

## EDU-CBCAOT: VMware Carbon Black Cloud: Advanced Operations and Troubleshooting

Course Code: EDU-CBAOT

Duration: 2 days

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### OVERVIEW

#### *Adaptive Prevention delivers Better Protection.*

This two-day, hands-on VMware training course provides you with the advanced knowledge, skills, and tools to achieve competency in performing advanced operations and troubleshooting of VMware Carbon Black Cloud. This course will go into integrating VMware Carbon Black Cloud with other third-party components and utilizing the API and the SDK to automate operations within the product and your security stack.

This course will also enable you to troubleshoot common problems during sensor installation, operations, and within the VMware Carbon Black Cloud console with hands-on lab problems.

### SKILLS COVERED

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

- Describe and determine use cases for integrating with VMware Carbon Black Cloud
- Configure, automate, and troubleshoot the VMware Carbon Black Cloud Syslog Integration
- Use VMware Carbon Black Cloud APIs to pull data with Postman
- Install and use the VMware Carbon Black Cloud Python SDK

- Automate operations using the VMware Carbon Black Cloud SDK and APIs
- Identify and troubleshoot VMware Carbon Black Cloud sensor installations
- Gather troubleshooting data within the browser to remediate or escalate problems
- Identify and resolve sensor usage, networking, and performance problems with the VMware Carbon Black Cloud sensor

### WHO SHOULD ATTEND?

Experienced security administrators and security analysts who are already familiar with VMware Carbon Black Cloud

### PREREQUISITES

Before taking this course, you should have completed the VMware Carbon Black Cloud: Plan and Deploy course.

You should also have the following understanding or knowledge:

- Good understanding of managing and working with various Linux and Windows operating systems
- Knowledge and working experience of security operations

### MODULES

#### Module 1: Course Introduction

- Introductions and course logistics
- Course objectives

**Module 2: VMware Carbon Black Cloud Integrations**

- Describe the integration capabilities with VMware Carbon Black Cloud
- Determine integration use cases for VMware Carbon Black Cloud
- Identify required components for integrating VMware Carbon Black Cloud
- Differentiate VMware Carbon Black Cloud integration vendors

**Module 3: VMware Carbon Black Cloud Syslog Integration**

- Describe the function of the Syslog Connector
- Generate API and SIEM keys from the Cloud console
- Validate a successful Syslog integration
- Describe how to automate the Syslog Connector
- Troubleshoot problems with the Syslog integration

**Module 4: Using Postman**

- Explain the concept and purpose of an API
- Interpret common REST API Status codes
- Recognize the difference between platform and product APIs
- Using the Postman Client to initiate API calls
- Create a custom access level and respective API key
- Create a valid API request

**Module 5: Using the VMware Carbon Black Cloud Python SDK**

- Install the VMware Carbon Black Cloud Python SDK
- Describe the different authentication methods

- Evaluate the best authentication method for a given task

**Module 6: Automating Operations**

- Automate basic Incident Response tasks using the VMware Carbon Black Cloud SDK and API
- Automate basic watchlist interactions using the VMware carbon Black Cloud SDK and API

**Module 7: Sensor Installation Troubleshooting**

- Describe sensor install log collection process
- Identify sensor install log parameters
- Create a detailed sensor install log
- Locate sensor install logs on an endpoint
- Interpret sensor install success from an install log
- Determine likely cause for install failure using sensor logs
- Propose resolution steps for a given sensor install failure

**Module 8: VMware Carbon Black Cloud Console Troubleshooting**

- Identify sensor bypass status reasons
- Simplify console data exports using search
- Describe differences in Audit Log detail levels
- Locate built-in browser tools
- Gather console diagnostics logs from a browser
- Review console diagnostics logs

**Module 9: Sensor Operations Troubleshooting**

- Identify available types of diagnostic logs
- Gather appropriate diagnostic logs for a given issue

- Identify steps for resolving software interoperability problems
- Identify steps for resolving resource problems
- Identify steps for resolving network problems

**END OF PAGE**