Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Using Fields

CODE:	LENGTH:	PRICE:
SPL_SUF	0.96 Hours (0.12 days)	kr5,075.00

Description

This three-hour course is for power users who want to learn about fields and how to use fields in searches. Topics will focus on explaining the role of fields in searches, field discovery, using fields in searches, and the difference between persistent and temporary fields. The last topic will introduce how fields from other data sources can be used to enrich search results.

Objectives

- What are Fields
- What is Field Discovery
- Using Fields in Searches
- Comparing Temporary versus Persistent Fields
- Enriching Data

Audience

Search Experts Knowledge Managers

Prerequisites

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

- How Splunk works
- Creating Search queries
- Knowledge Objects

Programme

Topic 1 – What are Fields?

- Understand fields and field auto-extraction
- Explore the Fields sidebar
- Add fields to the Selected Fields list
- Explore and generate reports from the Fields window

Topic 2 – What is Field Discovery?

- Understand Field Discovery
- Explore search modes and their effect on search results

Topic 3 – Using Fields in Searches

- Use fields correctly in basic searches
- Use fields with operators
- Use the rename command
- Use the fields command to improve search performance

Topic 4 – Comparing Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields

- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Topic 5 – Enriching Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

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

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.