ArcSight 7.x FlexConnector Configuration (ASFC160-76)

ID ASFC160-76 **Preis** 2.400,– € (exkl. MwSt.) **Dauer** 3 Tage

Wichtige Hinweise für die Buchung von Open-Text-Trainings

Bitte beachten Sie, dass für die Teilnahme an einem Open-Text-Training Vorkasse zu leisten ist. Eine Teilnahme an einem Training ist für 12 Monate nach Kursbuchung möglich. Stornierungen sind ausgeschlossen. Weitere Informationen entnehmen Sie bitte **unseren** Allgemeinen Geschäftsbedingungen.

Zielgruppe

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.

Voraussetzungen

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

Kursinhalt

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<br />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

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

✓ Highend-Technologietraining
✓ Business- & Softskill-Training
✓ Consulting Services
✓ Managed Training Services
✓ Digitale Lernlösungen
✓ Content-Entwicklung
✓ Remote Labs
✓ Talentprogramme
✓ Eventmanagement-Services

Trainingsmethoden

✓ Klassenraumtraining
✓ Instructor-Led Online Training
✓ FLEX Classroom – Klassenraum und ILO kombiniert
✓ Onsite & Customized Training
✓ E-Learning
✓ Blended & Hybrid Learning
✓ Mobiles Lernen

Technologien und Lösungen

✓ Digitale Transformation
✓ Artificial Intelligence (AI)
✓ Cloud
✓ Networking
✓ Cyber Security
✓ Wireless & Mobility
✓ Modern Workplace
✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren
rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft,
Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als
19.000 Zertifizierungen

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

info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800

info@itls.at / www.itls.at

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

info@flane.ch / www.flane.ch