Creating Knowledge Objects

Course Description:

This course is for knowledge managers.

The course will teach how to create knowledge objects for their search environment using the Splunk web interface. Topics will cover types of knowledge objects, the search-time operation sequence, and the processes for creating event types, workflow actions, tags, aliases, search macros, and calculated fields.

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 – Knowledge Objects & Search-time Operations

- Understand role of knowledge objects for enriching data
- Define search-time operation sequence

Module 2 – Create Event Types

- Define event types
- Create event types using three methods
- Use event types
- Find event types
- Tag event types
- Compare event types and reports

Module 3 – Create Workflow Actions

- Administer Splunk user roles
- Integrate Splunk with LDAP, Active Directory, or SAML

Module 4 – Create Tags and Aliases

- Describe field aliases
- Create field aliases
- Search with field aliases
- Define tags
- Create and view tags
- Search with tags
- Manage tags

Module 5 – Create Search Macros

- Define macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Use nested macros
- Use macros with other knowledge objects
- Use tags/event types with macros
- Create macros: considerations

Module 6 – Create Calculated Fields

- Explain calculated fields
- Create a calculated field
- Use a calculated field

Target Audience:

- Knowledge Managers