

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
© 2020 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.