

ArcSight FlexConnector Configuration Training will provide you with an overview of ArcSight connectors and explain the ESM Schema. Additionally attendees will learn how to configure the flex connector configuration files and understand the various parsing methods available including real examples from standard connectors. Parsing methods covered will include Fixed delimited, Regular Expressions, Database, and SNMP. Advanced configuration options such as multi-line REGEX, parser linking and conditional mapping will also be covered. You should have a good understanding of Regular Expressions to attend this course.

- **Introductions** *(30 Minutes)*  
*(Instructor Lead Presentation)*
- **Lesson I**  
**Introduction to ArcSight Connectors**  
*(Instructor Lead Presentation)*
  - What is an Arcsight SmartConnector?
  - SmartConnector Architecture
  - What is an Arcsight FlexConnector?
    - Types of FlexConnectors
  - Connector Installation
    - Common Installation Steps
    - Common Configuration Tasks
    - Selecting Connector Type
  - ArcSight Schema
    - Schema Groupings
- **Lesson II**  
**Creating the FlexConnector Configuration File**  
*(Instructor Lead Presentation and Hands On Activity)*
  - Configuration File Locations
  - Parser Configuration
  - Declaring Tokens
  - Event Mapping
  - Severity Mapping
  - Double Underscore Operators
  - FlexConnector Wizard
- **Lesson III**  
**Regular Expressions (REGEX) FlexConnectors**  
*(Instructor Lead Presentation and Hands On Activity)*
  - REGEX Configuration Tester
  - Regex Configuration File
    - Common Regex
    - Subparser Regex

- **Lesson IV**  
**Typical FlexConnector Configuration Files**  
*(Instructor Lead Presentation and Hands On Activity)*
  - Syslog FlexConnector
    - CISCO Aironet syslog configuration file
  - Time and ID based Database FlexConnector
    - Snort DB Configuration File
  - SNMP Configuration File
  
- **Lesson IV**  
**Advanced FlexConnector Parameters**  
*(Instructor Lead Presentation and Hands On Activity)*
  - Multi-Line Regex
  - Parser Linking
  - Conditional Mapping