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

Splunk Search Expert Fast Start

CODE:	LENGTH:	PRICE:
SPL_SSEFS	24 Hours (3 days)	€3,000.00

Description

This "Fast Start" course covers over 60 commands and functions and prepares students to be search experts. Students will learn how to effectively utilize time in searches, work with different time zones, use transforming commands and eval functions to calculate statistics, compare field values with eval functions and eval expressions, manipulate output, normalize fields and field values, use lookups and subsearches to enrich results, and correlate and filter data from multiple sources.
This class will take place over three 6-hour days (plus a 1-hour break each day)

Objectives

- Working with Time
- Statistical Processing
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis

Prerequisites

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

- How Splunk Works
- Creating Search queries
- Knowledge objects (specifically reports, lookups, and fields)

OR have taken the following:

- Foundation Fast Start OR
- What is Splunk, Intro to Splunk and Using Fields

Programme

Topic 1 – Working with Time

- Searching with Time
- Formatting Time
- Comparing index Time versus Search Time
- Using Time Commands
- Working with Time Zones

Topic 2 – Statistical Processing

- What is a Data Series?
- Transforming Data
- Manipulating Data with eval
- Formatting Data

Topic 3 – Comparing Values

- Using eval to Compare
- Filtering with where

Topic 4 – Result Modification

- Manipulating Output
- Modifying REsults Sets
- Managing Missing Data
- Modifying Field Values
- Normalizing with eval

Topic 5 – Leveraging Lookups and Subsearches

- Using Lookup Commands
- Adding a Subsearch
- Using the return Command

Topic 6 - Correlation Analysis

- Caclulate Co-Occurance Between Fields
- Analyze Multiple Datasets

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

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