ArcSight FlexConnector Configuration (ASFCC)

ID ASFCC **Preis** auf Anfrage **Dauer** 3 Tage

Zielgruppe

Sicherheitsadministratoren, Autoren/Architekten von Inhalten und IT-Integratoren, die benutzerdefinierte Konnektoren erstellen und installieren, um kritische Ereignisdaten-Feeds für ArcSight ESM oder Logger bereitzustellen, leitende Analysten für Netzwerke, Sicherheitssysteme, Unternehmensanwendungen und Datenbanken

Voraussetzungen

Um an diesem Kurs erfolgreich teilnehmen zu können, sollten Sie über die folgenden Voraussetzungen oder Kenntnisse verfügen:

- Erfolgreicher Abschluss des Kurses ArcSight ESM Admin und Analyst
- Erfolgreicher Abschluss des Kurses ArcSight ESM Advanced Administrator
- Kenntnisse über reguläre Ausdrücke

Kursziele

Nach Abschluss dieses Kurses sollten die Teilnehmer in der Lage sein:

- Installieren Sie die ArcSight Connector-Software, konfigurieren Sie einen funktionsfähigen FlexConnector und testen Sie mit einem ESM Active Channel
- Verwenden Sie den FlexConnector-Assistenten, um Konfigurationsdateien mit fester Trennlinie zu erstellen
- Verwenden Sie das Regex-Tester-Tool, um das Parsen von allgemeinen und Teilnachrichten sowie die Zuordnung von Token zu Ereignissen zu erstellen.
- Erstellen einer massgeschneiderten Kategorisierungsdatei für einen übergeordneten FlexConnector und Testen seiner Funktion in einem aktiven Channel
- Navigieren Sie in der Hierarchie der Konnektorkonfigurationsdateien, um die folgenden Dateien zu finden, anzuzeigen und zu bearbeiten

Kursinhalt

Modul 1: Einführung in FlexConnector

- Definieren Sie SmartConnectors und ihre Funktionen
- Verfolgen Sie den Einsatz der Geräte und die Verarbeitung des Ereignisflusses
- Beschreiben Sie die FlexConnectors-Typen
- Installieren Sie einen Stecker

Modul 2: Verwendung des ArcSight-Schemas

- Erfassen Sie vor der Entwicklung Ihres FlexConnectors die Anforderungen an die Veranstaltung
- Ereignisse normalisieren und zuordnen
- Sonderfälle differenzieren
- Liste der verschiedenen Schemagruppen

Modul 3: Grundlegende Konfigurationsdatei und Kategorisierung

- FlexConnector-Dateien lokalisieren
- Definieren Sie das Konfigurationsverfahren
- Wenden Sie die vier Schritte an, um eine FlexConnector-Konfigurationsdatei zu erstellen
  - Konfiguration des Parsers
  - Token-Erklärung
  - Ereignis-Zuordnung
  - Schweregradzuordnung
- Verwenden Sie den FlexConnector-Assistenten, um eine Konfigurationsdatei zu installieren
- Kategorisierung verwenden, um ein Ereignis zu profilieren
  - Es werden sechs Kriterien verwendet: Objekt, Verhalten, Ergebnis, Technik, Gerätegruppe und Signifikanz

Modul 4: Regex FlexConnectors

- Installieren Sie den Regex File Reader FlexConnector
- Gemeinsame Regex erstellen
- Define SubMessages
- Verwenden Sie den Regex-Tester Einführung in das Konzept der Teams

Modul 5: Installation von ESM Syslog Connectors mit benutzerdefinierten Parsern

- Identifizieren Sie die Syslog-Konnektoren
- Beschreiben Sie die syslog FlexConnector Komponenten

- Erstellen Sie die syslog FlexConnector-Konfigurationsdatei

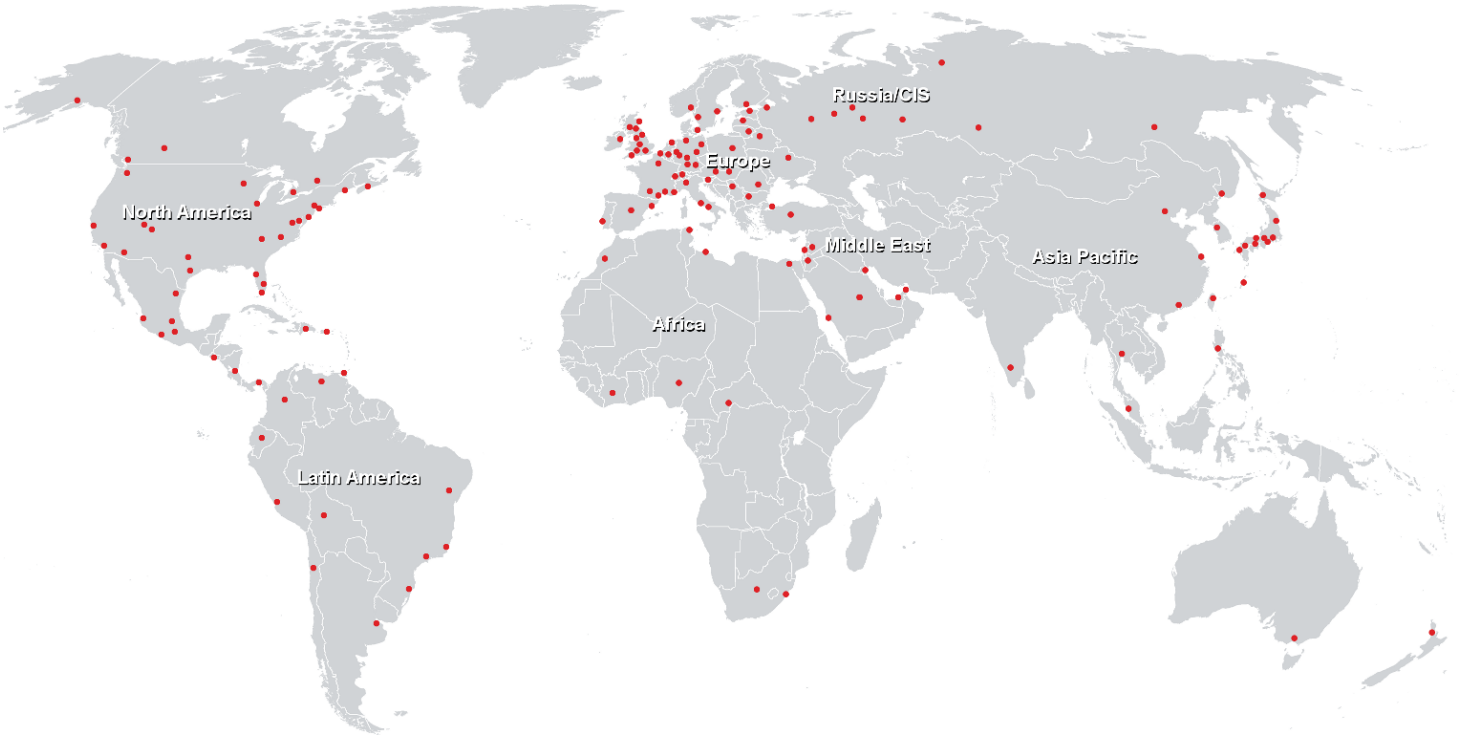
Modul 6: JSON Folder Follower Connector

- Die Eigenschaften der grundlegenden JSON-Objekte zu identifizieren
- Definieren Sie Token- und Mapping-Deklarationen für einen JSON Folder Follower FlexConnector
- Installation und Test eines JSON Folder Follower FlexConnector im Konsolenmodus durchführen

Modul 7: Fortgeschrittene Themen

- Beschreiben Sie den Zweck von mehrzeiligen Regex-Konfigurationsparametern:
  - Verketten von Zeilen, die zu einem einzigen Ereignis gehören
  - Identifizieren Sie den Beginn und/oder das Ende eines jeden Ereignisses
- Beschreibung der Parser-Verknüpfung, wenn zwei oder mehr FlexConnector-Typen benötigt werden, um dieselben Daten zu parsen
- Definieren und Erstellen von bedingten Mapping-Konfigurationen
- Veranschaulichung des LogFu-Tools, das ArcSight-Protokolle liest und analysiert und interaktive visuelle Darstellungen davon erzeugt

Weltweite Trainingscenter



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