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

Working with Time

CODE:	LENGTH:	PRICE:
SPL_SWWT	3.36 Hours (0.42 days)	€500.00

Description

This three-hour course is for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones.

Objectives

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

Audience

Search Experts Knowledge Managers

Prerequisites

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

- How Splunk works
- Creating Search queries
- The eval command

Programme

Topic 1 – Searching with Time

- Understand the_time field and timestamps
- View and interact with the event Timeline
- Use the earliest and latest time modifiers
- Use the bin command with the _time field

Topic 2 – Formatting Time

- Use various date and time eval functions to format time

Topic 3 – Using Time Commands

- Use the timechart command
- Use the timewrap command

Topic 4 – Working with Time Zones

- Understand how time and timezones are represented in your data
- Determine the time zone of your server
- Use strftime to correct timezones in results

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.