ArcSight ESM Administrator and Analyst (ASEAAA)

ID ASEAAA **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

In this introductory course you learn how to use the ArcSight console and ArcSight Command Center to monitor security events, configure ESM, manage users, and manage ESM network intelligence resources. You will also be introduced to triaging and resolving cases with ArcSight SOAR.

Highlights:

- Investigate security events
- Configure security content
- Investigate, identify, analyze, and remediate exposed security issues
- Use workflow management to provide real-time incident response and escalation tracking
- Modify and run standard reports to provide situational awareness and network status
- Establish ESM peering across multiple ESM instances
- Perform distributed event search and content management

Zielgruppe

Analysts, Content Engineers, Business Administrators

Voraussetzungen

None

Kursziele

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

- Make ArcSight ESM operational upon initial installation
- Describe how ESM works in the context of your network
- Create user accounts
- Implement built-in content
- Populate ESM with your network and assets to identify endpoints involved in an event
- Create site-specific business-oriented views

Kursinhalt

Module 1: ESM Overview

- Discuss what ArcSight ESM is and how it fits into a SOC
- List the problems ESM can solve
- Discuss basic processes to make an ESM installation successful
- Describe the basic ArcSight components (10' - 100,000' view)
- Identify basic user roles within an ArcSight Installation

Module 2: Command Center

- Discuss an overview of the Command Center
- Describe how to use the Site Map
- Describe how to monitor usage
- Discuss how to configure Dashboards and the different Dashlets you can add
- Describe how to use the Security Operations Center Dashboards
- Explain how to configure and view MITRE Dashboards
- Discuss how to monitor events with Active Channels
- Discuss how to view and use Field Sets
- Discuss how to view, export, and filter Active Lists

Module 3: ESM Console

- Install the ArcSight ESM Console
- Start the ArcSight ESM Console
- Use the Console Panels and Features
- Customize the ESM console

Module 4: Installing and Configuring ArcSight Connectors

- Describe a connector
- Describe normalization
- Describe a network model
- Describe SmartConnectors
- Deploy and configure SmartConnectors

Module 5: ArcSight Marketplace

- Describe what is the Marketplace
- Define Marketplace packages/use cases

Module 6: Schema, Fieldsets, and Active Channels

- Describe the ArcSight Event Schema
- Describe an Active Channel
- Describe what a field set is
- Describe the Event Life Cycle

Module 7: Filters

- Describe Filters and Filter Types
- Create and Modify Filters
- Debug Filters

Module 8: Dashboards & Data Monitors

- Identify Data Monitor types and functions
- Access and Use Dashboards
- Modify Dashboard Data Monitor Layouts

Module 9: Rules & Lists

- Describe rules and rule types
- Describe rule triggers and actions
- Describe Active Lists and Session Lists
- Create and validate rule behavior
- Create and validate Brute Force Login Attempt and Successful rules
- Create and validate Active and Session List integration rules

Module 10: User Administration

- Create, edit, rename, delete user groups
- Create, edit, move, delete users
- Manage resource permissions
- Access and modify global user password properties

Module 11: Notifications

- Describe the operation of ArcSight notifications
- Configure ArcSight notifications

Module 12: Incident Response and Automation with SOAR

- Understand SOAR
- Triage cases with SOAR
- Respond to Cases with Playbooks
- Close a case

Module 13: Queries and Query Viewers

- Explain Queries
- Define Query Viewers
- Explain the advantages of using Query Viewers
- Create the following functions with Query Viewers: Drilldowns, Baselines, Reports, Dashboard views

Module 14: Reports

- Define a report
- Run, view, and save a report
- Manage archived reports

Module 15: Content Management and Peering

- Peer ESMs
- Perform a search on a peer
- Create a package and sync to a peer
- Manually push a package
- Verify successful distribution of a package

Module 16: Event Search

- how keyword, field-based and pipeline searches are performed
- Describe how search results are displayed
- Use the unified Search page to initiate any type of search
- Use Search Helper and Search Builder features to save time constructing search expressions
- Load, modify, and save search filters and saved searches
- Enable peer ESM and Logger instances for searching

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