Configuring ArcSight SOAR for Effective Threat Response (CASFETR)

ID CASFETR **Price** 2,400.— €(excl. tax) **Duration** 3 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 configure ArcSight SOAR 3.8. You will learn how to configure SOAR to receive ESM alerts, integrate with other products to enrich cases, and create workflow playbooks, in addition to configuring other features of the product.

The course uses lectures and a series of hands-on labs to teach the course material. The hands-on labs for this course use version 3.8 of the SOAR software.

Highlights:

- Overview of ArcSight SOAR
- Configuring SOAR to receive ESM alerts
- Configuring integrations
- Creating workflow playbooks
- Running reports"

Who should attend

Administrators and Content Engineers responsible for configuring ArcSight security content.

Prerequisites

This course assumes a familiarity working with ArcSight ESM but it is not required

Course Objectives

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

- Configure SOAR to receive alerts from ESM
- Describe the SOAR workflow
- Configure integrations
- Configure filtering, classifying, consolidating
- and dispatching rules
- Create workflow playbooks
- Review system status
- Run, schedule, and export reports

Course Content

Module 1: Introduction to ArcSight SOAR

- Challenges Faced by Organizations
- What Is ArcSight SOAR?
- ArcSight SOAR Features.
- Deployment Overview of ArcSight SOAR.
- Accessing ArcSight SOAR

Module 2: Setting Up SOAR to Receive Alerts

- Installing a Forwarding Connector on ESM
- Configuring a Forwarding Connector User and Web User on ESM
- Configuring a Pre-persistent Rule to Tag the Events Forwarded to SOAR
- Adding an ESM Alert Source on SOAR
- Adding an ESM Integration on SOAR

Module 3: Understanding the SOAR Workflow

- Processing ESM Alerts with SOAR
- Rule Name Filters
- Classification
- Consolidation
- Dispatching Cases
- Automating Case Handling by Using Playbooks

Module 4: SOAR Integrations Overview

- SOAR Integrations Capabilities
- Use Cases Benefits
- Integrating SOAR with MISP
- Integrating SOAR with VirusTotal

Module 5: SOAR Users, Groups, SSO

- Creating User Groups in Fusion
- Creating Users in Fusion
- Importing Existing Users from ESM
- User Roles and Assigning Permissions
- ACLs in SOAR

Module 6: SOAR Case Management

- Understanding the SOAR Cases User Interface
- Viewing Case Details
- Managing Cases in SOAR

Module 7: Filtering, Classifying, Consolidating, and Dispatching Cases

- Filtering Alerts for Case Creation
- Classifying Cases on SOAR
- Consolidating Alerts to Create Cases
- Dispatching Cases

Module 8: Automating Responses with Workflow Playbooks

- What are Playbooks?
- Working with Playbooks
- Workflow Playbooks
- Scheduled Playbooks
- Managing Triggers
- Handling Manual Processes Through Tasks
- Out of The Box Workflows
-

Module 9: SOAR System Status

- Alerts
- Action and Rollback Queues
- Action History
- Enrichment History
- Process Queues
- Troubleshooting

Module 10: Monitoring Using SOAR Dashboards and Reports

- Reports in Fusion
- ArcSight SOAR Standard Content Resources
- Scheduling and Exporting Reports
- Running SOAR Legacy Reports (Jasper Reports)

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