





Security Operations FortiEDR

# **Course 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 Version:**

• FortiEDR 5.0

## **Course Duration:**

2 days

#### **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

#### **Outlines:**

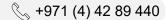
- 1. Product Overview and Installation
- 2. Administration
- 3. Security Policies
- 4. Fortinet Cloud Service and Playbooks
- 5. Communication Control
- 6. Events and Alerting
- 7. Threat Hunting and Forensics
- 8. Fortinet Security Fabric Integration and FortiXDR
- 9. RESTful API
- 1. Troubleshooting

## **Objectives:**

After completing this course, you will 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

k training@fastlane-mea.com



- Complete basic tasks in of each area of the management console: the Dashboard, the Even 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

#### Who should attend

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

