FortiSandbox

In this course, you will learn how to protect your organization and improve its security against advance threats that bypass traditional security controls. You will learn about how FortiSandbox detects advanced threats. You will also learn about how FortiSandbox dynamically generates local threat intelligence, and how other advanced threat protection (ATP) components leverage this threat intelligence information to protect organizations from advanced threats.

Product Version

- FortiSandbox 4.2

Course Duration

- Lecture time (estimated): 7 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 14 hours
  - 2 full days or 4 half days

Who Should Attend

This course is intended for network security engineers responsible for designing, implementing, and maintaining an advanced threat protection solution with FortiSandbox, in an Enterprise network environment.

Certification

This course does not have a certification exam.

Prerequisites

You must have an understanding of the topics covered in *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure*, or have equivalent experience.

It is also recommended that you have an understanding of the topics covered in *FCP - FortiMail*, *FCP - FortiWeb*, and *FCP - FortiClient*, or have equivalent experience.

Agenda

1. Attack Methodologies and the ATP Framework
2. Key Components
3. High Availability, Maintenance and Troubleshooting
4. Protecting the Edge
5. Protecting Email Networks
6. Protecting Web Applications
7. Protecting End Users
8. Protecting Third-Party Appliances
9. Results Analysis

Objectives

After completing this course, you will be able to:

- Identify different types of cyber attacks
- Identify threat actors and their motivations
- Understand the anatomy of an attack—the kill chain
- Identify the potentially vulnerable entry points in an Enterprise network
- Identify how ATP works to break the kill chain
- Identify the role of FortiSandbox in the ATP framework
- Identify appropriate applications for sandboxing
- Identify FortiSandbox architecture and key components
- Identify the appropriate network topology requirements
- Configure FortiSandbox
- Monitor FortiSandbox operation
- Configure FortiGate, FortiMail, FortiWeb, and FortiClient integration with FortiSandbox
- Identify the role of machine learning in preventing zero day attacks and advanced threats
- Configure machine learning on FortiWeb
- Analyze attack logs from machine learning system
- Troubleshoot FortiSandbox
- Perform analysis of outbreak events
- Remediate outbreak events based on log and report analysis

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-FSA

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.

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

FT-FSA-LAB

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

(ISC)^2

- CPE training hours: 7
- 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.