Correlation Analysis

Course Description:

This course is designed for Splunk power users who want to calculate co-occurrence between fields and analyze data from multiple datasets.

You will learn how to use the transaction, append, appendcols, union, and join commands to correlate events and combine data from various 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
- Result Modification
- Scheduling Reports and Alerts
- Introduction to Dashboards

Course Outlines:

Module 1 – Calculate Co-Occurence Between Fields

- Understand transactions
- Explore the transaction command

Module 2 – Analyze Multiple Data Sources

- Understand subsearch
- Use the append, appendcols, union, and join commands to combine, analyze, and compare multiple data sources

Target Audience:

- Users/Analysts
- Administrators
- Engineers