Enriching Data with Lookups

Course Description:

This course is for knowledge managers who want to use lookups to enrich their search environment.

The course 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.

Course Duration:

1 Day

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- How Splunk works
- Knowledge objects

Course Outlines:

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

Target Audience:

- Knowledge Manager