Course Outline

ProTech Professional Technical Services, Inc.

protechtraining.com

VMware Carbon Black Cloud Enterprise EDR VMCBEDR

Course Summary

Description

This one-day course teaches you how to use the VMware Carbon Black® Cloud Enterprise EDR product and leverage its 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 product through comprehensive coursework and hands-on scenario-based labs.

Objectives

At the end of this course, students will be able to:

- Describe the components and capabilities of VMware Carbon Black Cloud Enterprise EDR
- Identify the architecture and data flows for VMware Carbon Black Cloud Enterprise EDR communication
- Perform searches across endpoint data to discover suspicious behavior
- Manage watchlists to augment the functionality of VMware Carbon Black Cloud Enterprise EDR
- Create custom watchlists to detect suspicious activity in your environment
- Describe the process for responding to alerts in VMware Carbon Black Cloud Enterprise EDR
- Discover malicious activity within VMware Carbon Black Cloud Enterprise EDR
- Describe the different response capabilities available from VMware Carbon Black Cloud

Topics

- Course Introduction
- Data Flows and Communication
- Searching Data
- Managing Watchlists
- Alert Processing
- Threat Hunting in Enterprise EDR
- Response Capabilities

Audience

Security operations personnel, including analysts and managers.

Prerequisites

This course requires completion of the following course: VMware Carbon Black Cloud. Fundamentals

Duration

One day

VMware Carbon Black Cloud Enterprise EDR VMCBEDR

Course Outline

I. Course Introduction

A. Introductions and course logistics
B. Course objectives

II. Data Flows and Communication

A. Hardware and software requirements
B. Architecture
C. Data flows

III. Searching Data

A. Creating searches
B. Search operators
C. Analyzing processes
D. Analyzing binaries
E. Advanced queries

IV. Managing Watchlists

A. Subscribing
B. Alerting
C. Custom watchlists

V. Alert Processing

A. Alert creation
B. Analyzing alert data
C. Alert actions

VI. Threat Hunting in Enterprise EDR

A. Cognitive Attack Loop
B. Malicious behaviors

VII. Response Capabilities

A. Using quarantine
B. Using live response