NSE Certification Program

Exam Description

Security Operations Analyst

Certification

This exam is part of the Fortinet Certified Solution Specialist - Security Operations certification track. This certification validates your ability to design, administer, monitor, and troubleshoot Fortinet security operations solutions. This curriculum covers security operations infrastructures using advanced Fortinet solutions.

Visit the Cybersecurity Certification page for information about certification requirements.

Exam

The FCSS - *Security Operations 7.4 Analyst* exam evaluates your knowledge and skills in designing, deploying, and managing a Fortinet SOC solution using advanced FortiAnalyzer features and functions to detect, investigate, and respond to cyberthreats.

This exam tests your knowledge and skills related to configuring FortiAnalyzer SOC features and functions, various FortiAnalyzer deployment architectures, incident handling and analysis, and automation.

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

Audience

The FCSS - *Security Operations 7.4 Analyst* exam is intended for security professionals involved in the architectural design, implementation, and monitoring of Fortinet SOC solutions based on FortiAnalyzer.

Exam Details

Exam name	FCSS - *Security Operations 7.4 Analyst*
Exam series	FCSS_SOC_AN-7.4
Time allowed	65 minutes
Exam questions	32 multiple-choice questions
Scoring	Pass or fail. A score report is available from your Pearson VUE account.
Language	English
Product version	FortiAnalyzer 7.4, FortiOS 7.4

Exam Topics

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

- SOC concepts and adversary behavior
  - Analyze security incidents and identify adversary behaviors
  - Map adversary behaviors to MITRE ATT&CK tactics and techniques
  - Identify components of the Fortinet SOC solution
- Architecture and detection capabilities
  - Configure and manage collectors and analyzers
  - Design stable and efficient FortiAnalyzer deployments
  - Design, configure, and manage FortiAnalyzer Fabric deployments
- SOC operation
  - Configure and manage event handlers
  - Analyze and manage events and incidents
  - Analyze threat hunting information feeds
  - Manage outbreak alert handlers and reports
- SOC automation
  - Configure playbook triggers and tasks
  - Configure and manage connectors
  - Manage playbook templates
  - Monitor playbooks

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 - *Security Operations 7.4 Analyst* course and hands-on labs
- *FortiAnalyzer 7.4—Administration Guide*
- *FortiAnalyzer 7.4—Fabric Deployment Guide*
- *FortiAnalyzer 7.4—Examples Guide*
- *FortiAnalyzer—Playbook Variables Guide*
- *FortiAnalyzer—Architecture Guide*

Experience

- 1 year of experience with network security
- 6 months of experience working in SOC

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.