ArcSight Recon Analyst (2-7329)

ID 2-7329 **Preis** 3.200,– € (exkl. MwSt.) **Dauer** 4 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 course offers a comprehensive, hands-on introduction to ArcSight Recon for security analysts and threat hunters. It focuses on event search and reporting capabilities, hunting threats, and outlier detection.

Zielgruppe

This course is ideal for security analysts who want to enhance their threat detection and investigation capabilities by leveraging ArcSight Recon's event search, reporting, and dashboarding features to identify anomalies, uncover threats, and support proactive security operations.

Voraussetzungen

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

- Familiar with Boolean logic operators and ArcSight Schema groups and fields.
- Basic understanding of Command Shell in Windows and Linux, and familiarity with SIEM concepts

Kursziele

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

- Investigate events using Recon Search tools and Scheduled event searches.
- Explain the usage of Search resources such as Field Sets, Filters, and Operators.
- Describe, access, create and use Reports and Dashboards.
- Describe and use the default Cloud Security Dashboards and Reports.
- Implement Dashboards with Parabox Charts (known as parallel box plots charts).
- Describe and use the default MITRE ATT&CK Dashboards and Reports.
- Describe Threat Hunting types: unstructured and structured
- Create custom Search Queries, Reports and Dashboards to analyze event data using sample scenarios.
- Define Outliers Models and identify suspicious sources using Recon Analytics charts.

Kursinhalt

As a learner, you will begin by exploring event search and reporting features using Recon's default content to get familiar with the interface and its core functionalities. As the course progresses, you will engage in hands-on exercises to build more advanced event searches, reports, and dashboards from the ground up.

You will also analyze security events tied to specific use cases, such as detecting threats from former employees, investigating the Log4j vulnerability, and uncovering insider threats related to data exfiltration. By applying your knowledge of Recon, you will examine these scenarios to identify targets, indicators of compromise (IoCs), and potential attackers.

Highlights:

- Create search queries using ArcSight schema fields, keywords, field sets, search operators, and hashtags.
- Use default content reports and dashboards to analyze events of interest, including MITRE ATT&CK content.
- Create reports and dashboards using data worksheets from scratch.
- Analyze event data using Recon tools in sample scenarios, such as uncovering ex-employee threats and detecting Log4j vulnerability.

- Use Recon tools to analyze historical events and identify undetected threats in a sample unstructured threat-hunting scenario.
- Build and score the outlier model and explain outlier's analytics charts.

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