Statistical Processing

Course Description:

This course is for Splunk users, analysts, and administrators who want to advance their data analysis skills using Splunk's statistical commands.

This course covers essential statistical functions and commands such as stats, eventstats, streamstats, and tstats with a focus on summarizing, analyzing, and reporting on large 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

Course Outlines:

Module 1 – What is a Data Series

- Introduce data series
- Explore the difference between single-series, multi-series, and time series data series

Module 2 – Transforming Data

- Use the chart, timechart, top, and rare commands to transform events into data tables

Module 3 – Statistical Aggregation with the stats Command

- Define aggregation
- Explore the stats command and eight of its functions

Module 4 – Manipulating Data with the eval Command

- Explore the eval command
- Explore and perform calculations using mathematical and statistical eval functions
- Perform calculations and concatenations on field values
- Use the eval command as a function with the stats command

Module 5 – Formatting Data

- Use the rename command
- Use the sort command

Target Audience:

- Users/Analysts
- Administrators
- Engineers