Multivalue Fields

Course Description:

This course is for power users who want to become experts on searching and manipulating multivalue data.

The course will focus on using multivalue eval functions and multivalue commands to create, evaluate, and analyze multivalue data.

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

Course Outlines:

Module 1 – What are Multivalue Fields?

- Define multivalue fields
- Define self-describing data
- Understand how JSON data is handled in Splunk
- Use the spath command to interpret self-describing data
- Manipulate multivalue fields with mvzip and mvexpand
- Convert single-value fields to multivalue fields with specific commands and functions

Module 2 – Create Multivalue Fields

- Create multivalue fields with the makemv command and the split function of the eval command

Module 3 – Evaluate Multivalue Fields

- Use the mvcount, mvindex, and mvfilter eval functions to evaluate multivalue fields

Module 4 – Analyze Multivalue Data

- Use the mvsort, mvzip, mvjoin, mvmap, and mvappend eval functions and the mvexpand command to analyze multivalue data

Target Audience:

- Users/Analysts