FORTINET
Premier Authorized Training Center

fast lane

FortiNDR On-Premises Administrator (FT-FortiNDR)

Course Description

In this course, you will learn how to administer, manage, and troubleshoot an onpremises FortiNDR deployment. You will explore different use cases and discover the various source feeds of FortiNDR. You will learn how it integrates within the Fortinet Security Fabric and collaborates with other products to enhance malware detection and enforce automatic response. You will also explore the various features on FortiNDR that provide administrators with a broad picture of the detected anomalies and aids with forensic analysis.

Product Version

- FortiNDR 7.4

Course Duration

1 day

Certification:

This course does not have a certification exam.

Prerequisites

- You must have knowledge of networking and cybersecurity, and basic experience working with FortiGate and the Fortinet Security Fabric. It is also recommended that you have an understanding of the topics covered in the FCP - FortiGate Administrator course

Outlines

1. Introduction
2. Malware Detection and Security Analysis
3. Security Fabric Integration and Fortinet Ecosystem
4. Third-Party Inputs

Objectives

After completing this course, you will be able to:

- Describe how FortiNDR can protect your network
- Describe the FortiNDR operating modes
- Describe how FortiNDR monitors network traffic
- Describe how FortiNDR interacts other Fortinet or thirdparty products
- Describe how FortiNDR can scan network share drives
- Access FortiNDR GUI menus, CLI commands, and perform initial configuration tasks
- Analyze network insight information on detected attacks

- Manage false positive detection
- Analyze attack scenarios, timelines, and host stories
- Identify network outbreaks and assess network damage
- Configure static filters and NDR muting rules
- Configure Windows AD integration for device enrichment
- Analyze various logs on FortiNDR
- Integrate FortiNDR in Fortinet Security Fabric
- Describe how FortiNDR triggers responses
- Configure enforcement rules
- Configure automated actions
- Configure various FortiNDR integration modes
- Integrate FortiNDR with FortiMail and FortiSandbox
- Configure the logs and reports available on FortiNDR
- Generate FortiNDR reports (FortiAnalyzer/FortiSIEM)
- Configure ICAP integration
- Explain FortiNDR API capabilities
- Configure and analyze NetFlow logs and dashboards
- Configure device enrichment and remote authentication
- Configure network share scanning and quarantining l Analyze network share scan results

Who should attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiNDR onpremises deployments should attend this course.