Splunk Search Expert Fast Start (SE-FS)

Course Summary:

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 sub searches to enrich results, and correlate and filter data from multiple sources.

Course Duration:

3 Days

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 Objectives:

- Working with Time (WWT)
- Statistical Processing (SSP)
- Comparing Values (SCV)
- Result Modification (SRM)
- Leveraging Lookups and Subsearches (LLS)
- Correlation Analysis (SCLAS)

Course Outlines:

Module 1 – Working with Time

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

Module 2 – Statistical Processing

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

Module 3 – Comparing Values

- Using eval to Compare
- Filtering with were

Module 4 – Result Modification

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

Module 5 – Leveraging Lookups and Subsearches

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

Module 6 - Correlation Analysis

- Caclulate Co-Occurance Between Fields
- Analyze Multiple Datasets