Splunk Search Expert Fast Start

(SP-SE-FS)

COURSE OVERVIEW

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.

PREREQUISITES

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)

OR have taken the following:

- Foundation Fast Start OR
- What is Splunk? (Retired), Intro to Splunk (ITS) and [Using Fields (SUF)

COURSE OUTLINE

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

Splunk Search Expert Fast Start

(SP-SE-FS)

COURSE OUTLINE

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

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

Splunk Search Expert Fast Start

(SP-SE-FS)

COURSE OUTLINE

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