Installing and Configuring ArcSight Platform (ARC4300I)

ID ARC4300I **Price** 4,000.— €(excl. tax) **Duration** 5 days

Important notes for the booking of Open Text trainings

Please note that prepayment is required for participation in an Open Text training course. Participation in a training course is possible for 12 months after booking the course. Cancellations are excluded. For further information, please refer to **our** General Terms and Conditions.

Course Overview

This instructor-led course teaches you how to install and configure ArcSight Platform 23.2 on-premise with the ArcSight Platform Installation program.

Who should attend

This course is designed for Security Professionals and SOC Administrators, who are responsible for deploying and administrating the ArcSight Platform within their environment.

Prerequisites

To be successful in this course, you should have the following prerequisites or knowledge:

- ESM200 - ESM Administrator and Analyst or comparable ArcSight experience
- Experience working with command line tools
- Experience deploying applications in Windows and Linux environments
- Computer desktop, browser, and file system navigation skills
- Two Monitors to make it easy to review the guides on one screen, and the lab on the second screen

Course Objectives

On completion of this course, participants should be able to:

- Describe the ArcSight Platform and its Architecture
- Describe the system requirements
- Install ArcSight Platform
- Verify a successful installation
- Configure ArcSight Platform to ingest events
- Configure collectors and CTH with ArcMC
- Configure Topics and Routes
- Configure ESM and SOAR Integration
- Manage ArcSight Users
- Enable Single Sign-On
- Add features to an existing ArcSight installation

Course Content

- Architecture
- System Requirements
- YAML Files
- Installing ArcSight Platform
- Post-Install Activities
- Transformation Hub Management from Fusion ArcMC
- Producing Events and Transformation Hub Ingestion
- Collectors and CTH Deployment from ArcMC
- Topic and Route Management
- Integrating ESM and SOAR
- Enabling Single Sign-On
- Managing Users in ArcSight
- Adding More ArcSight Capabilities

Detailed Course Outline

Module 1: Architecture

- Describing the ArcSight Platform and its Architecture
- Describing the underlying CDF infrastructure
- Identifying the ArcSight Platform Capabilities
- Explaining other related components to the Platform
- Considerations and Best Practices

Module 2: System Requirements

- Describing the following:
  - System Requirements
  - Host Requirements
  - DNS requirements
  - NFS Requirements
  - ArcSight Database

Module 3: YAML Files

- Configuring the ArcSight Platform YAML Files

Module 4: Installing ArcSight Platform

- Pre-installing ArcSight
- Installing ArcSight

Module 5: Post-Install Activities

- Checking the status of the ArcSight Platform Installation
- Accessing and exploring the ITOM Management Portal
- Running the post-install command to finalize the deployment
- Uploading License Files under the ITOM Management Portal
- Logging into Fusion for the First Time

Module 6: Transformation Hub Management from Fusion ArcMC

- Validating a successful integration between Transformation Hub and the new containerized ArcMC available in Fusion
- Retrieving the master root certificate

Module 7: Producing Events and Transformation Hub Ingestion

- Recognizing and describing how events are produced
- Describing event formats: classic (CEF) and AVRO
- Installing a CEF Producer and AVRO Producer of events
- Detailed walkthrough of the configuration steps and all parameters
- Sending Test Alerts Replay Events to Transformation Hub
- Validating Topics and Transformation Hub Ingestion

Module 8: Collectors and CTH Deployment from ArcMC

- Defining the difference between a Collector and Connector
- Listing the advantages of using Collectors
- Describing what's needed to perform a Collector Deployment using ArcMC
- Deploying CTH from ArcMC and route events from th-syslog to other topics

Module 9: Topic and Route Management

- Managing Topic and Routes
- Local vs Global Event Enrichment
- Types of Stream Processor Instances in Transformation Hub
- Configuring Topics and Routes – Step by Step Example for Global Event Enrichment

Module 10: Integrating ESM and SOAR

- Configuring the ESM and SOAR Integration
- Verifying a Successful Integration

Module 11: Enabling Single Sign-On

- Configuring the ESM Admin User for Single Sign-on
- Enabling Single Sign-on

Module 12: Managing Users in ArcSight

- Managing ArcSight Users Overview
- Managing ESM Users
- Managing Fusion Users
- Managing SOAR Users
- Defining Recon User Permissions and Roles
- Defining Intelligence User Permissions and Roles

Module 13: Adding More ArcSight Capabilities

- Describing the benefits of adding more ArcSight capabilities
- Adding more ArcSight capabilities
- Specify mandatory filtering on pre-defined fields or user-specified fields
- Create lookup values for field attributes
- Create and use parameters and parameter groups

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch