FortiSandbox Administrator

Course Description

In this course, you will learn how to protect your organization and improve its security against advanced 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.

Who Should Attend

This course is intended for network security professionals responsible for designing, implementing, and maintaining a Fortinet advanced threat protection solution with FortiSandbox.

Prerequisites

You must have an understanding of the topics covered in FCF - FortiGate Fundamentals (or have equivalent experience).

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

- FortiGate Administrator
- FortiMail
- FortiWeb
- FortiClient EMS

Agenda

1. Attack Methodologies
2. Deployment and System Settings
3. Scanning and Rating Components
4. High Availability
5. FortiGate Integration
6. FortiMail Integration
7. FortiWeb Integration
8. FortiClient EMS Integrations
9. Results Analysis

Objectives

After completing this course, you will be able to:

- Identify threat actors and their motivations

- Identify different types of counterattacks
- Describe the Fortinet solutions for different stages of the Cyber Kill Chain
- Analyze the MITRE ATT&CK matrix
- Identify FortiSandbox architecture and key components
- Plan a FortiSandbox deployment
- Describe FortiSandbox input methods
- Select an appropriate deployment mode and configure initial settings
- Explain FortiSandbox interface requirements
- Configure alert emails, SNMP monitoring, and a remote backup
- Analyze dashboards, the operation center, and system events
- Monitor FortiSandbox operation and troubleshoot system issues
- Manage guest VMs
- Configure VM association settings and scan options
- Configure high availability cluster settings and health checks
- Monitor cluster health and individual nodes
- Configure FortiGate, FortiMail, FortiWeb, and FortiClient EMS integration with FortiSandbox
- Configure threat intelligence sharing
- Monitor submission logs from various Fortinet Security Fabric devices
- Troubleshoot integration issues
- Analyze scan job reports

System Requirements

If you take the online version of this class, candidates must have a computer that has the following:

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

You should use a Wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Product Versions

FortiSandbox 5.0

Course Duration

- Lecture time (estimated): 7 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 13 hours

- 2 full days or 4 half days

Formats

- Instructor-led (classroom and online)
- Self-paced online

ISC2

- CPE training hours: 7
- CPE lab hours: 6
- CISSP domains: Security Operations

Part Number (SKU)

See Purchasing Process for more information

Certification

This course is not in the certification program.