FortiEDR

Duration: 2 Days

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.

Target Audience:

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

Prerequisites:

A basic understanding of cybersecurity concepts

Course Objectives:

- 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

Course Outline:

- Product Overview and Installation
- Administration
- Security Policies
- Fortinet Cloud Service and Playbooks
- Communication Control
- Events and Alerting
- Threat Hunting and Forensics
- Fortinet Security Fabric Integration and FortiXDR
- RESTful API
- Troubleshooting