VMware Carbon Black EDR Administrator

Code:	EDU-VCBEDRA
Length:	1 days
URL:	View Online

This one-day 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.

Skills Gained

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

Who Can Benefit

System administrators and security operations personnel, including analysts and managers.

Prerequisites

There are no prerequisites for this course.

Course Details

Product Alignment

- VMware Carbon Black EDR

Outline

Course Introduction

- Introductions and course logistics
- Course objectives

Planning and Installation

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

Server Administration

- Configuration and settings
- Carbon Black EDR users and groups

Process Search and Analysis

- Filtering options
- Creating searches
- Process analysis and events

Binary Search and Banning Binaries

- Filtering options
- Creating searches
- Hash banning

Search best practices

- Search operators
- Advanced queries

Threat Intelligence

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

Watchlists

- Creating watchlists

- Use and functionality

Alerts / Investigations / Response

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