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.

Product Version

- FortiSIEM 6.3.0
- FortiSOAR 7.0.1
- FortiGate 7.0.1

Course Duration

- Lecture time (estimated): 13 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 20 hours / 3 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 used to monitor and secure the networks of customer organizations.

Certification

This course is intended to help participants prepare for the NSE 7 Advanced Analytics certification exam.

Prerequisites

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

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure
- NSE 5 FortiSIEM
It is also highly recommended that you have an understanding, or equivalent experience with, Python programming, Jinja2 template language for Python, Linux systems, and SOAR technologies.

**Agenda**

1. Introduction to Multi-Tenancy
2. Defining Collectors and Agents
3. Operating Collectors
4. Windows and Linux Agents
5. Rules
7. Multiple Subpattern Rules
8. Introduction to Baseline
9. Baseline
10. UEBA
11. MITRE ATT&CK
12. Clear Conditions
13. Remediation

**Objectives**

After completing this course, you should 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 the incident attributes that trigger an incident
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Examine the MITRE ATT&CK framework integration on FortiSIEM and FortiSOAR
- Deploy FortiSIEM UEBA agents
- Examine UEBA rules, reports, event types, and windows template

- 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 NSE 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: 13
- CPE lab hours: 7
- 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.