Enriching Data with Lookups

(SP-EDL)

COURSE OVERVIEW

This three-hour module is for knowledge managers who want to use lookups to enrich their search environment. Topics will introduce lookup types and cover how to upload and define lookups, create automatic lookups, and use advanced lookup options. Additionally, students will learn how to verify lookup contents in search and review lookup best practices.

PREREQUISITES

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

- How Splunk works
- Knowledge Objects

WHO SHOULD ATTEND

Knowledge Managers

COURSE OBJECTIVES

- What is a Lookup?
- Creating Lookups
- Geospatial Lookups
- External Lookups
- KV Store Lookups
- Best Practices for Lookups

Enriching Data with Lookups (SP-EDL)

COURSE OUTLINE

Module 1 - What is a Lookup?

- Define a lookup and the default lookup types
- Lookups and the search-time operation sequence

Module 2 - Create Lookups

- Describe lookups at search time
- Use file-based lookups
- Examine a CSV lookup file
- Create (upload, define, configure) a lookup
- Apply advanced lookup options
- Create and use an automatic lookup at search

Module 3 - Geospatial Lookups

- Describe the use of geospatial lookups
- Examine KML/KMZ geospatial lookup files
- Add a geospatial lookup file
- Define a geospatial lookup

Module 4 - External Lookups

- Define the use of external lookups
- Examine an external_lookup.py lookup script
- Configure external lookups

Module 5 - KV Store Lookups

- Define the use of KV Store lookups
- Identify the steps to set up a KV Store lookup
- Examine the KV Store lookups collections.conf file
- Create a KV Store lookup definition
- Identify options for populating a KV Store lookup
- Compare file-based CSV lookups to KV Store lookups

Module 6 - Best Practices for Lookups

- Various best practices for using lookups

1900 Campus Commons Drive, Suite 100
Reston, VA 20191 703.972.2288