
VMware Carbon Black EDR Administrator

Duration: 1 Day **Course Code: VMCBEA**

Overview:

This one-day VMware Carbon Black course teaches you how to use the VMware Carbon Black® EDR™ 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 Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs.

Product Alignment: **VMware Carbon Black EDR**

Target Audience:

System administrators and security operations personnel, including analysts and managers

Objectives:

- By the end of the course, you should be able to meet the following objectives:
 - Describe the components and capabilities of the Carbon Black EDR server
 - Identify the architecture and data flows for Carbon Black EDR communication
 - Describe the Carbon Black EDR server installation process
 - Manage and configure the Carbon Black EDR sever based on organizational requirements
 - Perform searches across process and binary information
 - Implement threat intelligence feeds and create watchlists for automated notifications
 - Describe the different response capabilities available from the Carbon Black EDR server
 - Use investigations to correlate data between multiple processes
-

Prerequisites:

■

Content:

1 Course Introduction

- Introductions and course logistics
- Course objectives

2 Planning and Installation

- Hardware and software requirements
- Architecture
- Data flows
- Server installation review
- Installing sensors

3 Server Administration

- Configuration and settings
- Carbon Black EDR users and groups

4 Process Search and Analysis

- Filtering options
- Creating searches
- Process analysis and events

5 Binary Search and Banning Binaries

- Filtering options
- Creating searches
- Hash banning

6 Search best practices

- Search operators
- Advanced queries

7 Threat Intelligence

- Enabling alliance feeds
- Threat reports details
- Use and functionality

8 Watchlists

- Creating watchlists
- Use and functionality

9 Alerts / Investigations / Response

- Using the HUD
- Alerts workflow
- Using network isolation
- Using live response

Further Information:

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

info@globalknowledge.be

www.globalknowledge.com/en-be/