Creating Field Extractions

Course Description:

This course is for knowledge managers who want to learn about field extraction and the Field Extractor (FX) utility.

The course will cover when certain fields are extracted and how to use the FX to create regex and delimited field extractions.

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 – Use the Field Extractor

- Explore the different types of extracted fields and when they are extracted
- Define the Splunk Web Field Extractor (FX)

Module 2 – Create Regex Field Extractions

- Identify basics of regular expressions (regex)
- Explore the regex field extraction workflow
- Edit regex for field extractions

Module 3 – Create Delimited Field Extractions

- Identify delimited field values in event data
- Explore the delimited field extraction workflow
- Explain the use of forwarder management
- Configure forwarders to be deployment clients
- Managing forwarders using deployment apps

Target Audience:

- Knowledge Managers