ArcSight 7.x FlexConnector Configuration (ASFC160-76)

ID ASFC160-76 **Prix** sur demande **Durée** 3 jours

A qui s'adresse cette formation

This course is intended for security administrators, content authors/architects, and IT integrators, who build and install custom connectors to provide critical event data feeds to ArcSight ESM or Logger. This can include senior analysts for networks, security systems, enterprise applications and databases.

Pré-requis

To be successful in this course, you should have the following prerequisites or knowledge:

- Successful completion of ArcSight ESM Admin and Analyst course
- Successful completion of ArcSight ESM Advanced Administrator course
- Working knowledge of Regular Expressions

Contenu

Introduction to FlexConnector

- Define SmartConnectors and their functions
- Follow device deployment and the event flow processing
- Describe FlexConnectors types
- Install a Connector

Using the ArcSight Schema

- Gather event requirements prior to developing your FlexConnector
- Normalize and map events
- Differentiate special cases
- List the different schema groups

Basic Configuration File and Categorization

- Locate FlexConnector files
- Define the configuration procedure
- Apply the four steps to create a FlexConnector configuration file
    - Parser configuration
    - Token declaration
    - Event mapping
    - Severity mapping
- Use the FlexConnector wizard to install a configuration file
- Utilize Categorization to profile an event
o Six criteria are used: Object, Behavior, Outcome, Technique, Device Group, and Significance

Regex FlexConnectors

- Install the Regex File Reader FlexConnector
- Create common Regex
- Define SubMessages
- Use the Regex Tester

Installing ESM Syslog Connectors with Custom Parsers

- Identify the syslog Connectors
- Describe the syslog FlexConnector components
- Create the syslog FlexConnector configuration file

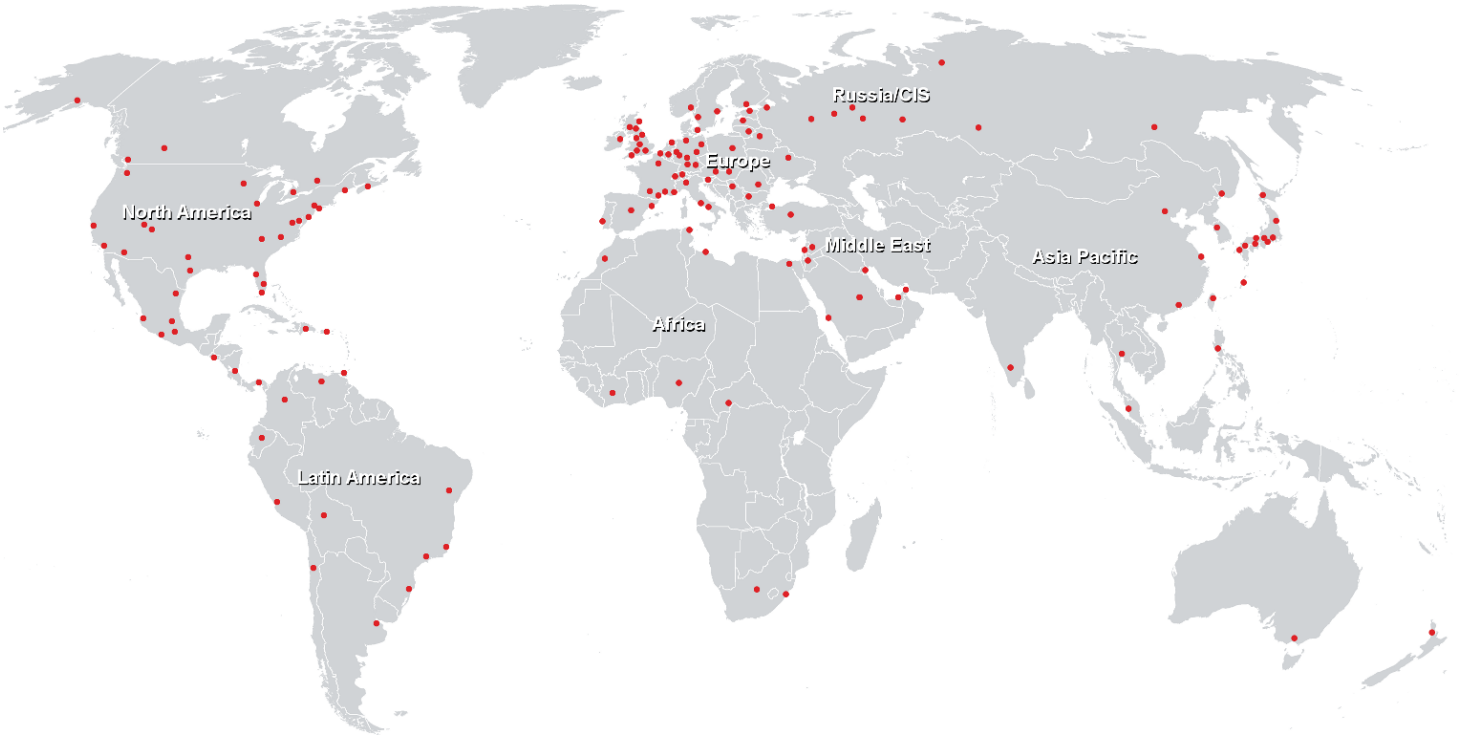
JSON Folder Follower Connector

- Identify the properties of basic JSON objects
- Define Token and Mappings declarations for a JSON Folder Follower FlexConnector
- Perform installation and testing of a JSON Folder Follower FlexConnector in console mode

Advanced Topics

- Describe the purposes of multi-line Regex configuration parameters:
    - Concatenate lines belonging to a single event
    - Identify the start and/or end of each event
- Describe parser linking when two or more FlexConnector types may be needed to parse the same data
- Define and create conditional mapping configurations
- Illustrate the LogFu tool which reads and parses ArcSight logs and generates interactive visual presentations of them

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