ArcSight FlexConnector Configuration (ASFCC)

ID ASFCC **Preis** 2.250,– € (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.

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Dieser Kurs richtet sich an Sicherheitsadministratoren, Autoren/Architekten von Inhalten und IT-Integratoren, die benutzerdefinierte Konnektoren erstellen und installieren, um ArcSight ESM oder Logger mit wichtigen Ereignisdaten zu versorgen. Dazu können leitende Analysten für Netzwerke, Sicherheitssysteme, Unternehmensanwendungen und Datenbanken gehören.

Höhepunkte:

- ArcSight Connector-Software installieren
- Einen FlexConnector planen und konfigurieren

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

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