NSE Certification Program

Exam Description

Advanced Analytics

Certification

This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track. This certification validates your ability to design, administer, monitor, and troubleshoot Fortinet security operations solutions.

Visit the Cybersecurity Certification page for information about certification requirements.

Exam

The *Fortinet NSE 7 - Advanced Analytics 6.3* exam evaluates your knowledge of, and expertise with, FortiSIEM and FortiSOAR devices in SOC or MSSP environments.

The exam tests applied knowledge of FortiSIEM configuration, and operation, and includes operational scenarios, incident analysis, integration with FortiSOAR, and troubleshooting scenarios.

Once you pass the exam, you will receive the following exam badge:

Audience

The *Fortinet NSE 7 - Advanced Analytics 6.3* exam is intended for network and security professionals responsible for the management, configuration, administration, monitoring of FortiSIEM devices and integration of FortiSOAR and FortiSIEM in an enterprise or service provider deployment used to monitor and secure the networks of a customer's organization.

Exam Details

Exam name	Fortinet NSE 7 - Advanced Analytics 6.3
Exam series	NSE7_ADA-6.3
Time allowed	60 minutes
Exam questions	35 multiple-choice questions
Scoring	Pass or fail. A score report is available from your Pearson VUE account
Language	English
Product version	FortiSIEM 6.3.0, FortiSOAR 7.0.1, FortiOS 7.0.1

Exam Topics

Successful candidates have applied knowledge and skills in the following areas and tasks:

- Multi-Tenancy SOC Solution for MSSP
  - Describe multi-tenancy solutions for SOC environment
  - Define and deploy collectors and agents
  - Install and manage FortiSIEM Windows and Linux agents
- FortiSIEM Rules
  - Explain FortiSIEM rule processing
  - Construct FortiSIEM rules
  - Explain the MITRE ATT&CK® framework
- FortiSIEM Baseline and UEBA
  - Explain FortiSIEM baseline and profile reports
  - Construct FortiSIEM baseline rules
  - Configure UEBA on FortiSIEM
- Clear Conditions and Remediation
  - Remediate incidents on FortiSIEM manually and automatically
  - Remediate incidents using FortiSOAR

Training Resources

The following resources are recommended for attaining the knowledge and skills that are covered on the exam. The recommended training is available as a foundation for exam preparation. In addition to training, you are strongly encouraged to have hands-on experience with the exam topics and objectives.

- *FCSS - Advanced Analytics 6.3* course and hands-on labs
- *FCP - FortiSIEM 6.3* course and hands-on labs
- *FortiSIEM Parser 6.3* course and hands-on labs
- *FortiSIEM 6.3—User Guide*
- *FortiSOAR 7.0—Administration Guide*

Experience

Hands-on experience with the deployment, administration, and troubleshooting of FortiSIEM and FortiSOAR devices in MSSP or SOC environments. Hands-on experience with integrating FortiSIEM and FortiSOAR with various Fortinet and third-party products.

Exam Sample Questions

A set of sample questions is available from the Fortinet Training Institute. These questions represent the exam content in question type and content scope. However, the questions do not necessarily represent all the exam content, nor are they intended to assess your readiness to take the certification exam.

See the Fortinet Training Institute for the course that includes the sample questions.

Examination Policies and Procedures

The Fortinet Training Institute recommends that you review the exam policies and procedures before you register for the exam. Access important information on the Fortinet Training Institute Policies page, and find answers to common questions on the FAQ page.

Questions?

If you have more questions about the NSE Certification Program, contact us through the Fortinet Training Institute Helpdesk page.