let’s Review.

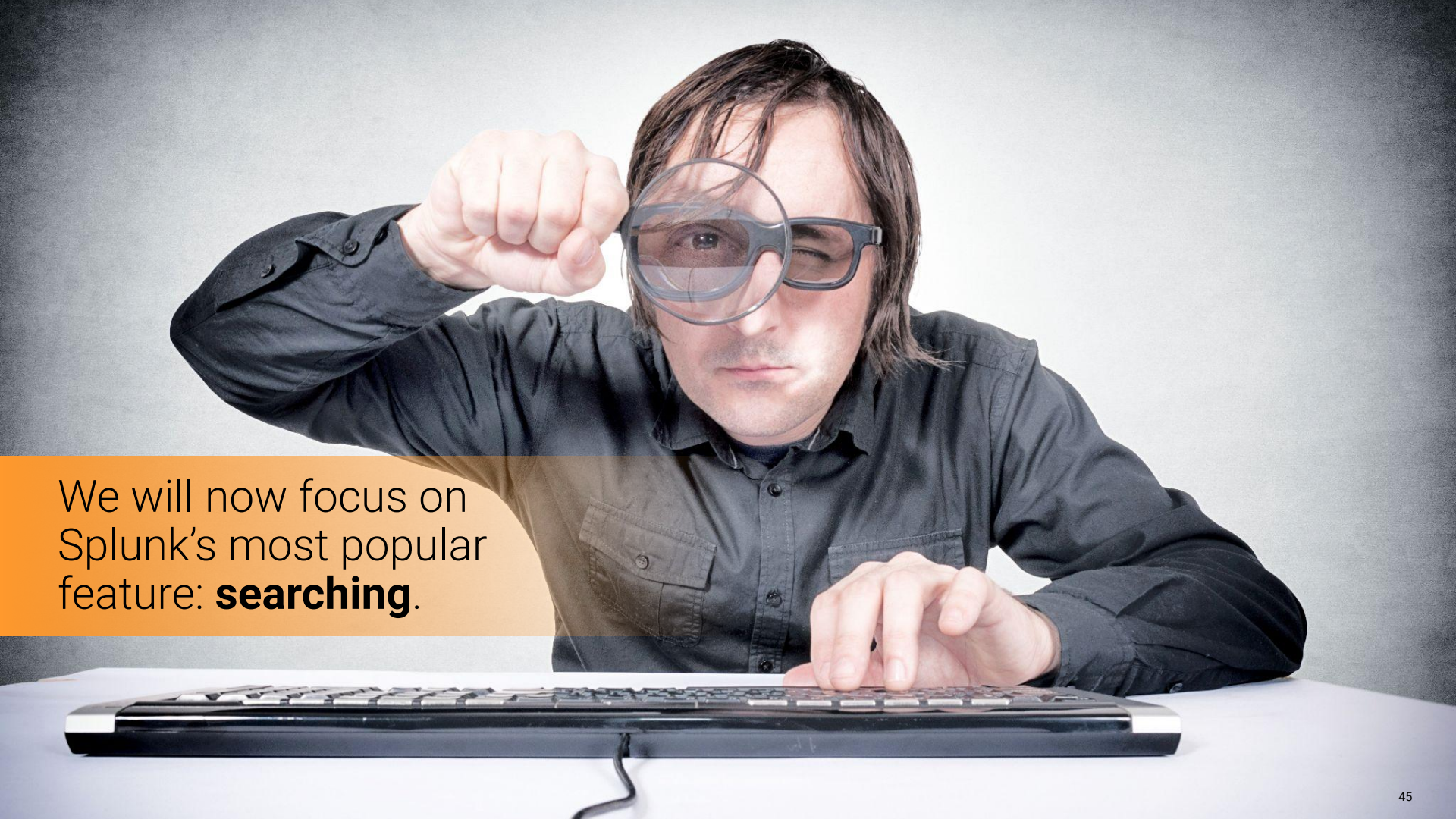
Questions?

Countdown timer

15:00

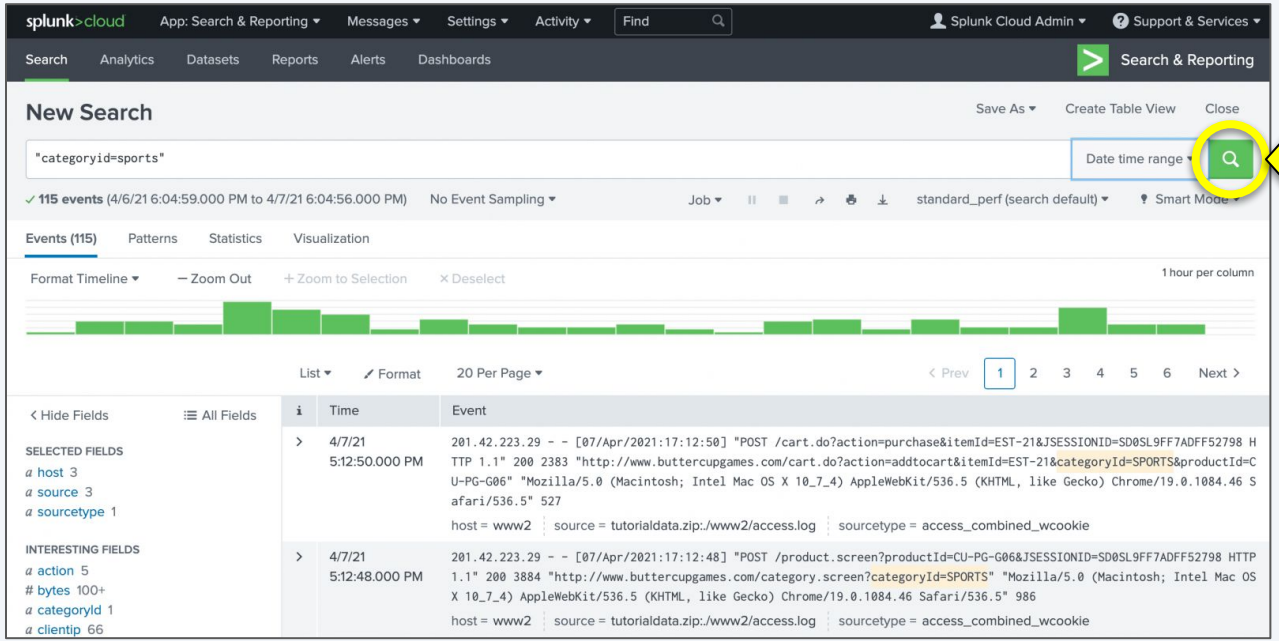
(with alarm)

Searching with Splunk


We will now focus on Splunk's most popular feature: **searching**.

Searching with Splunk

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



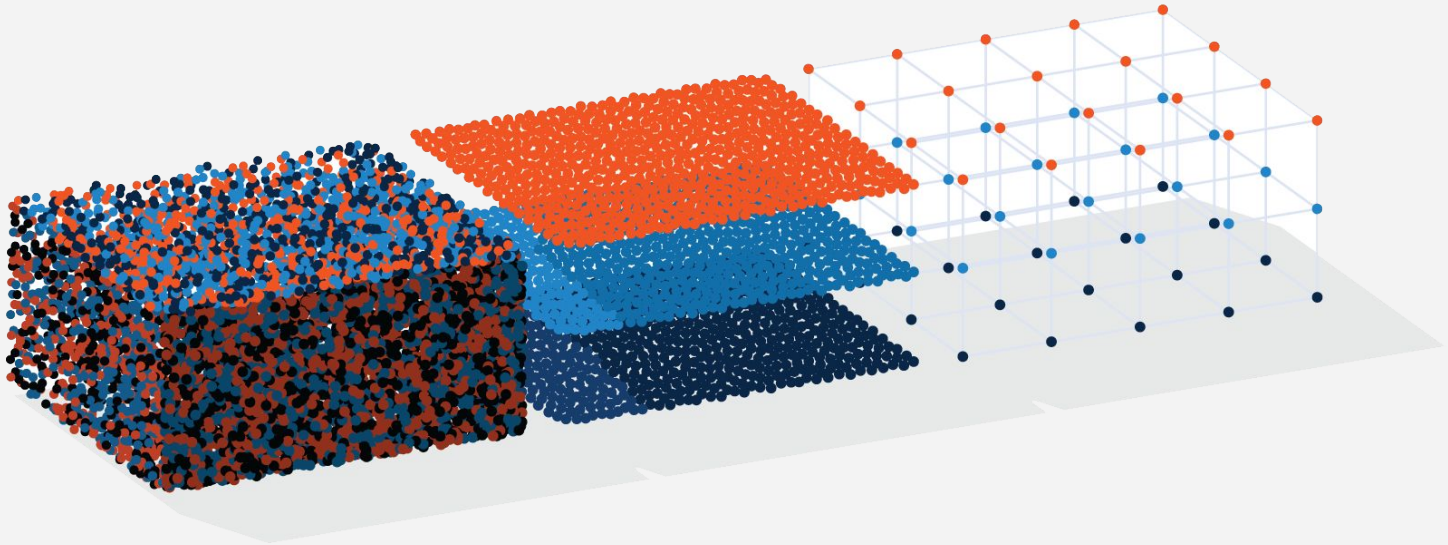
Splunk queries **can be customized** to look only for specific data or to manipulate how the data is displayed.

Searching in Splunk

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

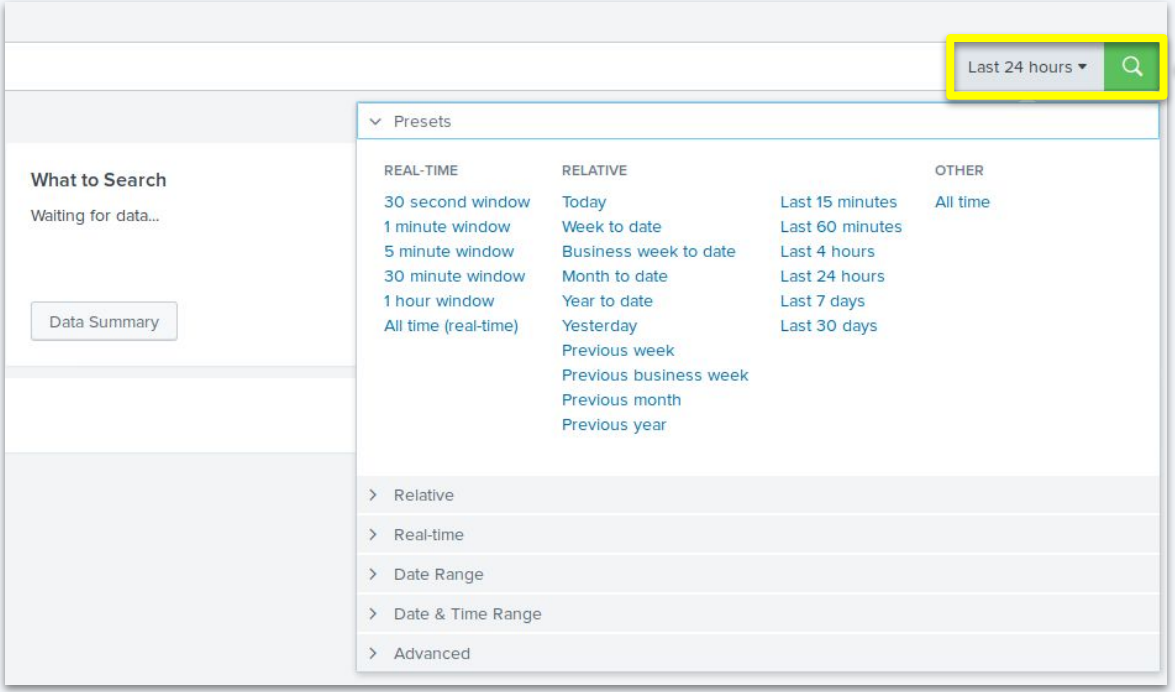
For example

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



Searching Splunk

Splunk searching is almost always a time-based search.



All events have associated timestamps.

To search for events, we must designate a time range or real-time period.

Searching Splunk

A user can select the following:

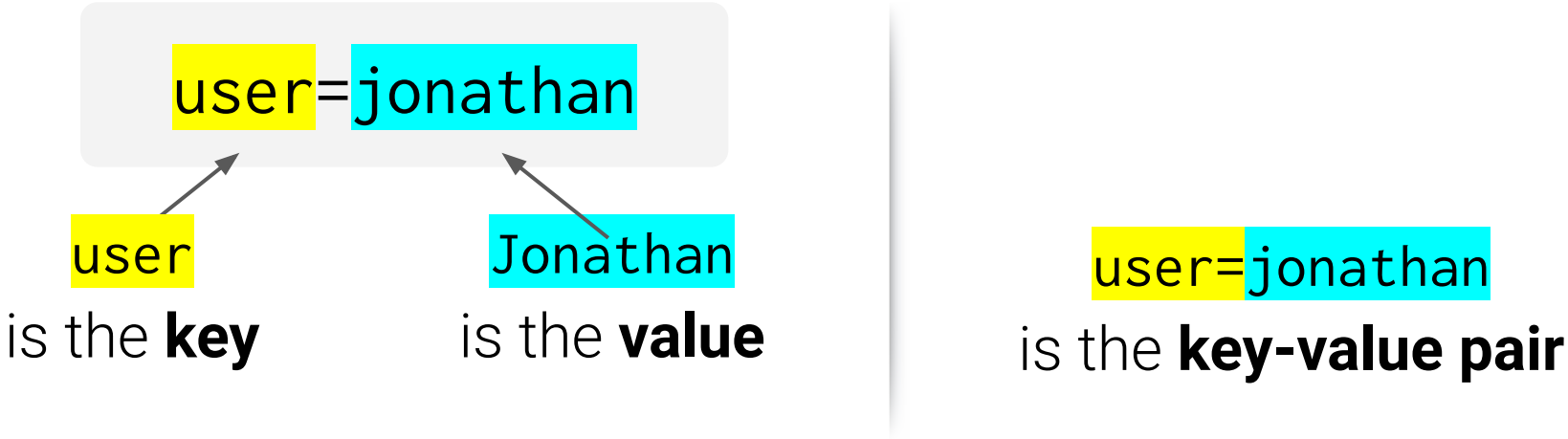
Real-time search	Relative search	All time
Returns a window of real-time data as it is happening and continues to update as the events occur.	Returns data by date, date range, time, or time range. Results will not change even if more events occur.	Returns all available data based on the search.

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

Key-Value Pairs

Key-value pairs, the most common method used to search for data, match keywords with specific information (values).

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

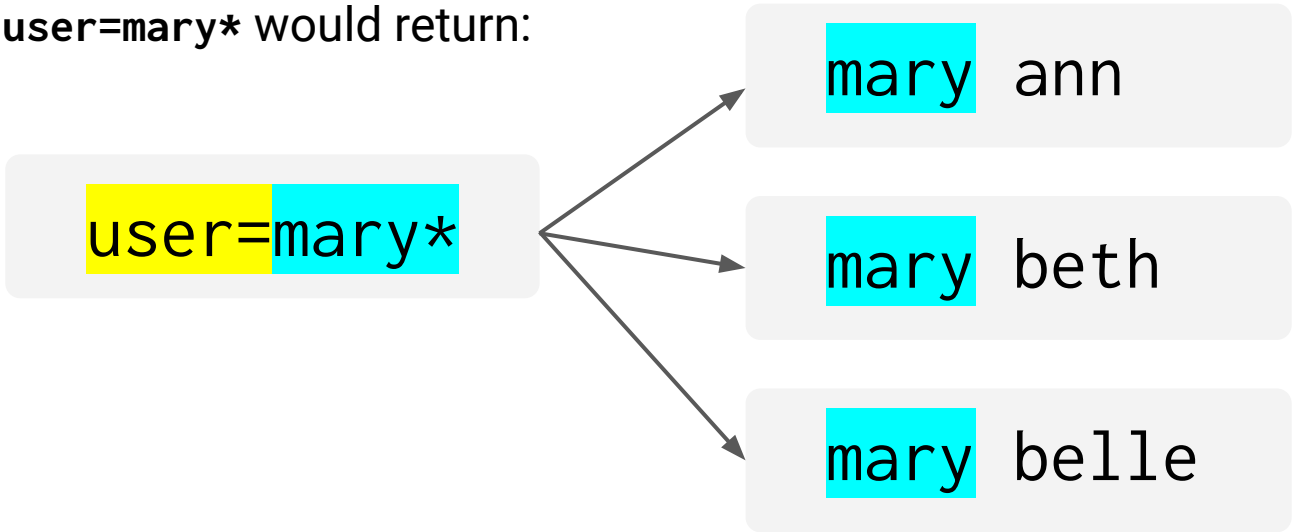


Wildcards

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:

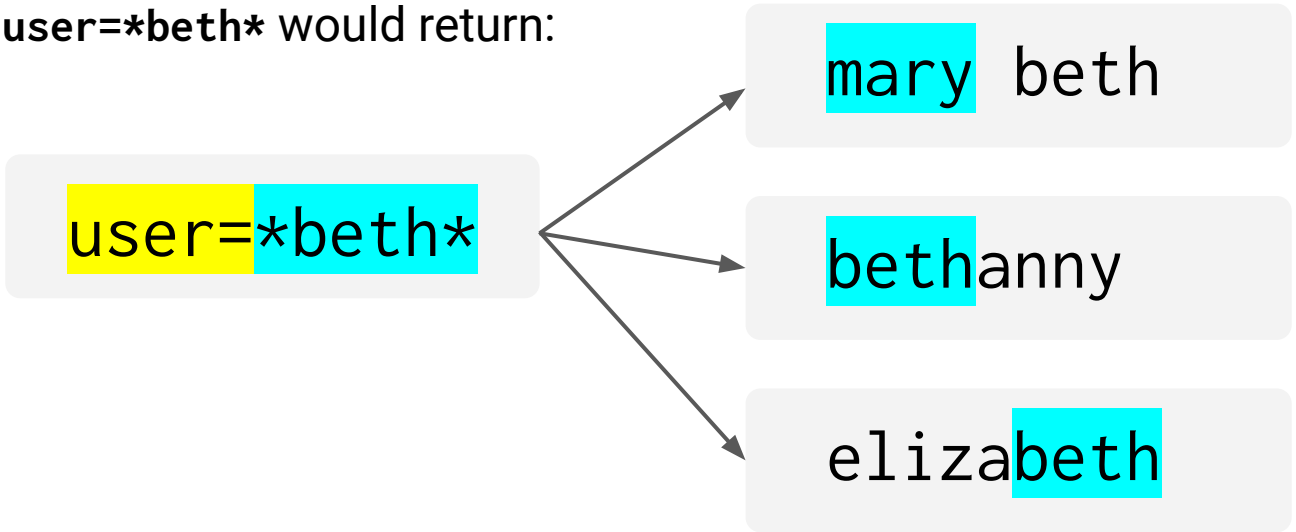


Wildcards

Wildcards can also be used to find a value surrounded by any character.

For example:

`user=*beth*` 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

We will use the following scenario:

- Your manager has reported some suspicious login activity on your Linux servers.
- She would like you to write a query to look at these login activities, specifically for logins coming from the source `IP 10.11.36.17`.
- She believes this IP is from a machine infected with malware.

Note: `src_ip` is the field name for the source IP.

Instructor Demonstration

Searching

Activity: SPL Search

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

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Searching Fields with Splunk

Searching Fields with Splunk

So far, we have manually typed out the keys and values for our SPL queries.

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

Sometimes we don't know the values or the format of the values that exist in the search results.

Each server and application creates their own key and value names.

Complexities of SPL Queries

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

The **key** might be:

- `Activity`
- `Event_type`
- `User_activity`

The **value** might be:

- `Login`
- `Logon`
- `Logged In`

Instructor Demonstration

Splunk Fields

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.

Default fields

Appear in every log event.

Interesting fields

Appear in at least 20% of the log events.

Value count

On the right of each field is a number indicating the count of different values for that field.

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:

15 Minutes

Time's Up! Let's Review.

Questions?

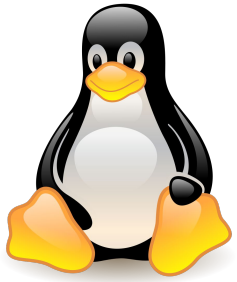
Advanced Searches with Piping

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 whether a specific user is being targeted by an attacker.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?


The End