Splunk Enterprise Data Administration (SEDA)

ID SEDA **Prix** CHF 2 500,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

- Les administrateurs qui sont responsables de la transmission des données aux indexeurs Splunk.

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Admin (SECA)
Splunk Certified Cybersecurity Defense Engineer (SCCDE)

Pré-requis

Pour réussir, les étudiants doivent avoir une solide compréhension des modules suivants :

- Fondamentaux 1
- Fondamentaux 2

Ou les modules à sujet unique suivants :

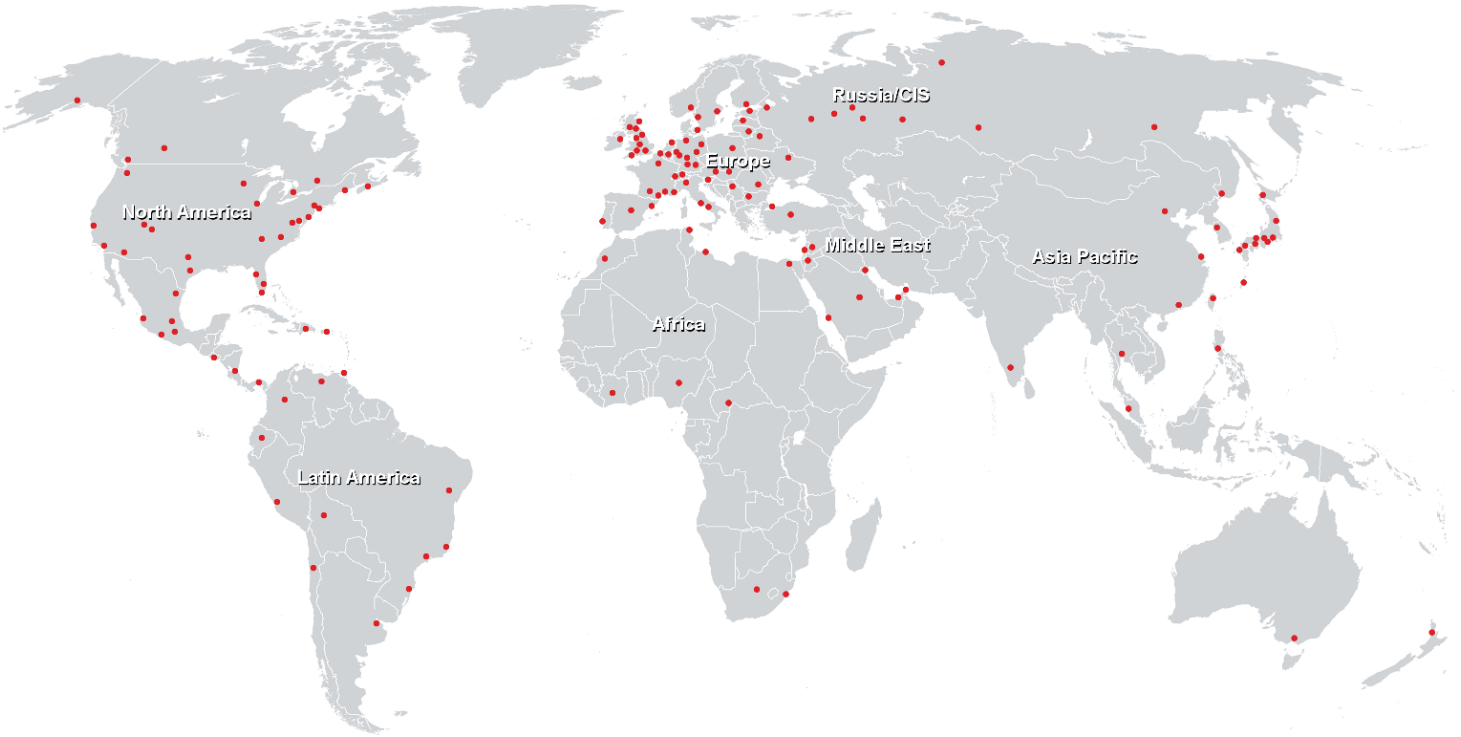
- !What is Splunk? (WIS)
- Introduction à Splunk (ITS)
- Introduction aux objets de connaissance (IKO)
- Créer des objets de connaissance (CKO)
- Créer des champs d'extraction (CFE)

Objectifs

- Comprendre les types de sources
- Gérer et déployer des transitaires
- Configurer les entrées de données
- Moniteurs de fichiers
- Entrées réseau (TCP/UDP)
- Entrées de scripts
- Entrées HTTP (via le collecteur d'événements HTTP)
- Personnaliser le processus d'analyse syntaxique de la phase d'entrée
- Définir des transformations pour modifier les données avant l'indexation
- Définir les configurations des objets de connaissance au moment de la recherche

Splunk Enterprise Data Administration (SEDA)

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