

VMware Carbon Black Cloud Endpoint Standard

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

This one-day course teaches you how to use the VMware Carbon Black Cloud Endpoint™ Standard 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 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 Endpoint Standard
- Identify the architecture and data flows for Carbon Black Cloud Endpoint Standard communication
- 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™

Who Can Benefit

System administrators and 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 Cloud Endpoint Standard
- VMware Carbon Black Cloud Endpoint™ Advanced
- 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
- Analyzing events
- Search operators
- Advanced queries

Policy Components

- Rules
- Local scanner
- Sensor capabilities

Prevention Capabilities Using Rules

- Rule types
- Rule creation
- Reputation priority
- Configuring rules
- Evaluating rule impact

Processing Alerts

- Alert triage
- Alert actions

Response Capabilities

- Using quarantine
 - Using live response
 - Hash banning
-

ExitCertified® Corporation and iMVP® are registered trademarks of ExitCertified ULC and ExitCertified Corporation and Tech Data Corporation, respectively
Copyright ©2021 Tech Data Corporation and ExitCertified ULC & ExitCertified Corporation.
All Rights Reserved.

Generated 1