

## Splunk Search Expert Fast Start (SE-FS)

ID SE-FS Prix CHF 3 300,- (Hors Taxe) Durée 3 jours

### Pré-requis

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? (WIS), [Intro to Splunk \(ITS\)](#) and [Using Fields \(SUF\)](#)

### Objectifs

At the end of the course, you should be able to :

- Search with Time
- Format Time
- Compare Index Time versus Search Time
- Use Time Commands
- Work with Time Zones
- Understand what is Data Series
- Transform Data
- Manipulate Data with eval
- Format Data
- Use eval to Compare
- Filter with where
- Manipulate Output
- Modify Result Sets
- Manage Missing Data
- Modify Field Values
- Normalize with eval
- Use Lookup Commands
- Add a Subsearch
- Use the return Command
- Calculate Co-Occurrence Between Fields
- Analyze Multiple Datasets

- 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

### Contenu

#### Topic 1 – Working with Time

---

## Splunk Search Expert Fast Start (SE-FS)

---

### Centres de formation dans le monde entier



### Fast Lane Institute for Knowledge Transfer (Switzerland) AG

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

[info@flane.ch](mailto:info@flane.ch), <https://www.flane.ch>