Course Outline

Splunk Advanced User

Course Summary

Objective

After completing this course, students will be able to:
- Create complex searches
- Customize dashboards
- Optimize performance of search queries.

Audience

The “Advanced Splunk User” course is targeted for more experienced and knowledgeable users of Splunk.

Topics

- Introduction to Knowledge Objects
- Filtering & Formatting Results
- Creating Field Extractions
- Creating Field Aliases and Calculated Fields
- Creating Tags and Event Types

Prerequisite

Before taking this course, students should have taken the Splunk User course.

Duration

Two Days
Splunk Advanced User

Course Outline

I. Introduction to Knowledge Objects
   A. Identify naming conventions
   B. Review permissions
   C. Manage knowledge objects

II. Filtering & Formatting Results
   A. The eval command
   B. Using the search and where commands to filter results
   C. The filnull command

III. Creating Field Extractions
   A. Perform regex field extractions using the Field Extractor (FX)
   B. Perform delimiter field extractions using the FX

IV. Creating Field Aliases and Calculated Fields
   A. Describe, create, and use field aliases
   B. Describe, create and use calculated fields

V. Creating Tags and Event Types
   A. Create and use tags
   B. Describe event types and their uses
   C. Create an event type