Training: Micro Focus
ASFC160 - ArcSight FlexConnector Configuration

TRAINING GOALS:

ArcSight FlexConnector Configuration provides you with an overview of the ArcSight SmartConnectors framework and explains the ArcSight ESM Schema. It teaches you how to construct and manipulate FlexConnector configuration and property files and use various parsing methods including fixed delimited, regular expressions, syslog, and JSON. Examples from standard connectors are used to illustrate device-specific methodologies. Advanced configuration options such as multi-line Regex, parser linking and conditional mapping are also covered.

Upon successful completion of this course, you should be able to:

- Install ArcSight Connector software, configure a functional FlexConnector, and test with an ESM Active Channel
- Use the FlexConnector Wizard to create fixed delimited configuration files
- Use the Regex Tester tool to create common and sub-message parsing and token-to-event mapping
- Create a tailored Categorization file for a parent FlexConnector and test its function in an active channel
- Navigate the connector configuration file hierarchy to locate, display and edit

Audience/Job Roles

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.

CONSPECT:

- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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
    - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

REQUIREMENTS:

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

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Micro Focus (course completion).

TRAINER:

Authorized Micro Focus Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007