

## Introduction to Splunk

### Summary

This course is for new Splunk users who want to learn how to search, analyze, and visualize data using Splunk's Search Processing Language (SPL).

This course will introduce you to Splunk's interface and basic searching techniques, and cover how to create reports, dashboards, and visualizations. By the end of the course, you will be equipped with the foundational skills to navigate Splunk, perform basic searches, and continue on your learning journey with our wide offering of educational classes.

### Prerequisites

- No prerequisites are required for this course.

### Course Outline

#### Module 1 – Intro to Splunk

- Splunk components
- Basic Splunk functions

#### Module 2 – Using Splunk

- Define Splunk apps
- Understand Splunk user roles
- Search & Reporting app
- Splunk Web interface

#### Module 3 – Using Search

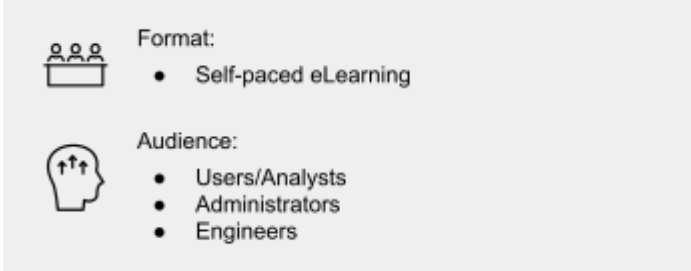
- Run basic searches
- Set the time range of a search
- Save search results
- Identify the contents of search results
- Work with events
- Share search jobs
- Export search results
- Select search modes
- Control a search job

#### Module 4 – Exploring Events

- Refine searches
- Understand timestamps
- Use the events tab to add and remove terms from a search

#### Module 5 – Search Processing Language

- Use wildcards to search for multiple terms
- Understand case sensitivity in searches
- Use booleans to include and exclude search criteria



**Format:**

- Self-paced eLearning

**Audience:**

- Users/Analysts
- Administrators
- Engineers

- Use special characters with search terms

## Module 6 – What are Commands?

- Understand the anatomy of Splunk's search language:
  - Search terms
  - Commands
  - Functions
  - Arguments
  - Clauses
- Understand best practices for writing searches

## Module 7 – What are Knowledge Objects?

- Identify the five categories of knowledge objects:
  - Data interpretation
  - Data classification
  - Data Enrichment
  - Data Normalization
  - Data Models
- Understand types of knowledge objects

## Module 8 – Creating Reports and Dashboards

- Save a search as a report
- Edit reports
- Use transforming commands to create visualizations
- Create a dashboard
- Add a report to a dashboard
- Edit a dashboard

## About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email [education@splunk.com](mailto:education@splunk.com).