FortiEDR

In this two-day class, you will learn how to use FortiEDR to protect your endpoints against advanced attacks with real-time orchestrated incident response functionality.

Product Version

FortiEDR 4.2

Formats

- Instructor
- Instructor-led online
- Self-paced online

Agenda

1. Overview and Technical Positioning
2. Installation and Architecture
3. Administration
4. Best Practices and Deployment
5. The User Interface in Depth Part 1
6. The User Interface in Depth Part 2
7. Events and Alerting
8. Help Desk Level 1 Triage
9. Communication Control
10. Next-Generation Antivirus
11. Threat Hunting
12. RESTful API
13. Multi-Tenancy
14. Fortinet Cloud Service
15. Advanced Troubleshooting
16. Endpoint Security 101
17. PowerShell and CScript
18. Alert Analysis 401

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
- Schedule, organize, and tune a new deployment
- Carry out basic troubleshooting steps, including: verifying that FortiEDR is installed and actively blocking malware, identifying whether FortiEDR has blocked a process or connection, finding logs, and contacting FortiEDR Support
- Perform important administrative tasks, including: managing console users, updating collectors, deleting personal data for GDPR compliance, and viewing system events
- 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
- Define next-generation antivirus, its role in FortiEDR, and where it falls in the order of operations
- Find and remove malicious executables from all the devices in your environment
- Use RESTful API to manage your FortiEDR environment
- Administer a multi-tenant environment
- Recognize what Fortinet Cloud Service is and how it works
- Troubleshoot collector upgrades and performance issues
- Obtain collector logs and memory dumps
- Have a basic understanding of the history of malware, how it exploits trust, and the persistence techniques used in malware today
- Triage PowerShell and CScript events, verify their destinations, and retrieve memory
- Prioritize, investigate, and analyze security events
- Remediate malicious events and create exceptions to allow safe processes

Who Should Attend

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

Prerequisites

- Basic understanding of cybersecurity concepts

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or 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 Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Certification

This course is intended to help you prepare for the FortiEDR 4.2 specialist exam.

This is one of the courses that prepares you to take the NSE 5 certification exam.