

## **SPLK-LLS: Leveraging Lookups and Subsearches**

Course Code: SPLK-LLS

Duration: 1 day

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### **OVERVIEW**

This three-hour course is designed for power users who want to learn how to use lookups and subsearches to enrich their results. Topics will focus on lookup commands and explore how to use subsearches to correlate and filter data from multiple sources.

### **SKILLS COVERED**

- Please refer to course overview

### **WHO SHOULD ATTEND?**

Search Experts Knowledge Managers

### **PREREQUISITES**

To be successful, students should have a solid understanding of the following:

- How Splunk works
- Creating Search queries
- Lookups

### **MODULES**

#### **Module 1: Using Lookup Commands**

- Understand lookups
- Use the inputlookup command to search lookup files
- Use the lookup command to invoke field value 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

**END OF PAGE**