

VMware Carbon Black EDR Administrator

Course Overview

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product and leverage the capabilities to configure and maintain the system according to your organization's security posture and policies.

This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs.

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
- Describe the Carbon Black EDR server installation process
- Manage and configure the Carbon Black EDR sever based on organizational requirements
- Perform searches across process and binary information
- Implement threat intelligence feeds and create watchlists for automated notifications
- Describe the different response capabilities available from the Carbon Black EDR server
- Use investigations to correlate data between multiple processes

Target Audience

System administrators and security operations personnel, including analysts and managers

Prerequisites

There are no prerequisites for this course.

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 **Planning and Architecture**
 - Hardware and software requirements
 - Architecture
 - Data flows
 - Server installation review
 - Installing sensors
- 3 **Server Installation & Administration**
 - Configuration and settings
 - Carbon Black EDR users and groups
- 4 **Process Search and Analysis**
 - Filtering options
 - Creating searches
 - Process analysis and events
- 5 **Binary Search and Banning Binaries**
 - Filtering options
 - Creating searches
 - Hash banning
- 6 **Search best practices**
 - Search operators
 - Advanced queries
- 7 **Threat Intelligence**
 - Enabling alliance feeds
 - Threat reports details
 - Use and functionality
- 8 **Watchlists**
 - Creating watchlists
 - Use and functionality
- 9 **Alerts / Investigations / Response**
 - Using the HUD
 - Alerts workflow
 - Using network isolation
 - Using live response

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.