Advanced Analytics

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 nested queries and lookup tables work for advanced analytics using FortiSIEM. You will also learn how to integrate FortiSOAR with FortiSIEM.

Product Version

- FortiSIEM 6.7.4
- FortiSOAR 7.3.2
- FortiGate 7.2.2

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 9 hours
- Total course duration (estimated): 19 hours
  - 3 full days or 5 half days

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—that are used to monitor and secure the networks of customer organizations should attend this course.

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.

Prerequisites

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

- *FCP - FortiGate Security*
- *FCP - FortiGate Infrastructure*
- *FCP - FortiSIEM*

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

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

Agenda

1. Introduction to Multi-Tenancy
2. Defining FortiSIEM Collectors and FortiSOAR Connectors
3. Operating Collectors
4. Windows and Linux Agents
5. Rules
6. Single Subpattern Security Rules
7. Multiple Subpattern Rules
8. Baselines
9. Baseline Rules
10. FortiSIEM UEBA
11. Nested Queries and Lookup Tables
12. Clear Conditions
13. Remediation

Objectives

After completing this course, you should be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deploymen
- 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

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-ADA

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using a purchase order (PO) through Fortinet Resellers or Authorized Training Partners.

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-ADA-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)2

- CPE training hours: 10
- CPE lab hours: 9
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.