# Installing and Configuring ArcSight Platform (ARC4300I)

**ID** ARC4300I **Preis** 4.000,– € (exkl. MwSt.) **Dauer** 5 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.

## Kursüberblick

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

## Zielgruppe

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

## Voraussetzungen

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

## Kursziele

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

## Kursinhalt

- 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

## Detaillierter Kursinhalt

### 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

# 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