Course Outline

Splunk Bootcamp

Course Summary

Topics

- Splunk User Course
- Splunk Advanced User Course
- Splunk Advanced Searching, Reporting & Visualizations

Prerequisite

A basic knowledge of Splunk/completion of the Splunk Fundamentals 1 course is required for this course. We will set up a lab environment that they will be able to access via their personal laptops

Duration

Four Days

Course Outline

Splunk Bootcamp

Course Outline

I. ***Splunk User Course*** (prerequisite: none).
The Splunk User course is targeted for beginner and intermediate users of Splunk.
A. Introduction to Splunk
B. Basic Searching
C. Using Fields in Search
D. Search Language Fundamentals
E. Using Basic Transforming Commands
F. Creating Reports & Dashboards
G. Creating & Using Lookups
H. Creating Scheduled Reports & Alerts
I. Using Pivot

II. ***Splunk Advanced User Course*** (prerequisite: Splunk User Course).
The Splunk Advanced User course is targeted for more experienced and knowledgeable users of Splunk.
A. Introduction to Knowledge Objects
B. Filtering & Formatting Results
C. Creating Field Extractions
D. Creating Field Aliases and Calculated Fields
E. Creating Tags and Event Types
F. Creating & Using Macros
G. Creating Workflow Actions
H. Creating Data Models & Testing with Pivot
I. Datasets & the Common Information Model

III. ***Splunk Advanced Searching, Reporting & Visualizations*** (prerequisite: Splunk User Course, Splunk Advanced User Course and a working knowledge of CLI for the Visualizations piece).
The Splunk Advanced Searching, Reporting & Visualizations focuses on more advanced search and reporting commands along with an overview of how to create custom visualizations.
A. Using Search Efficiently
B. Search Tuning
C. Manipulating and Filtering Data
D. Working with Multivalue Fields
E. Using Advanced Transactions
F. Working with Time
G. Combining Searches
H. Using Subsearches
I. Creating Custom Visualizations