Splunk Power User Fast Start (POWER-U)

ID POWER-U **Prix** CHF 4 400,– (Hors Taxe) **Durée** 4 jours

A qui s'adresse cette formation

- Utilisateurs Splunk souhaitant approfondir leurs compétences en recherche et analyse de données
- Analystes de données ou analystes SOC travaillant avec Splunk
- Administrateurs ou ingénieurs IT utilisant Splunk au quotidien
- Professionnels souhaitant maîtriser les fonctionnalités avancées de recherche et de gestion des connaissances dans Splunk

Cette formation prépare à la/aux certifications

Splunk Core Certified Power User (SCCPU)
Splunk Core Certified Advanced Power User (SPCCAPU)

Pré-requis

Pour réussir, vous devez avoir une bonne compréhension des éléments suivants :

- Fonctionnement de Splunk
- Création de recherches et visualisations de base
- RECOMMANDÉ : Splunk Search Expert Fast Start (SE-FS)

Objectifs

A l'issue de la formation, vous devrez être en mesure de :

- Utiliser plus de 60 commandes et fonctions pour transformer, manipuler, normaliser, corréler et filtrer les données
- Filtrer les données à l'aide de modificateurs temporels et de commandes liées au temps, et utiliser des fonctions de formatage pour gérer différents formats de date et d'heure
- Calculer des statistiques à l'aide de commandes de transformation ainsi que de fonctions mathématiques et statistiques eval
- Comparer, manipuler et normaliser les données à l'aide de plusieurs commandes, notamment la commande eval et un ensemble de fonctions statistiques, de comparaison, conditionnelles et de formatage
- Calculer les cooccurrences entre champs et analyser des données provenant de plusieurs ensembles de données
- Créer, organiser, gérer et partager des objets de connaissance

Contenu

Sujet 1 – Working with Time

- Formatage du temps
- Comparaison entre le temps d'indexation et le temps de recherche
- Utilisation des commandes temporelles
- Gestion des fuseaux horaires

Sujet 2 – Statistical Processing

- Qu'est-ce qu'une série de données ?
- Transformation des données
- Manipulation des données avec eval
- Formatage des données

Sujet 3 – Comparing Values

- Utiliser eval pour comparer
- Filtrer avec where

Sujet 4 – Results Modification

- Manipulation des sorties
- Modification des ensembles de résultats
- Gestion des données manquantes
- Modification des valeurs de champs
- Normalisation avec eval

Sujet 5 – Correlation analysis

- Calculer la cooccurrence entre champs
- Analyser plusieurs ensembles de données

Sujet 6 – Introduction to Knowledge Objects

- Que sont les objets de connaissance ?
- Paramètres des objets de connaissance
- Gestion des objets de connaissance

Sujet 7 – Creating Knowledge Objects

- Objets de connaissance et opérations au moment de la recherche
- Création de types d'événements
- Utilisation du générateur de types d'événements
- Création d'actions de workflow
- Création de tags et d'alias
- Création de macros de recherche

Sujet 8 – Creating Fields extraction

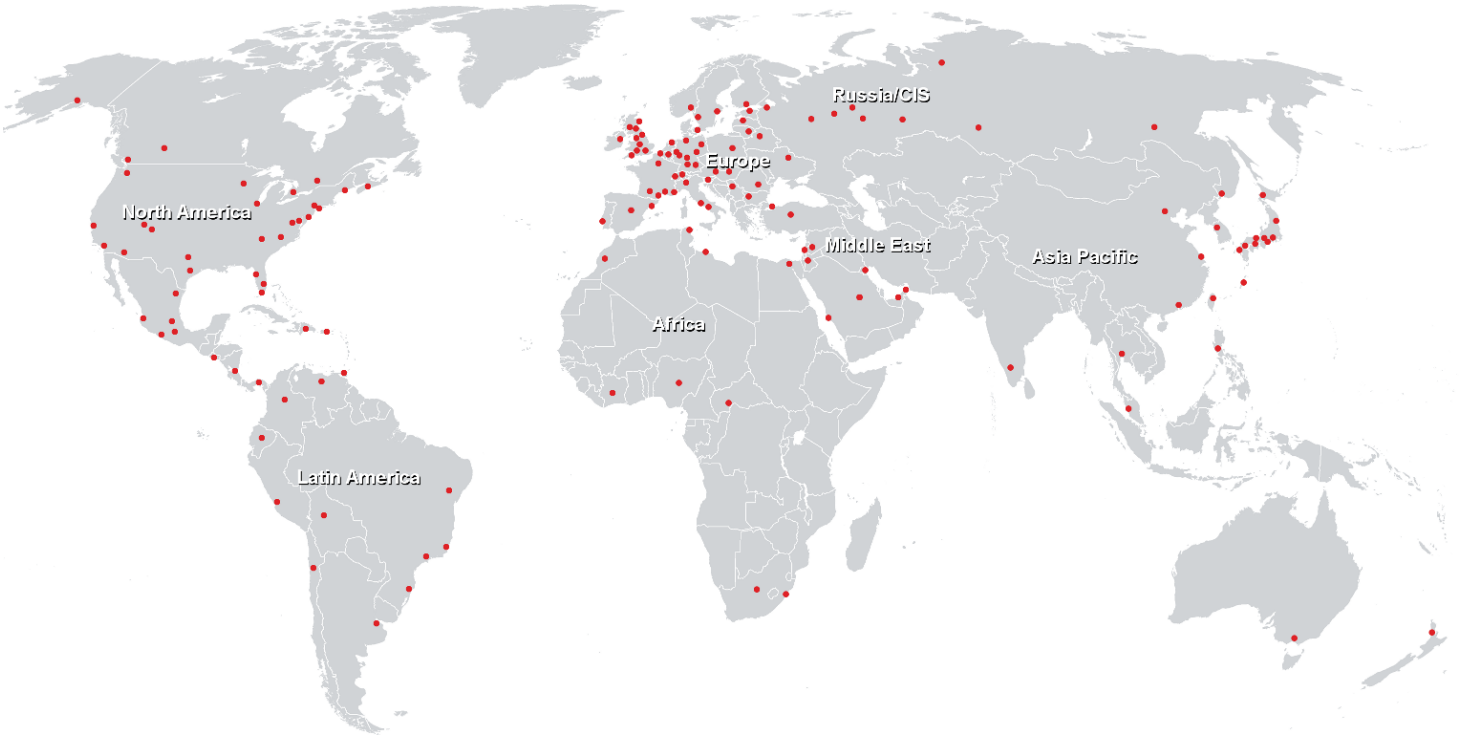
- Utilisation de l'outil d'extraction de champs
- Création d'extractions de champs avec regex
- Création d'extractions de champs délimités

Sujet 9 – Data models

- Introduction aux ensembles de données des modèles de données
- Conception de modèles de données
- Création d'un pivot
- Accélération des modèles de données

Splunk Power User Fast Start (POWER-U)

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, https://www.flane.ch