FortiSandbox

In this 1-day class, you will learn the basics of FortiSandbox — how malware works, how virus writers try to avoid detection, and how you can regain the advantage in the battle to secure your network from zero-day threats.
In interactive labs, you will explore how to deploy FortiSandbox in integration with other Fortinet devices, and how to use the various available methods of inspection for both files and harmful web sites. You will also learn how to optimize sandboxing performance for your specific network, how to submit malware samples to Fortinet's security research labs.

Product Version

FortiSandbox 2.0.3

Formats

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

* Private class only. Please contact your Fortinet Sales Representative.

Agenda

1 Sandboxing Concepts
2 Basic Setup
3 Inline Deployment
4 Sniffer Deployment
5 Other File Submission Methods & URL Scanning
6 Logs & Reports
7 Troubleshooting

Objectives

After completing these courses, you will be able to:

- Explain why antivirus engines can't always catch zero-day exploits
- Describe how smart viruses try to avoid detection
- Compare the mechanisms of antivirus signatures, heuristics, and sandboxing
- Deploy a FortiSandbox
- Integrate other Fortinet devices such as FortiMail, FortiWeb, and FortiGate
- Validate the built-in Microsoft software licenses
- Leverage a FortiManager as a local FortiGuard server for your FortiSandbox
- Monitor new malware detections on your FortiSandbox
- Submit samples of new viruses to FortiGuard
- Understand the basics of an incident response plan

Who Should Attend

Anyone who is responsible for day-to-day management and/or configuration of a FortiSandbox appliance.

Prerequisites

NSE 4 and FortiMail Specialist certifications are recommended.

System Requirements

If you take an online format of this class, you must have a computer with:

- High-speed Internet connection
- Up-to-date web browser
- PDF viewer
- Speakers / headphones
- Either:
- HTML 5 support **or**
- Up-to-date Java runtime environment (JRE) with Java plugin enabled in your web browser

Wired Ethernet connection (**not Wi-Fi**) recommended. **Firewalls including Windows Firewall or FortiClient must allow connections with the online labs.**

Certification

This course prepares you for the FortiSandbox 2.0.3 Specialist Exam. This is part of the courses that prepare you for the NSE 6 certification exam.