FORTINET
Premier Authorized Training Center

NSE 6 CERTIFIED
SECURITY OPERATIONS
FORTINET

fast lane

FortiSOAR Analyst

Course Description

In this course, you will learn how FortiSOAR helps organizations orchestrate and automate security operations, integrate security and network tools, and collaborate during incident handling. You will design playbooks that route decisions based on input data, automate enrichment and response actions, and support malicious indicator handling.

Course Duration:

3 Days

Prerequisites:

You must have an understanding of the topics covered in the *FortiOS Administrator* course (or have equivalent experience).

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

- *FortiManager Administrator*
- *FortiSOAR Administrator*
- Basic familiarity with Python programming
- Basic familiarity with the Jinja2 templating language
- Basic familiarity with email security and SIEM technology

Outlines:

1. Introduction to FortiSOAR
2. SOC Playbook Development
3. Jinja, Dynamic Variables, and Dynamic Values
4. Application Editor
5. Templates, Dashboards, and Widgets
6. Controlling Playbook Logic
7. Querying and Transforming Data
8. Incident Handling and FortiSOAR
9. Troubleshooting Playbooks and Connectors
10. Working With APIs

Objectives:

After completing this course, you will be able to:

- Describe SOAR, SIEM, automation, and orchestration
- Describe modules, deployment models, and FortiSOAR device types
- Navigate the FortiSOAR GUI
- Customize navigation with the navigation editor
- Describe the SOAR Framework solution pack
- Describe templates, dashboards, and reports
- Describe security management, role-based access, and teams
- Describe FortiSOAR playbook triggers
- Describe FortiSOAR playbook steps
- Create a playbook
- Ingest data from FortiSIEM
- Create preprocessing rules
- Describe Jinja and JSON, and how FortiSOAR uses them
- Describe dynamic variables and values
- Describe built-in functions
- Design and publish a module
- Export and import FortiSOAR entities
- Configure dashboards
- Configure widgets in templates
- Apply operators to evaluate conditions
- Demonstrate the JSON and YAQL query filters
- Describe FortiSOAR incidents
- Describe campaigns
- Describe the MITRE ATT&CK Matrix for Enterprise
- Describe incident phases on FortiSOAR
- Describe the incident handling workflow on FortiSOAR
- Configure shift and queue management
- Configure war rooms
- Troubleshoot common playbook issues
- Troubleshoot common connector issues
- Configure logging levels and log files for analysis
- Describe API basics
- Configure the FortiSOAR API
- Configure FortiManager API integration with FortiSOAR
- Describe FortiAI on FortiSOAR

Who should attend

SOC analysts responsible for developing playbooks; creating modules, templates, dashboards, and widgets; and performing incident handling with FortiSOAR should attend this course.