Training: Fortinet
FortiSandbox Administrator

Premier Authorized Training Center

TRAINING GOALS:

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.

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

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Analyze scan job reports

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.

CONSPECT:

- Attack Methodologies
- Deployment and System Settings
- Scanning and Rating Components
- High Availability
- FortiGate Integration
- FortiMail Integration
- FortiWeb Integration
- FortiClient EMS Integrations
- Results Analysis

REQUIREMENTS:

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:

- FCP - FortiGate Administrator
- FCP - FortiMail
- FCP - FortiWeb
- FCP - FortiClient EMS

Difficulty level



Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

CERTIFICATE:

The participants will obtain certificates signed by Fortinet (course completion).

This course prepares you also for the *FCP - FortiSandbox Administrator* exam. By passing this exam, you will be awarded the associated exam badge.

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

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

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310