Advanced Analytics (FORT-ADVANALYTICS)

ID FORT-ADVANALYTICS **Price** 2,900.— €(excl. tax) **Duration** 3 days

This training is provided by our partner Fortinet.

Important notes for the booking of trainings directly provided by Fortinet

If you are unable to attend the training date you have booked (e.g. illness, etc.) or if Fortinet cancels the course, a credit note is not possible under any circumstances. In both cases of cancellation, the validity of your credit remains for 12 months after the order.

For more information, please refer to the **Fortinet Terms and Conditions**.

Course Overview

In this course, you will learn how to use FortiSIEM in a multi-tenant environment. You will learn about rules and their architecture, how incidents are generated, how baseline calculations are performed, the different methods of remediation available, and how the MITRE ATT&CK framework integrates with FortiSIEM. You will also learn how to integrate FortiSOAR with FortiSIEM.

Certification - This course is intended to help you prepare for the Fortinet NSE 7 - Advanced Analytics 6.7 certification exam. This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track.

Who should attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiSIEM and FortiSOAR devices in an enterprise or service provider deployment used to monitor and secure the networks of customer organizations.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- FortiGate Security (FORT-SECI)
- FortiGate Infrastructure (FORT-SECII)
- FortiSIEM Analyst (FORT-SIEM)

It is also highly recommended that you have an understanding of the following topics, or equivalent experience:

- Python programming
- Jinja2 template language for Python
- Linux systems
- SOAR technologies

Course Objectives

After completing this course, candidates will be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deployment
- Deploy FortiSIEM in a hybrid environment with and without collectors
- Design multi-tenant solutions with FortiSIEM
- Deploy collectors in a multi-tenant environment
- Manage EPS assignment and restrictions on FortiSIEM
- Manage resource utilization of a multi-tenant FortiSIEM cluster
- Maintain and troubleshoot a collector installation
- Deploy and manage Windows and Linux agents
- Create rules by evaluating security events
- Define actions for a single pattern security rule
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Deploy FortiSIEM UEBA agents
- Examine log-based UEBA rules
- Examine nested queries for advanced analytics
- Configure lookup tables for advanced analytics
- Configure clear conditions on FortiSIEM
- Analyze some out-of-the-box remediation scripts
- Configure various remediation methods on FortiSIEM
- Integrate FortiSOAR with FortiSIEM
- Remediate incidents from FortiSOAR

Detailed Course Outline

- Introduction to Multi-tenancy
- Defining FortiSIEM Collectors and FortiSOAR Connectors
- Operating Collectors
- Windows and Linux Agents
- Rules
- Single Subpattern Security Rule
- Multiple Subpattern Rules
- Baselines
- Baseline Rules
- FortiSIEM UEBA
- Nested Queries and Lookup Tables
- Clear Conditions
- Remediation

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