Intro to Splunk

This eLearning course teaches students how to use Splunk to create reports and dashboards and explore events using Splunk's Search Processing Language. Students will learn the basics of Splunk's architecture, user roles, and how to navigate the Splunk Web interface to create robust searches, reports, visualizations, and dashboards..

Course Topics

- Introduction to Splunk's interface
- Basic searching
- Using fields in searches
- Search fundamentals
- Transforming commands
- Creating visualizations
- Creating reports and dashboards
- Identifying types of knowledge objects

Prerequisite Knowledge

None

Course Format

eLearning

Course Objectives

Topic 1 – Intro to Splunk

- Splunk components
- Basic Splunk functions

Topic 2 – Using Splunk

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

Topic 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

Topic 4 - Exploring Events

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

Topic 5 – Search Processing Language

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

Topic 6 – What are Commands?

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

Topic 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

Topic 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

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.
270 Brannan St. San Francisco, CA 94107
+1 866.GET.SPLUNK (1 866.438.7758)
Contact sales