ArcSight Recon Analyst (2-7329)

ID 2-7329 **Price** 3,200.— €(excl. tax) **Duration** 4 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 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.

Who should attend

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.

Prerequisites

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

Course Objectives

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.

Course Content

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.

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