VCBCEEDR
VMware Carbon Black Cloud Enterprise EDR

Duration: 1 Day

Course Overview:

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.

Prerequisites:

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Who Should Attend:

The primary audience for this course is as follows:

- Security operations personnel including analysts and managers

Course Objectives:

Upon completing this course, the learner will be able to meet these overall 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

Course Outline:

Module 1: Course Introduction
- Introductions and course logistics
- Course objectives

Module 2: Data Flows and Communication
- Hardware and software requirements
- Architecture
- Data flows

Module 3: Searching Data
- Creating searches
- Search operators
- Analyzing processes
- Analyzing binaries
- Advanced queries

Module 4: Managing Watchlists
- Subscribing
- Alerting
- Custom watchlists

Module 5: Alert Processing
- Alert creation
- Analyzing alert data
- Alert actions

Module 6: Threat Hunting in Enterprise EDR
- Cognitive Attack Loop
- Malicious behaviors

Module 7: Response Capabilities
- Using quarantine
- Using live response