vmware LEARNING

VMware Endpoint Security: Core Technical Skills

Course Overview

In this 5-hour e-learning course, you explore security concepts and practices, focusing on the features and security capabilities of VMware Carbon Black Cloud®. The course provides use cases, examples, and hands-on simulations to demonstrate skills that you require as a security professional. This course will also teach you about securing endpoints in their environment.

Course Objectives

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

- Identify types of cybersecurity vulnerabilities
- Recognize attack mitigation strategies
- Describe the stages of an attack from the point of view of the attacker
- Identify control points in the VMware approach to security
- Describe how a defense-in-depth security approach works
- Identify features of VMware Carbon Black Cloud solutions
- Recognize when and how to assign reputations in VMware Carbon Black Cloud
- Identify use cases for VMware Carbon Black Cloud products
- Determine the best VMware Carbon Black Cloud sensor installation method for given use cases
- Recognize the search capabilities in VMware Carbon Black Cloud
- Create watchlists to detect threats
- Identify ways to respond to and dismiss alerts in VMware Carbon Black Cloud
- Describe when and how to use Live Response
- Recognize how to modify settings on the Policy page in VMware Carbon Black Cloud
- Describe how to remove malware from endpoints
- Describe when and how to use Inbox in the VMware Carbon Black Cloud console
- Identify tasks that can be performed in the VMware Carbon Black Cloud console
- Identify the pillars of a zero-trust approach to security

Target Audience

System architects, system administrators, IT managers, VMware partners, and individuals responsible for implementing and managing VMware Carbon Black Cloud architectures

Prerequisites

Basic understanding of operating systems and networking concepts

Course Modules

1 Introduction to Security
- Define the term cybersecurity
- Identify types of cybersecurity vulnerabilities
- Recognize attack mitigation strategies

2 Cybersecurity Attacks
- Describe the stages of an attack from the point of view of the attacker
- Identify different types of cybersecurity attacks

3 Recognizing Unusual Behavior
- Identify examples of behaviors associated with security tactics, techniques, and procedures
- Identify examples of indicators of compromise

4 VMware Security
- Recognize the central concepts in the intrinsic approach to security developed by VMware
- Identify the control points in the VMware approach to security

5 Zero Trust
- Identify the pillars of a zero-trust approach to security
- Recognize VMware products that support the implementation of a zero-trust approach to security

6 Defense in Depth
- Describe a defense-in-depth security approach
- Identify the functions of basic security controls

7 Endpoint Protection Strategies
- Distinguish between antivirus and next-generation antivirus solutions
- Identify features of VMware Carbon Black Cloud solutions

8 Using Reputations to Protect Endpoints
- Identify the priority of different reputations in VMware Carbon Black Cloud
- Recognize when and how to assign reputations in VMware Carbon Black Cloud

9 Endpoint Security Tools
- Identify use cases for Carbon Black Cloud Endpoint Standard
- Identify use cases for Carbon Black Cloud Audit and Remediation
- Identify use cases for Carbon Black Cloud Enterprise EDR

10 VMware Carbon Black Cloud Console
- Identify tasks that can be performed in the VMware Carbon Black Cloud console

11 Cloud Analysis and Malware Removal
- Describe the term unknown file in the context of VMware Carbon Black Cloud
- Describe how cloud analysis helps prevent malware
- Describe how to remove malware from endpoints

12 Inbox and Audit Log
- Describe when and how to use the Inbox in the VMware Carbon Black Cloud console
- Describe when and how to use audit logs in the VMware Carbon Black Cloud console

13 Installing VMware Carbon Black Cloud Sensor
- Determine the best VMware Carbon Black Cloud sensor installation method for given use cases
- Recognize the steps for performing an attended installation of a VMware Carbon Black Cloud sensor
- Recognize the steps for performing an unattended installation of a VMware Carbon Black Cloud sensor

14 Performing Searches in VMware Carbon Black Cloud
- Identify types of data collected in VMware Carbon Black Cloud
- Recognize the search capabilities in VMware Carbon Black Cloud
- Perform searches with VMware Carbon Black Cloud

15 Using Watchlists for Monitoring Cybersecurity threats
- Explain the purpose of a watchlist
- Describe the use cases for watchlists in VMware Carbon Black Cloud

vmware

- Create watchlists to detect threats

16 **Responding to Alerts in the VMware Carbon Black Cloud**
- Recognize different alert types
- Recognize information that is provided about alerts in VMware Carbon Black Cloud
- Identify ways to respond to and dismiss alerts in VMware Carbon Black Cloud

17 **Using Recommended Queries and Live Response**
- Describe the purpose of using recommended queries in VMware Carbon Black Cloud
- Identify categories of recommended queries
- Describe when and how to use Live Response
- Run recommended queries
- Run a Live Response session

18 **Securing Endpoints with Policies**
- Recognize the purpose of built-in policies
- Recognize how to modify settings on the Policy page in VMware Carbon Black Cloud

19 **Integrating Security**
- Describe the benefits to integrating security solutions
- Identify the integration capabilities of VMware Carbon Black Cloud

Contact

If you have questions or need help registering for this course, click here.