Carbon Black EDR Install, Configure, Manage v7.x

Course Code: 000279

Course Description

This three-day, hands-on training course provides you with the knowledge, skills, and tools to achieve competency in installing, configuring, and managing the VMware Carbon Black® EDR™ environment. This course introduces you to product features, capabilities, and workflows for managing endpoint security. Hands on labs enable learners to reinforce topics by performing operations and tasks within the product in a training environment.

Delivery Method

Instructor-Led

Duration

Three Days

Course Objectives

Upon completion of this course, you will be able to:

- Describe the architecture of a Carbon Black EDR implementation
- Perform the installation, upgrade, and configuration of the Carbon Black EDR server
- Describe the purpose and use of multiple datastores in the server
- Perform live queries across endpoints to gather additional data
- Perform effective searches across the dataset to find security artifacts related to the endpoints
- Manage Threat Intelligence Feeds and Watchlists
- Describe connectors in Carbon Black EDR
- Troubleshoot server and sensor problems
- Analyze data found in the Heads-Up Display
- Manage investigations to group and summarize security incidents and artifacts
- Perform the different response capabilities available to users in Carbon Black EDR
- Use the Carbon Black EDR API to automate tasks

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

Prerequisites

There are no prerequisites for this course

Course Outline

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

Module 2: Planning and Architecture
- Describe the architecture and components of Carbon Black EDR
- Explain single and cluster server requirements
- Identify the communication requirements for Carbon Black EDR

Module 3: Server Installation, Upgrade, and Administration
- Install the Carbon Black EDR server
- Describe the options during the installation process
- Install a Carbon Black EDR sensor
- Confirm data ingestion in the Carbon Black EDR server
- Identify built-in administration tools
- Manage sensor groups
- Manage users and teams

Module 4: Exploring Server Datastores
- Describe the datastores used in Carbon Black EDR
- Interact with the available datastores

Module 5: Performing Live Query
- Describe live query capabilities
- Perform queries across endpoints

Module 6: Searching and Best Practices
- Describe the capabilities and data available in the process search
- Perform process searches to find specific endpoint activity
- Describe the capabilities and data available in the binary search
- Perform binary searches to find application data
- Describe the query syntax and advanced use cases
- Perform advanced queries across the dataset

Module 7: Threat Intelligence Feeds and Watchlists
- Define Threat Intelligence Feeds
- Manage the available Threat Intelligence Feeds
- Describe the use of Watchlists
- Manage Watchlists in the environment

Module 8: Connectors in VMware Carbon Black EDR
- Configure connectors in Carbon Black EDR
- Troubleshoot connectors

Module 9: Troubleshooting VMware Carbon Black EDR
- Identify the available troubleshooting scripts in the Carbon Black EDR server
- Run troubleshooting scripts to identify problems
- Generate a sensor log bundle
- Identify the location of sensor registry keys

Module 10: Head-Up Display Page Overview
- Identify panels relating to endpoint data
- Analyze endpoint data provided by the panels
- Identify panels relating to operations data
- Analyze operations data provided by the panels
- Identify panels relating to server data
- Analyze server data provided by the panels
- Define alert generation in Carbon Black EDR
- Manage alerts

Module 11: Performing Investigations
- Describe investigations
- Explore data used in an investigation
- Manage investigations
- Manage investigation events
- Describe hash banning
- Manage banned hashes

Module 12: Performing Investigations

- Describe isolation in Carbon Black EDR
- Manage isolating endpoints
- Describe live response capabilities
- Manage live response sessions

Module 13: Overview of Postman and the VMware Carbon Black EDR API

- Explain the use of the API
- Differentiate the APIs available for Carbon Black EDR
- Explain the purpose of API tokens
- Create an API token
- Explain the API URL
- Create a valid API request
- Import a collection to Postman
- Initiate an API request from Postman
- Perform operations manually using Postman
- Analyze the use cases for Postman
- Show basic automation tasks using the API and curl
- Compare the usage of curl with Postman