FortiDeceptor Administrator

In this course, you will learn how to deceive, expose, and eliminate threats early in the attack kill chain using FortiDeceptor. FortiDeceptor lures attackers into revealing themselves by engaging with a range of deception assets distributed throughout the network environment.

Product Version

FortiDeceptor 5.3

The *FortiDeceptor 5.3* course is applicable only to hardware devices and VMs.

Course Duration

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

Who Should Attend

Cybersecurity professionals responsible for the day-to-day administration, management, and troubleshooting of FortiDeceptor should attend this course.

Certification

This course does not have a certification exam.

Prerequisites

You should have an understanding of the topics covered in the FCP - *FortiGate Administrator* course, or have equivalent experience.

Agenda

1. Introduction
2. Deception and Incidents
3. Deception Strategies
4. FortiDeceptor Integration

Objectives

After completing this course, you should be able to:

- Describe how FortiDeceptor integrates into Enterprise networks
- Describe FortiDeceptor modules and key features
- Access FortiDeceptor and view the dashboard
- Configure network and system settings
- Configure FortiDeceptor central management
- Configure FortiDeceptor for air-gapped deployments
- Configure deployment networks
- Deploy decoy VMs and configure lure resources
- Use the deployment wizard to create and deploy decoys
- Select the appropriate decoys, services, and lures
- Create and deploy FortiDeceptor token packages
- Analyze the FortiDeceptor deployment map
- Analyze incidents, attacks, and the attack map
- Navigate the MITRE ICS matrix
- Design deception strategies based on network requirements
- Differentiate light-stack and full-stack deception
- Detect and mitigate new outbreaks
- Follow best practices for decoy and token deployment
- Follow best practices for AD integration
- Design deception based on network topology requirements
- Formulate deception strategies against specific attack vectors
- Integrate FortiDeceptor with the Fortinet Security Fabric and other Fortinet products
- Integrate FortiDeceptor with third-party products

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-FDC

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 the following methods:

- Credit card, through the course on the Fortinet Training Institute
- 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.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FDC-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

ISC2

- CPE training hours: 3
- CPE lab hours: 3
- 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.