ArcSight Enterprise Security Manager Administration (AESMA)

ID AESMA **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 course covers how to plan and install ArcSight Enterprise Security Manager (ESM) in Compact and Distributed Mode. You will also learn how to install and configure SmartConnectors, Forwarding Connectors, Syslog Connectors, customize ESM and the Console, configure Storage Groups, backup and restore ESM, manage certificates, manage users, and access Administrator reports and dashboards.

Highlights:

- Installing ArcSight ESM
- Installing Connectors
- Managing ArcSight ESM

Who should attend

This course is for Administrators who install, maintain, and troubleshoot ESM components

- Design and implement integrations between ArcSight ESM and other ArcSight products
- Proactively investigate the health of the ESM CORRE environment.

Prerequisites

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

- Knowledge of ESM Concepts
- (Minimum) 6 Months ArcSight Administration Experience
- Database SQL statements experience
- Linux Administration experience
- Successful Completion of ArcSight ESM Administrator & Analyst Course or Equivalent Experience

Course Objectives

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

- Identify the ESM communication strategy used between the various devices and components within an ESM Network
- Define each ESM operation modes and components, Compact and Distributed, and the issues ESM Distributed Mode comes to solve
- Plan, install, and run ESM in Distributed Mode
- Identify functions and navigate the Command Center UI
- Install and customize the ESM console
- Install and configure ArcSight SmartConnectors
- Install and configure a Forwarding Connector
- Setup Notifications
- Import Zone and Asset information with the Network Model wizard
- Customize ArcSight ESM using the properties files
- Describe and install ArcSight upgrades and patches
- Create Users and define User Permissions
- Review Administrator Reports, Dashboards and Filters
- Configure and manage storage groups
- Describe CORRE daily job archives
- Recognize how to Back up and restore ESM
- Describe and deploy uses of SSL technology in ArcSight ESM

Course Content

- Introduction to ESM Administration
- ESM Distributed Components
- Installing ESM Distributed Mode
- Maintaining ESM Properties Files and Upgrades
- Installing the ESM Console
- Installing SmartConnectors
- Managing the Network Model
- Configuring SmartConnector Destinations
- Installing the ESM Super and Syslog Connectors
- SmartConnectors Configurations and Advanced Features

- Command Center
- Accessing Administrator Content
- Content Management and Peering
- ESM User Administration and Notification
- ESM Certification Management
- ESM Backup and Restore

Detailed Course Outline

Module 1: Introduction to ESM Administration

- Describe each ESM system component

Module 2: ESM Distributed Components

- Recognize where ESM fits within the ArcSight Architecture
- Define each ESM operation modes, Compact and Distributed, and the issues ESM Distributed Mode comes to solve
- Describe the ESM Distributed Mode components
- Recognize the ArcSight Data Platform (ADP) and its components

Module 3: Installing ESM Distributed Mode

- Plan System Hardware Requirements
- Check Operating System Pre-Installation
- Install ESM Persistor Node
- Install ESM Correlator Aggregator Node
- Configure Integration of the Persistor Node
- Add Correlator Aggregator Services
- Configure Message Bus Data and Control Instances from Persistor
- Configure Repository Instances from Persistor
- Configure Distributed Cache on Correlator Aggregators
- Run Cert Admin Approveall
- Start All Cluster Wide Services from Persistor Node

Module 4: Maintaining ESM Properties Files and Upgrades

- Customize ArcSight ESM using Properties File
- Prepare System for an Upgrade
- Upgrade ESM
- Upgrade the ESM Console

Module 5: Installing the ESM Console

- Install the ESM Console
- Customize the ESM Console
- Describe Tools available in the ESM Console

Module 6: Installing SmartConnectors

- Describe how Connectors collect, normalize, and cache events
- Install and configure ArcSight SmartConnectors
- Identify Connector Command Scripts
- Describe how Connectors can be managed from an ESM Console, a Connector Appliance, or ArcSight Management Center

Module 7: Managing the Network Model

- List Network Model resources
- Describe Asset Model resources
- Add the following modelling resources:
- Assets
- Asset Ranges
- Zones
- Network and attach it to a connector
- Import Zone and Asset information with the Network Model wizard
- Explain the use of the Asset Import Connector

Module 8: Configuring SmartConnector Destinations

- Get SmartConnector Status
- Set SmartConnector Flow-Control
- Use SmartConnector Administrative Dashboards
- Configure SmartConnectors for Failover and Dual Destinations

Module 9: Installing the ESM Super and Syslog Connectors

- Installing and configure a Forwarding Connector
- Installing and configure a Syslog connector

Module 10: SmartConnectors Configurations and Advanced Features

- Configuring SmartConnectors using advanced features such as turbo mode, map files, event filtering, network options and event aggregation
- Constructing advanced configuration settings for optimal performance and data enrichment

Module 11: Command Center

- Logging onto the ArcSight Command Center
- Identifying functions and navigate the User Interface
- Using the ArcSight Command Center Help Facility
- Configure:
- Authentication
- Content
- Storage
- Appliances
- Identifying stock content dashboards

Module 12: Accessing Administrator Content

- Reviewing Administrator Reports, Dashboards and Filters
- Running and Archiving Reports
- Using Administrator Data Monitors

Module 13: Content Management and Peering

- Peering ESMS
- Performing Peer Searches
- Creating Packages and Pushing content to a Peer

Module 14: ESM User Administration and Notification

- Creating Users and setting User Notifications
- Managing Resource Permissions
- Accessing and Modifying Password Properties
- Configuring ArcSight Notifications

Module 15: ESM Certification Management

- Describing uses of SSL technology in ArcSight ESM
- Describing SSL setup options
- Keytool/keytoolgui
- Certadmin
- Identifying the steps to deploy:
- Self-signed Certificates
- Approve/revoke distributed mode Certificates
- CA (Certificate Authority)-signed Certificates

Module 16: ESM Backup and Restore

- Restoring the ESM Manager’s configurations
- Backing up and restoring ESM
- Describing CORR-E Daily Job Archiving

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