Descripción del Curso

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.

Quien debe asistir

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

Requisitos previos

You must have an understanding of the topics covered in NSE 4 FortiGate Security and NSE 4 FortiGate Infrastructure, or have equivalent experience.

It is also recommended that you have an understanding of the topics covered in NSE 6 FortiMail, NSE 6 FortiWeb, and NSE 5 FortiClient, or have equivalent experience.

Agenda

1. Attack Methodologies and the ATP Framework
2. FortiSandbox 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

Objetivos

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

Requisitos del Sistema

If you take an online format of this class, you must use 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.

Certificación

This course prepares you for the NSE 7 Advanced Threat Protection certification exam.

Duración

2 días
