Result Modification

Course Description:

This course is designed for Splunk users, analysts, and administrators who want to learn how to modify and manipulate output and normalize data.

You will learn how to use the untable, xyseries, appendpipe, eventstats, and streamstats commands to modify result sets and use the eval command and eval functions to manipulate field values and normalize data across multiple data sources.

Course Duration:

1 Day

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
- Comparing Values

Course Outlines:

Module 1 – Manipulating Output

- Convert a 2-D table into a flat table with the untable command
- Convert a flat table into a 2-D table with the xyseries command

Module 2 – Modifying Result Sets

- Append data to search results with the appendpipe command
- Calculate event statistics with the eventstats command
- Calculate "streaming" statistics with the streamstats command

Module 3 – Modifying Field Values

- Understand the eval command
- Use conversion and text eval functions to modify field values
- Reformat fields with the foreach command

Module 4 – Normalizing with eval

- Normalize data with eval functions
- Identify eval functions to use for data and field normalization

Target Audience:

- Users/Analysts
- Administrators
- Engineers