Using Fields (SUF)

ID SUF **Price** on request **Duration** 3 hours

Who should attend

Splunk modules are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Prerequisites

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

- How Splunk works
- Creating search queries
- Knowledge objects

Course Objectives

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

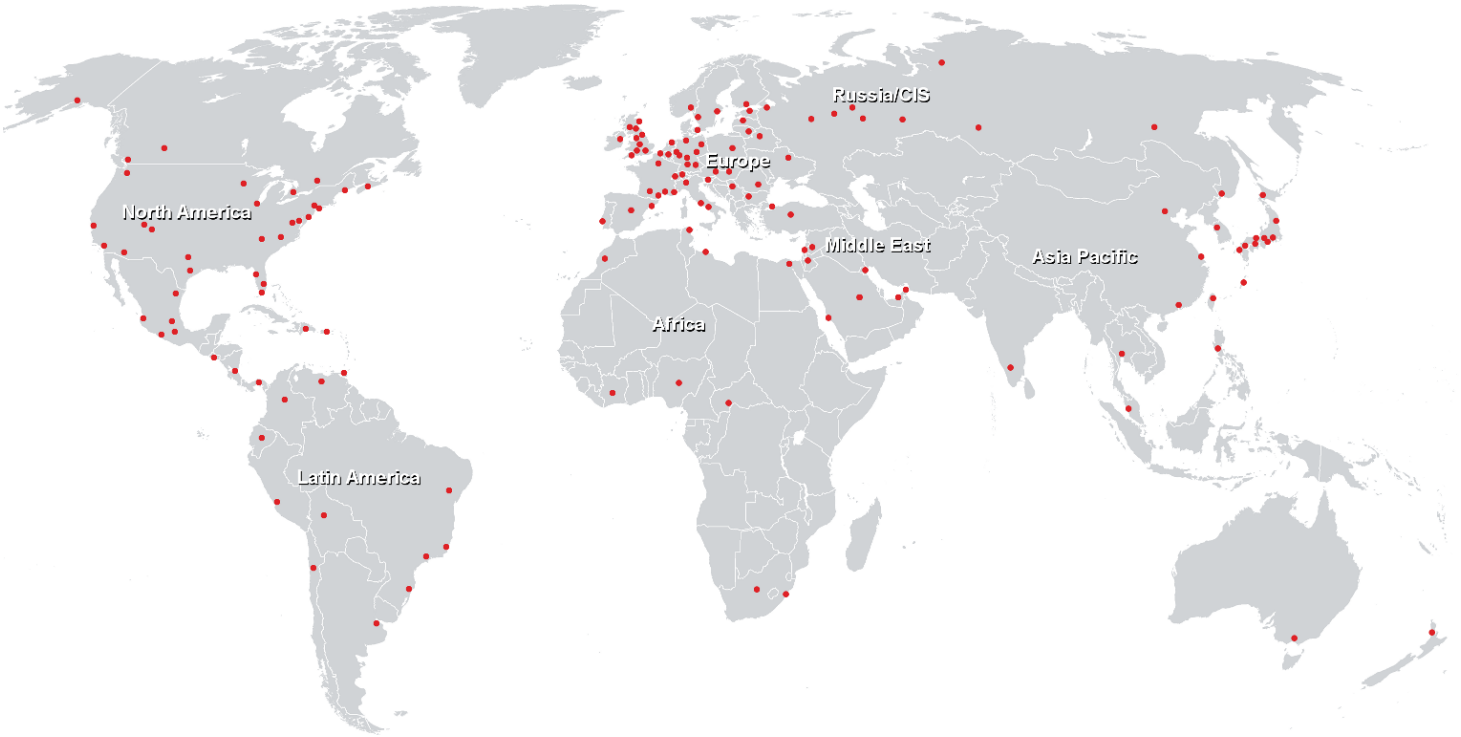
- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Topic 5 – Enriching Data

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

Using Fields (SUF)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch