FortiEDR Administrator

Total course duration (estimated): 16 hours

2 full days

In this course, you will learn how to use **FortiEDR** to secure endpoints against advanced threats using real-time, automated incident response. The training also explains how FortiEDR continuously protects endpoints by detecting and responding to attacks automatically as they happen.

This course is ideal for security professionals who are responsible for administering, managing, or supporting FortiEDR in their organization.

Prerequisites

You must have a basic understanding of cybersecurity concepts.

Agenda

1. Product Overview and Installation

2. Administration

3. Security Policies

4. Fortinet Cloud Service and Playbooks

5. Communication Control

6. Events and Incidents

7. Threat Hunting

8. Fabric Integration and FortiXDR

9. RESTful API

10. Troubleshooting

Objectives

After completing this course, you will be able to:

- Understand the FortiEDR security approach and how it operates
- Identify FortiEDR components, how they communicate, and how they are configured
- Perform key administrative tasks such as managing console users, updating collectors, removing personal data for GDPR compliance, deploying multitenant environments, and reviewing system events
- Explain what Fortinet Cloud Services are and how they function
- Navigate and perform basic tasks across the management console, including the Dashboard, Incidents, Threat Hunting, Communication Control,

Inventory, and Administration sections, as well as Security Policies and Playbooks

- Manage security events and track their status
- Block communications from risky or unwanted applications that are not necessarily malicious
- Detect and remove malicious executables across all endpoint devices
- Understand FortiEDR integration with the Fortinet Security Fabric and how FortiXDR works
- Use RESTful APIs to manage and automate FortiEDR operations
- Prioritize, investigate, and analyze security events effectively
- Remediate malicious activities and create exceptions for trusted processes
- Perform basic troubleshooting across all FortiEDR components
- Collect and analyze collector logs and memory dumps