Search Expert 1

This "Fast Start" course covers over 60 commands and functions and prepares students to be search experts. Students will learn how to effectively utilize time in searches, work with different time zones, use transforming commands and eval functions to calculate statistics, compare field values with eval functions and eval expressions, manipulate output, normalize fields and field values, use lookups and subsearches to enrich results, and correlate and filter data from multiple sources.

Course Topics

- Working with Time
- Statistical Processing
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis

Prerequisite Knowledge

To be successful, students should have a solid understanding of the following:

- How Splunk Works
- Creating Search queries
- Knowledge objects (specifically reports, lookups, and fields)

Course Format

Instructor-led

Course Objectives

Topic 1 – Working with Time

- Searching with Time
- Formatting Time
- Comparing Index Time versus Search Time
- Using Time Commands
- Working with Time Zones

Topic 2 – Statistical Processing

- What is a Data Series?
- Transforming Data
- Manipulating Data with eval
- Formatting Data

Topic 3 – Comparing Values

- Using eval to Compare
- Filtering with where

Topic 4 – Result Modification

- Manipulating Output
- Modifying Results Sets
- Managing Missing Data
- Modifying Field Values
- Normalizing with eval

Topic 5 – Leveraging Lookups and Subsearches

- Using Lookup Commands
- Adding a Subsearch
- Using the return Command

Topic 6 – Correlation Analysis

- Calculate Co-Occurrence Between Fields
- Analyze Multiple Datasets

What You Learn

- Utilize over 60 commands and functions to transform, manipulate, normalize, correlate, and filter data.
- Filter data using time modifiers and time commands and use formatting functions to accommodate various time formats.
- Calculate statistics using transforming commands and mathematical and statistical eval functions.
- Compare, manipulate, and normalize data using several commands including the all-powerful eval command and an array of statistical, comparison, conditional, and formatting functions.
- Enrich results with lookups and subsearches to correlate and filter data from multiple sources and use specific commands to calculate co-occurrence between fields and analyze data from multiple datasets.

Skills You Will Gain

Big Data, Business Analytics, Business Intelligence, Data Analysis, Data Analysis Software, Data Science, Data Visualization, Machine Learning, Problem Solving, Statistics, Syntax

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