 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 addition 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
• On Demand

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.