

FortiEDR Administrator

Course Description

In this course, you will learn how to use FortiEDR to protect your endpoints against advanced attacks with real-time orchestrated incident response functionality. You will also learn about how FortiEDR protects your endpoints automatically in real time.

Who Should Attend

Security professionals involved in the administration and support of FortiEDR should attend this course.

Prerequisites

You must have a basic understanding of cybersecurity concepts.

Agenda

1. Product Overview and Installation
2. Administration
3. Security Policies
4. Fortinet Cloud Security and Playbooks
5. Communication Control
6. Events and Incidents
7. Threat Hunting
8. RESTful API
9. Troubleshooting

Objectives

After completing this course, you should be able to:

- Explain the FortiEDR approach and how it works
- Identify the communicating components and how they are configured
- Perform important administrative tasks, including managing console users, updating collectors, deleting personal data for GDPR compliance, deploying multi-tenant environments, and viewing system events
- Define at Fortinet Cloud Service is and how it works
- Complete basic tasks in each area of the management console: the Dashboard, Incidents, Threat Hunting, Communication Control, Inventory, and Administration tabs, and the Security Policies and Playbooks pages
- Manage security events and their status
- Block communication from applications that are risky or unwanted, but not inherently malicious
- Find and remove malicious executables from all the devices in your environment
- Explain how FortiEDR integrates with Fortinet Security Fabric, and how FortiXDR works

- Use RESTful API to manage your FortiEDR environment
- Prioritize, investigate, and analyze security events
- Remediate malicious events and create exceptions to allow safe processes
- Perform various basic troubleshooting tasks on all FortiEDR components
- Obtain collector logs and memory dumps

System Requirements

If you take an online version of this class, you must have a computer with:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers / headphones
- One of the following:
 - HTML5 support
 - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled in your web browser

You should use a wired Ethernet connection, *not* a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Product Versions

- FortiEDR 7.0

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 12 hours
 - 2 full days or 4 half days

Formats

- Instructor-led training
- Self-paced training

ISC2

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

Part Number (SKU)

See Purchasing Process for more information

Certification

