Configuring ArcSight SOAR for Effective Threat Response (CASFETR)

ID CASFETR **Preis** 2.250,– € (exkl. MwSt.) **Dauer** 3 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 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"

Zielgruppe

Administrators and Content Engineers responsible for configuring ArcSight security content.

Voraussetzungen

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

Kursziele

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

Kursinhalt

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)

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