FortiNDR On-Premises Administrator

In this course, you will learn how to administer, manage, and troubleshoot an on-premises 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

- Lecture time (estimated): 4 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 8 hours
  - 1 full day or 2 half days

Who Should Attend

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

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.

Agenda

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 third-party 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
- Analyze network share scan results

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-NDR-ADM

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-NDR-ADM-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

ISC2

- CPE training hours: 4
- CPE lab hours: 4
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.