

---

## VMware Carbon Black Cloud Endpoint Standard

**Duration: 1 Day**    **Course Code: VMCBCES**

---

### Overview:

This one-day VMware Carbon Black course teaches you how to use the VMware Carbon Black Cloud Endpoint™ Standard product and leverage the 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 Cloud Endpoint Standard VMware Carbon Black Cloud Endpoint™ Advanced VMware Carbon Black Cloud Endpoint™ Enterprise

---

### Target Audience:

System administrators and security operations personnel, including analysts and managers

---

### Objectives:

- Describe the components and capabilities of VMware Carbon Black Cloud Endpoint Standard
  - Identify the architecture and data flows for Carbon Black Cloud Endpoint Standard communication
  - Perform searches across endpoint data to discover suspicious behavior
  - Manage the Carbon Black Cloud Endpoint Standard rules based on organizational requirements
  - Configure rules to address common threats
  - Evaluate the impact of rules on endpoints
  - Process and respond to alerts
  - 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
- Analyzing events
- Search operators
- Advanced queries

### 4 Policy Components

- Rules
- Local scanner
- Sensor capabilities

### 5 Prevention Capabilities Using Rules

- Rule types
- Rule creation
- Reputation priority
- Configuring rules
- Evaluating rule impact

### 6 Processing Alerts

- Alert triage
- Alert actions

### 7 Response Capabilities

- Using quarantine
- Using live response

Hash banning

---

## 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/)