VMware Carbon Black EDR Advanced Analyst

Price	Duration	Delivery Methods
$925.00	1 Day	VILT, Private Group

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, scenariobased 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

Agenda

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