Advanced Threat Protection

In this 2-day course, participants will learn the following:

- How to protect their organization and improve its security against advance threats that bypass traditional security controls
- How FortiSandbox detects threats that traditional antivirus product miss
- How FortiSandbox dynamically generates local threat intelligence, which can be shared throughout the network
- How other advanced threat protection (ATP) components—FortiGate, FortiMail, FortiWeb, and FortiClient—leverage this threat intelligence information to protect organizations, from end-to-end, from advanced threats

Product Version

FortiSandbox 2.5

Formats

- Instructor-led classroom
- Instructor-led online*
- Self-paced online

*Private class only. Please contact your Fortinet sales representative.

Agenda

1. Attack Methodologies and the ATP Framework
2. Introduction to FortiSandbox
3. Protecting the Edge
4. Protecting Email Networks
5. Protecting Web Applications
6. Protecting End Users
7. Protecting Third-Party Appliances
8. Results Analysis

Objectives

After completing this course, participants 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 the ATP framework works to break the kill chain
- Identify the role of FortiSandbox in the ATP framework
- Identify appropriate applications for sandboxing
- Identify FortiSandbox architecture
- Identify FortiSandbox key components
- Identify the appropriate network topology requirements
- Configure FortiSandbox
- Monitor FortiSandbox operation
- Configure FortiGate integration with FortiSandbox
- Configure FortiMail integration with FortiSandbox
- Configure FortiWeb integration with FortiSandbox
- Configure FortiClient integration with FortiSandbox
- Troubleshoot FortiSandbox-related issues
- Perform analysis of outbreak events
- Remediate outbreak events based on log and report analysis

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.

Prerequisites

Participants must have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure

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

- NSE 6 FortiMail
- NSE 6 FortiWeb

System Requirements

If participants take an online format of this class, they must have a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers / headphones
- One of the following:
  - HTML 5 support
  - An up-to-date Java runtime environment (JRE) with Java plugin enabled in the web browser

Participants should use a wired Ethernet connection *not* a Wi-Fi connection. The firewall or FortiClient must allow connections to the online labs.

Certification

This course is intended to help participants prepare for the NSE 7 Advanced Threat Protection certification exam.