VMware Carbon Black Cloud Enterprise EDR

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

This one-day 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.

Skills Gained

By the end of the course, you should be able to meet the following 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

Who Can Benefit

Security operations personnel, including analysts and managers

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Course Details

Product Alignment

- VMware Carbon Black® EDR™
- VMware Carbon Black Cloud Endpoint™ Enterprise

Outline

Course Introduction

- Introductions and course logistics
- Course objectives

Data Flows and Communication

- Hardware and software requirements
- Architecture
- Data flows

Searching Data

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

Managing Watchlists

- Subscribing
- Alerting
- Custom watchlists

Alert Processing

- Alert creation
- Analyzing alert data
- Alert actions

Threat Hunting in Enterprise EDR

- Cognitive Attack Loop
- Malicious behaviors

Response Capabilities

- Using quarantine
- Using live response

Schedule (as of 3)

Date	Location	
Apr 20, 2021 – Apr 20, 2021	Virtual	Enroll
May 5, 2021 – May 5, 2021	Virtual	Enroll
May 28, 2021 – May 28, 2021	Virtual	Enroll
Jun 15, 2021 – Jun 15, 2021	Virtual	Enroll
Jul 8, 2021 – Jul 8, 2021	Virtual	Enroll
Jul 20, 2021 – Jul 20, 2021	Virtual	Enroll