

# VMware Carbon Black EDR Advanced Analyst

## Course Overview

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product during incident response. Using the SANS PICERL framework, you will configure the server and perform an investigation on a possible incident. This course provides guidance on using Carbon Black EDR capabilities throughout an incident with an in-depth, hands-on, scenario-based lab.

## Course Objectives

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

- Utilize Carbon Black EDR throughout an incident
- Implement a baseline configuration for Carbon Black EDR
- Determine if an alert is a true or false positive
- Fully scope out an attack from moment of compromise
- Describe Carbon Black EDR capabilities available to respond to an incident
- Create additional detection controls to increase security

## Target Audience

Security operations personnel, including analysts and incident responders

## 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 **VMware Carbon Black EDR & Incident Response**
  - Framework identification and process
- 3 **Preparation**
  - Implement the Carbon Black EDR instance according to organizational requirements
- 4 **Identification**
  - Use initial detection mechanisms
  - Process alerts
  - Proactive threat hunting
  - Incident determination
- 5 **Containment**
  - Incident scoping
  - Artifact collection
  - Investigation
- 6 **Eradication**
  - Hash banning
  - Removing artifacts
  - Continuous monitoring
- 7 **Recovery**
  - Rebuilding endpoints
  - Getting to a more secure state
- 8 **Lessons Learned**
  - Tuning Carbon Black EDR
  - Incident close out

## 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](http://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.