Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Creating Knowledge Objects

CODE:	LENGTH:	PRICE:
SPL_SCKO	0.96 Hours (0.12 days)	€500.00

Description

This three-hour course is for knowledge managers who want to learn 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.

Objectives

- Knowledge Objects and Search-time Operations
- Creating Event Types
- Using Event Type Builder
- Creating Workflow Actions
- Creating Tags and Aliases
- Creating Serach Macros

Audience

Knowledge Managers

Prerequisites

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

- How Splunk works
- Knowledge Objects

Programme

Topic 1 – Knowledge Objects & Search-time Operations

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

Topic 2 – Creating Event Types

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

Topic 3 – Creating Workflow Actions

- Identify what are workflow actions
- Create a GET, POST, and search workflow action
- Test workflow actions

Topic 4 – Creating Tags and Aliases

- Describe field aliases and tags
- Create field aliases and tags
- Search with field aliases and tags

Topic 5 – Creating Search Macros

- Explain search macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Create and use nested macros
- Use macros with other knowledge objects

Topic 6 – Creating Calculated Fields

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

Further Information

Individuals who enroll in this class will also be enrolled in an (eLearning with Labs) component. Completion of labs and quizzes is required in order to receive proof of completion.

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.