Leveraging Lookups and Subsearches

Course Description:

This course is designed for Splunk users, analysts, and administrators who want to enhance their searches with lookups and subsearches.

You will learn how to use lookups to enrich your data and how to write subsearches to correlate and filter data from multiple sources.

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
- Comparing Values
- Result Modification
- Scheduling Reports and Alerts
- Introduction to Dashboards

Course Outlines:

Module 1 – Using Lookup Commands

- Understand lookups
- Use the inputlookup command to search lookup files
- Use the lookup command to invoke field value lookups
- Use the outputlookup command to create lookups
- Invoke geospatial lookups in search

Module 2 – Adding a Subsearch

- Define subsearch
- Use subsearch to filter results
- Identify when to use subsearch
- Understand subsearch limitations and alternatives

Module 3 – Using the return Command

- Use the return command to pass values from a subsearch
- Compare the return and fields commands

Target Audience:

- Users/Analysts
- Administrators
- Engineers