

## Leveraging Lookups and Subsearches

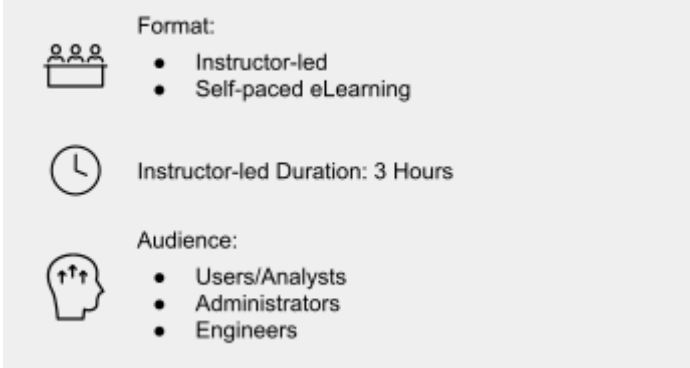
### Summary

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.

### 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



**Format:**

- Instructor-led
- Self-paced eLearning

**Instructor-led Duration: 3 Hours**

**Audience:**

- Users/Analysts
- Administrators
- Engineers

### Course Outline

#### 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

## About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email [education@splunk.com](mailto:education@splunk.com).