



VCBCM VMware Carbon Black Portfolio: Configure and Manage

Duration: 5 Days

Course Overview:

This 5-day course teaches you how to install, configure, and manage the VMware Carbon Black® Portfolio suite of products, which include:

- VMware Carbon Black® App Control™ Administrator
- VMware Carbon Black® EDR™ Administrator
- VMware Carbon Black Cloud Endpoint™ Standard
- VMware Carbon Black® Cloud Audit and Remediation
- VMware Carbon Black® Cloud Enterprise EDR™

You learn how to use the capabilities of the products according to the organization's security posture and organizational policies. This course provides an in-depth, technical understanding of the Carbon Black Portfolio through comprehensive coursework, hands-on labs, and scenario-based exercises.

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- System administration experience on Microsoft Windows or Linux operating systems.

Who Should Attend:

The primary audience for this course is as follows:

- System administrators and 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 Carbon Black App Control
- Manage and configure the Carbon Black App Control server based on organizational requirements
- Create policies to control enforcement levels and agent functionality
- Implement rules to support the organization's security posture
- Use the Carbon Black App Control tools to understand agent and server data
- 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 server 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
- Describe the components and capabilities of Carbon Black Cloud Endpoint Standard
- Identify the architecture and data flows for VMware Carbon Black Cloud products
- 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
- Describe the components and capabilities of Carbon Black Cloud Enterprise EDR
- Perform searches across endpoint data to discover suspicious behavior
- Manage watchlists to augment the functionality of Carbon Black Cloud Enterprise EDR
- Create custom watchlists to detect suspicious activity in your environment
- Describe the process for responding to alerts in Carbon Black Cloud Enterprise EDR
- Discover malicious activity within Carbon Black Cloud Enterprise EDR
- Describe the different response capabilities available from VMware Carbon Black Cloud
- Describe the components and capabilities of Carbon Black Cloud Audit and Remediation
- Describe the use case and functionality of recommended queries
- Achieve a basic knowledge of SQL
- Describe the elements of a SQL query
- Evaluate the filtering options for queries
- Perform basic SQL queries on endpoints
- 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: VMware Carbon Black App Control Administrator

- Login Accounts and Groups
- Policies
- Computer Details
- Custom Rules
- Tools
- Events
- Baseline Drift

Module 3: VMware Carbon Black EDR

- Planning and Architecture
- Server Installation & Administration
- Process Search and Analysis
- Binary Search and Banning Binaries
- Search best practices
- Threat Intelligence
- Watchlists
- Alerts / Investigations / Responses

Module 4: VMware Carbon Black Cloud Endpoint Standard

- Data Flows and Communication
- Searching Data
- Policy Components
- Prevention Capabilities Using Rules
- Processing Alerts
- Response Capabilities

Module 5: VMware Carbon Black Cloud Enterprise EDR

- Managing Watchlists
- Alert Processing
- Threat Hunting in Enterprise EDR
- Response Capabilities

Module 6: VMware Carbon Black Cloud Audit and Remediation

- Query Basics
- Recommended Queries
- SQL Basics
- Filtering Results
- Basic SQL Queries
- Advanced Search Capabilities
- Response Capabilities