FORTINET CERTIFIED PROFESSIONAL

Security Operations

FORTINET Training Institute

Course Description

FortiEDR

In this class, you will learn how to use FortiEDR to protect your endpoints against advanced attacks with real-time orchestrated incident response functionality. You will also explore FortiEDR features and how they protect your endpoints automatically in real time.

Product Version

- FortiEDR 5.0

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 12 hours
  - 2 full days or 3 half days

Who Should Attend

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

Certification

This course is intended to help you prepare for the *Fortinet NSE 5 - FortiEDR 5.0* exam. This exam is part of the Fortinet Certified Professional - Security Operations certification track.

Prerequisites

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 Alerting
7. Threat Hunting and Forensics
8. Fortinet Security Fabric Integration and FortiXDR
9. RESTful API
10. 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, deploy multi-tenant environment and viewing system events
- Recognize what Fortinet Cloud Service is and how it works
- Complete basic tasks in of each area of the management console: the Dashboard, the Event Viewer, the Forensics tab, the Threat Hunting module, Communication Control, Security Policies, Playbooks, Inventory, and the Administration tab
- 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
- Understand 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
- Carry out various basic troubleshooting tasks on all FortiEDR components
- Obtain collector logs and memory dumps

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-EDR

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 a 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-EDR-LAB

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

(ISC)^2

- CPE training hours: 6
- CPE lab hours: 6
- CISSP domains: Communication and Network Security

Program Policies and FAQs

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