Using Fields

Course Description:

This course is for power users who want to learn about fields and how to use fields in searches.

The course will focus on explaining the role of fields in searches, field discovery, using fields in searches, and the difference between persistent and temporary fields. The last topic will introduce how fields from other data sources can be used to enrich search results

Course Duration:

3 Hours

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- How Splunk works
- Creating search queries
- Knowledge objects

Course Outlines:

Module 1 – What are Fields?

- Define fields and field auto-extraction
- Explore the Fields sidebar
- Add fields to the Selected Fields list
- Explore and generate reports from the Fields window

Module 2 – What is Field Discovery?

- Understand Field Discovery
- Explore search modes and their effect on search results

Module 3 – Use Fields in Searches

- Use fields correctly in basic searches
- Use fields with operators
- Use the rename command
- Use the fields command to improve search performance

Module 4 – Compare Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Module 5 – Enrich Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

Target Audience:

- Users/Analysts
- Administrators
- Engineers