

## **Enterprise Computing Solutions - Education Services**

# **TRAINING OFFERING**

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com Phone: +46 8 555 188 00

## FERTINET. NSE 6 - FortiEDR Administrator

CODE: LENGTH: PRICE:

FNT\_FT-EDR 16 Hours (2 days) Request Price

#### **Description**

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 Versions** 

• FortiEDR 5.0

#### **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
- 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
- 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 basic troubleshooting tasks on all FortiEDR components
- Obtain collector logs and memory dumps

#### **Audience**

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

## **Prerequisites**

A basic understanding of cybersecurity concepts.

#### **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.

### **Programme**

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

#### **Test and Certification**

#### Exam:

This course prepares you for the Fortinet NSE 5 - FortiEDR 5.0 exam. By passing this exam, you will be awarded the associated exam badge.

#### Certification:

This exam is part of the FCP Security Operations certification track.

#### **Session Dates**

På begäran, kontakta oss

#### Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.