Comparing Values

Course Description:

This course is designed for Splunk users, analysts, and administrators who want to compare and analyze datasets.

You will use the eval, where, and if commands, along with the like and case functions to compare and visualize datasets.

Course Duration:

3 Hours

Prerequisites:

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

- Intro to Splunk
- Using Fields
- Visualizations
- Working with Time
- Statistical Processing

Course Outlines:

Module 1 – Using eval to Compare

- Explore the eval command
- Explain evaluation functions
- Identify and use comparison, conditional, and text functions
- Normalize data with the case function
- Use the fieldformat command to format field values

Module 2 – Filtering with where & Managing Missing Data

- Use the where command to filter results
- Use wildcards with the where command
- Filter fields with the information functions, isnull and isnotnull
- Manage missing data with the fillnull command

Target Audience:

- Users/Analysts
- Administrators
- Engineers