vmware EDUCATION SERVICES

VMware Carbon Black EDR Advanced Administrator

Course Overview

This one-day course teaches you how to use the advanced features of the VMware Carbon Black® EDR™ product. This usage includes gaining access to the Linux server for management and troubleshooting in addition to configuring integrations and using the API. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs. This class focuses exclusively on advanced technical topics related to the technical back-end configuration and maintenance.

Course Objectives

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

- Describe the components and capabilities of the Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Identify the architecture for a cluster configuration and Carbon Black EDR cluster communication
- Describe the Carbon Black EDR server data types and data locations
- Use the API to interact with the Carbon Black EDR server without using the UI
- Create custom threat feeds for use in the Carbon Black EDR server
- Perform the integration with a syslog server
- Use different server-side scripts for troubleshooting
- Troubleshoot sensor-side configurations and communication

Target Audience

System administrators and security operations personnel, including analysts and managers

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black EDR Administrator

Course Delivery Options

- Classroom
- Live Online
- Onsite

Product Alignment

- VMware Carbon Black EDR

Course Modules

1 Course Introduction
- Introductions and course logistics
- Course objectives

2 Architecture
- Data flows and channels
- Sizing considerations
- Communication channels and ports

3 Server Datastores
- SOLR database
- Storage configurations and data aging
- Partition states
- Postgres
- Modulestore

4 EDR API
- CBAPI overview
- Viewing API calls in the browser
- Utilizing the API to access data

5 Threat Intelligence Feeds
- Feed structure
- Report indicator types
- Custom threat feed creation and addition

6 Syslog Integration
- SIEM support
- Configuration

7 Troubleshooting
- Server-side scripts
- Server logs
- Sensor operations

Contact

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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMWARE SKU: EDU-VCBEDRAA-OE REV. 3/2020