FORTINET
Training Institute

FortiSOAR Design and Development

In this course, you will learn how to use FortiSOAR to design simple to complex playbooks, examine the role of FortiSOAR in mitigating malicious indicators, and learn how to create interactive dashboards to display relevant information about alerts and incidents. You will also learn how to integrate FortiSOAR with FortiGate, FortiSIEM, and FortiMail.

Product Version

FortiSOAR 7.3.0

FortiSIEM 6.6.0

FortiGate 7.2.1

FortiMail 6.4.3

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 17 hours / 3 days

Who Should Attend

This course is intended for cybersecurity professionals responsible for planning, designing, and customizing FortiSOAR deployments, integrating FortiSOAR with FortiGate, FortiSIEM, and FortiMail, and FortiSOAR playbook design and development.

Certification

This course does not have a 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 6 FortiSOAR Administrator

It is recommended that you have an understanding of Python programming and Jinja2 templating language, and familiarity with email security and SIEM technologies is also beneficial.

Agenda

1. Introduction to FortiSOAR
2. Dashboard Templates and Widgets
3. Module Templates and Widgets
4. Application Editor
5. Dynamic Variable and Values
6. Jinja Filters, Functions, and Conditions
7. Introduction to Playbooks
8. Playbook Core Steps
9. Playbook Evaluate Steps
10. Playbook Connectors, Data Ingestion, and Execution Steps

Objectives

After completing this course, you will be able to:

- Identify the role of FortiSOAR in a SOC environment
- Plan a FortiSOAR deployment
- Manage incidents and alerts in a SOC environment
- Explore, create, and customize dashboards
- Explore the structure of a template
- Create, customize, and analyze dashboard widgets
- Create, customize, and publish modules
- Search for records and filter search records
- Analyze field-type options in the field editor
- Build a user prompt from a manual trigger step
- Define variables and dictionaries in Jinja
- Configure step utilities within a playbook step
- Configure various core steps of a playbook
- Configure different modes of data ingestion
- Install/configure connectors and apply to a playbook
- Configure various utility steps
- Configure referenced playbooks
- Configure and use dynamic variables and values
- Use expressions to customize playbook input and outputs
- Use common Jinja filters and functions
- Use filters to extract data from complex data structures
- Build loop functions and conditional statements

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 as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

Self-Paced Training

Includes online training videos and resources through the Fortinet 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.

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

(ISC)2

- CPE training hours: 10
- 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.