opentext™

Fast Lane

ArcSight 7.x FlexConnector Configuration (ASFC160-76)

ID ASFC160-76   **Price** 2,400.— €(excl. tax)   **Duration** 3 days

Important notes for the booking of Open Text trainings

Please note that prepayment is required for participation in an Open Text training course. Participation in a training course is possible for 12 months after booking the course. Cancellations are excluded. For further information, please refer to **our** General Terms and Conditions.

Who should attend

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.

Prerequisites

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

Course Content

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

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services
✓ High End Technology Training
✓ Business & Soft Skill Training
✓ Consulting Services
✓ Managed Training Services
✓ Digital Learning Solutions
✓ Content Development
✓ Remote Labs
✓ Talent Programs
✓ Event Management Services

Training Methods
✓ Classroom Training
✓ Instructor-Led Online Training
✓ FLEX Classroom – Classroom & Online Hybrid
✓ Onsite & Customized Training
✓ E-Learning
✓ Blended & Hybrid Learning
✓ Mobile Learning

Technologies & Solutions
✓ Digital Transformation
✓ Artificial Intelligence
✓ Cloud
✓ Networking
✓ Cyber Security
✓ Wireless & Mobility
✓ Modern Workplace
✓ Data Center

Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610

info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080

info@flane.ch / www.flane.ch