

## Creating Knowledge Objects

### Summary

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.

### Prerequisites

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

### Course Outline

#### 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

**Format:**

- Instructor-led
- Self-paced eLearning

**Instructor-led Duration: 3 Hours**

**Audience:**

- Knowledge Managers

## 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

## 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).