

---

## VMware Carbon Black Cloud Enterprise EDR

**Duration: 1 Day**    **Course Code: VMCBCEEDR**

---

### Overview:

This one-day VMware Carbon Black course teaches you how to use the VMware Carbon Black® Cloud Enterprise EDR™ product and leverage its capabilities to configure and maintain the system according to your organization's security posture and policies. This course provides an in-depth, technical understanding of the product through comprehensive coursework and hands-on scenario-based labs.

Product Alignment: **VMware Carbon Black® EDR™** VMware Carbon Black Cloud Endpoint™ Enterprise

---

### Target Audience:

Security operations personnel, including analysts and managers

---

### Objectives:

- Describe the components and capabilities of VMware Carbon Black Cloud Enterprise EDR
  - Identify the architecture and data flows for VMware Carbon Black Cloud Enterprise EDR communication
  - Perform searches across endpoint data to discover suspicious behavior
  - Manage watchlists to augment the functionality of VMware Carbon Black Cloud Enterprise EDR
  - Create custom watchlists to detect suspicious activity in your environment
  - Describe the process for responding to alerts in VMware Carbon Black Cloud Enterprise EDR
  - Discover malicious activity within VMware Carbon Black Cloud Enterprise EDR
  - Describe the different response capabilities available from VMware Carbon Black Cloud
- 

### Prerequisites:

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals
-

## Content:

### 1 Course Introduction

- Introductions and course logistics
- Course objectives

### 2 Data Flows and Communication

- Hardware and software requirements
- Architecture
- Data flows

### 3 Searching Data

- Creating searches
- Search operators
- Analyzing processes
- Analyzing binaries
- Advanced queries

### 4 Managing Watchlists

- Subscribing
- Alerting
- Custom watchlists

### 5 Alert Processing

- Alert creation
- Analyzing alert data
- Alert actions

### 6 Threat Hunting in Enterprise EDR

- Cognitive Attack Loop
- Malicious behaviors

### 7 Response Capabilities

- Using quarantine
- Using live response

---

## Further Information:

For More information, or to book your course, please call us on 0800/84.009

[info@globalknowledge.be](mailto:info@globalknowledge.be)

[www.globalknowledge.com/en-be/](http://www.globalknowledge.com/en-be/)