

FortiSOAR Administrator

In this course, you will learn about FortiSOAR architecture, and how to deploy, configure, manage, operate, and monitor FortiSOAR in a SOC environment. You will learn about various system customization options, HA deployment, security management using role-based access control (RBAC), and various system monitoring tools.

Product Version

- FortiSOAR 7.3.0

Course Duration

- Lecture time (estimated): 7 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 13 hours
 - 2 full days or 3 half days

Who Should Attend

This course is intended for cybersecurity professionals responsible for planning, deploying, configuring, and managing FortiSOAR deployments in a SOC environment.

Certification

This course is intended to help you prepare for the *Fortinet NSE 6 - FortiSOAR 7.3 Administrator* certification exam. This certification is part of the Fortinet Certified Professional - Security Operations certification track.

Prerequisites

- You must have an understanding of the topics covered in *FCP - FortiGate Security*, or have equivalent experience.
- Familiarity with SOC technologies and processes is recommended.

Agenda

1. Introduction to FortiSOAR
2. Device Management
3. System Configuration
4. High Availability
5. Searching, War Rooms, and Upgrading
6. System Monitoring and Troubleshooting

Objectives

After completing this course, you will be able to:

- Identify challenges of security teams, and assist security teams with SOAR best practices
- Identify the role of SOAR in assisting security teams
- Describe the basics of SOAR technology
- Manage licenses
- Deploy and manage a FortiSOAR VM
- Configure teams, roles, and users
- Configure authentication
- Schedule the purging of audit logs and executed playbook logs
- Configure playbook recovery
- Configure environment variables
- Configure company branding
- Configure system fixtures
- Configure the recycle bin
- Monitor and manage audit logs
- Use the configuration manager
- Monitor system resources
- Deploy, configure, manage, and troubleshoot a FortiSOAR high availability cluster
- Identify the types of logs used for troubleshooting
- Collect log files used for troubleshooting
- Troubleshoot key services and processes on 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-FSR-ADM

Self-Paced Training

Includes online training videos and resources through the [Fortinet Training Institute](#) library, free of charge.

See [Purchasing Process](#) for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 7
- CPE lab hours: 6
- 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](#).

