ArcSight-ESM-Advanced Analyst with Certified Expert Exam (ESM320-76)

ID ESM320-76 **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 provides you with the knowledge required to use advanced ArcSight ESM content to find and correlate event information, perform actions such as notifying stakeholders, graphically analyze event data, and report on security incidents. You will familiarize and/or reinforce your understanding of the advanced correlation capabilities within ArcSight ESM that provide a significant edge in detecting active attacks.

This course covers ArcSight security problem solving methodology using advanced ESM content to find, track, and re-mediate security incidents. During the training, you will use variables and correlation activities, customize report templates for dynamic content, and customize Dashboards to monitor incidents.

The last day of class offers a hands-on exam. Passing the exam awards you with Certified Expert badge.

Who should attend

This course is intended for analysts responsible for:

- Defining their organization's security objectives
- Building or using advanced content to correlate, view and respond to those security objectives.
-

Prerequisites

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

- Common security devices such as IDS and firewalls
- Common network device functions, such as routers, switches, and hubs
- TCP/IP functions such as CIDR blocks, subnets, addressing, and communications
- Basic Windows operating system tasks and functions
- Possible attack activities, such as scans, man in the middle, sniffing, DoS, and possible abnormal activities, such as worms, Trojans, and viruses
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, and safeguards
- Completed the ArcSight ESM Administrator and Analyst course or 6 months experience administering ArcSight ESM

Course Objectives

Upon successful completion of this course, you should be able to:

- Navigate ArcSight ESM console and command center to correlate, investigate, analyze and remediate both exposed and obscure threats
- Construct ArcSight variables to provide advanced analysis of the event stream
- Develop ArcSight lists and rules to allow advanced correlation activities
- Optimize event-based data monitors to provide real-time viewing of event traffic and anomalies
- Design new report templates and create functional reports
- Find events through the search tools

Course Content

- Module 1: ESM Overview
- Module 2: Command Center
- Module 3: ArcSight Console
- Module 4: Active Channels
- Module 5: Filters
- Module 6: Variable Customization

- Module 7: Data Monitors and Dashbords
- Module 8: ESM Lists
- Module 9: ESM Rules
- Module 10: Query Viewers Authoring
- Module 11: ESM Reports
- Module 12: Unified Event Search Tools

Detailed Course Outline

Module 1: ESM Overview

- Identify ESM Architecture
- Describe the content of the ArcSight Event Schema
- List the phases of the ArcSight Event Lifecycle
- Describe the event processing and schema population performed during each phase of the event lifecycle
- List the resources and tools applicable to specific phases of the event lifecycle

Module 2: Command Center

- Access the ArcSight ESM Command Center
- Monitor Usage Metrics
- View System Metrics
- Use the SOC/MITRE Dashboards
- Access and use Active Lists
- Utilize Field Sets

Module 3: ArcSight Console

- Launch the ArcSight Console
- Identify toolbar components and their functions
- List the different views available in the Viewer panel
- Identify three methods to access Console Help
- Describe the Reference Resources and their characteristics
- Identify ESM Console preference options
- Customize your ESM Console

Module 4: Active Channels

- Create a new Active Channel
- View the details of an event
- Identify Dynamic and Static Active Channels

Module 5: Filters

- Describe Filter types and usage
- Add, edit and save Filters to an Active Channel
- Define the Common Conditions Editor

Module 6: Variable Customization

- Describe functions available in Variables
- Create both Local and Global Variables
- Promote Local to Global Variables
- Share Global Variables among multiple resources

Module 7: Data Monitors and Dashbords

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

Module 8: ESM Lists

- Describe the differences between Active and Session Lists
- Create and validate Active and Session List integration Rules

Module 9: ESM Rules

- Create and validate the following:
- Rule behavior
- Brute Force Login Attempt and Successful rules
- Light Weight rules and Pre-Persistent rules

Module 10: Query Viewers Authoring

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

Module 11: ESM Reports

- List the components in the Report Workflow
- List the different types of Reports
- Run a Report from the Navigator panel
- View an Archive Report from the Navigator panel
- Set up a scheduled Report job
- Build a custom Report
- Build a custom Trend Report

Module 12: Unified Event Search Tools

- Describe 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

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