SP-POWER-U - Splunk Power User Fast Start

Days: 4

Prerequisites: Students should understand how Splunk works and be able to create basic searches and visualizations.

Audience: Splunk users, analysts, and aspiring power users who need advanced search, reporting, field extraction, correlation, and knowledge-management skills.

Description: This four-day instructor-led fast-start course covers more than 60 Splunk commands, functions, and knowledge objects. Students learn searching best practices, statistical processing, result manipulation, correlation, field extraction, and data modeling to turn machine data into actionable information.

Course Objectives: Upon completion of this course, students will:

- Use more than 60 commands and functions to transform, manipulate, normalize, correlate, and filter data.
- Work effectively with time modifiers, time commands, time formats, and time zones.
- Calculate and present statistics using transforming commands and eval functions.
- Compare, manipulate, and normalize field values and result sets.
- Analyze multiple datasets and calculate co-occurrence between fields.
- Create, manage, and share knowledge objects, field extractions, and data models.

OUTLINE:

MODULE 1: WORKING WITH TIME

- Formatting time
- Index time versus search time
- Time commands
- Time zones

MODULE 2: STATISTICAL PROCESSING

- Data series
- Transforming data
- Manipulating data with eval
- Formatting data

MODULE 3: COMPARING VALUES

- Use eval to compare values
- Filter with where

MODULE 4: RESULT MODIFICATION

- Manipulate output and result sets
- Manage missing data
- Modify and normalize field values

MODULE 5: CORRELATION ANALYSIS

- Calculate co-occurrence between fields
- Analyze multiple datasets

MODULE 6: INTRODUCTION TO KNOWLEDGE OBJECTS

- Knowledge object concepts and settings
- Manage knowledge objects

MODULE 7: CREATING KNOWLEDGE OBJECTS

- Search-time operations
- Event types and Event Type Builder
- Workflow actions
- Tags and aliases
- Search macros

MODULE 8: CREATING FIELD EXTRACTIONS

- Field Extractor
- Regex field extractions
- Delimited field extractions

MODULE 9: DATA MODELS

- Data model datasets
- Design data models
- Create pivots
- Accelerate data models