VMware Carbon Black EDR: Install, Configure, Manage V7.x

VMware Carbon Black EDR: Install, Configure, Manage V7.x

Dieser dreitägige, praxisorientierte Kurs vermittelt Ihnen das Wissen, die Fähigkeiten und die Tools, um die VMware Carbon Black® EDR™-Umgebung kompetent zu installieren, zu konfigurieren und zu verwalten. In diesem Kurs werden Sie mit den Produktfunktionen, Möglichkeiten und Workflows für das Management der Endpunktsicherheit vertraut gemacht. Praktische Übungen ermöglichen es den Teilnehmern, die Themen durch die Durchführung von Operationen und Aufgaben innerhalb des Produkts in einer Schulungsumgebung zu vertiefen.

Kursinhalt
- Course Introduction
- Planning and Architecture
- Server Installation, Upgrade, and Administration
- Exploring Server Datastores
- Performing Live Query
- Searching and Best Practices
- Threat Intelligence Feeds and Watchlists
- Connectors in VMware Carbon Black EDR
- Troubleshooting VMware Carbon Black EDR
- Head-Up Display Page Overview
- Performing Investigations
- Responding to Endpoint Incidents
- Overview of Postman and the VMware Carbon Black EDR API

Die Teilnehmer erhalten englischsprachige Dokumente von Broadcom zum Download als pdf im Kurs.

Zielgruppe
- Sicherheitsanalysten, Bedrohungsjäger oder Incident Responder
- Sicherheitsexperten, die mit Unternehmens- und Endpunktsicherheitstools arbeiten

Voraussetzungen
Es gibt keine Voraussetzungen für diesen Kurs.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**VCIC**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Österreich	**3 Tage**	**€ 2.070,-**
Online Training	**3 Tage**	**€ 2.070,-**
Termine auf Anfrage		

Stand 07.05.2025

VMware by Broadcom

ExperTeach

Inhaltsverzeichnis

VMware Carbon Black EDR: Install, Configure, Manage V7.x

1 Course Introduction
- Introductions and course logistics
- Course objectives

2 Planning and Architecture
- Describe the architecture and components of Carbon Black EDR
- Explain single and cluster server requirements
- Identify the communication requirements for Carbon Black EDR

3 Server Installation, Upgrade, and Administration
- Install the Carbon Black EDR server
- Describe the options during the installation process
- Install a Carbon Black EDR sensor
- Confirm data ingestion in the Carbon Black EDR server
- Identify built-in administration tools
- Manage sensor groups
- Manage users and teams

4 Exploring Server Datastores
- Describe the datastores used in Carbon Black EDR
- Interact with the available datastores

5 Performing Live Query
- Describe live query capabilities
- Perform queries across endpoints

6 Searching and Best Practices
- Describe the capabilities and data available in the process search
- Perform process searches to find specific endpoint activity
- Describe the capabilities and data available in the binary search
- Perform binary searches to find application data
- Describe the query syntax and advanced use cases
- Perform advanced queries across the dataset

7 Threat Intelligence Feeds and Watchlists
- Define Threat Intelligence Feeds
- Manage the available Threat Intelligence Feeds
- Describe the use of Watchlists
- Manage Watchlists in the environment

8 Connectors in VMware Carbon Black EDR
- Configure connectors in Carbon Black EDR
- Troubleshoot connectors

9 Troubleshooting VMware Carbon Black EDR
- Identify the available troubleshooting scripts in the Carbon Black EDR server
- Run troubleshooting scripts to identify problems
- Generate a sensor log bundle
- Identify the location of sensor registry keys

10 Head-Up Display Page Overview
- Identify panels relating to endpoint data
- Analyze endpoint data provided by the panels
- Identify panels relating to operations data
- Analyze operations data provided by the panels
- Identify panels relating to server data
- Analyze server data provided by the panels
- Define alert generation in Carbon Black EDR
- Manage alerts

11 Performing Investigations
- Describe investigations
- Explore data used in an investigation
- Manage investigations
- Manage investigation events

12 Responding to Endpoint Incidents
- Describe isolation in Carbon Black EDR
- Manage isolating endpoints
- Describe live response capabilities
- Manage live response sessions
- Describe hash banning
- Manage banned hashes

13 Overview of Postman and the VMware Carbon Black EDR API
- Explain the use of the API
- Differentiate the APIs available for Carbon Black EDR
- Explain the purpose of API tokens
- Create an API token
- Explain the API URL
- Create a valid API request
- Import a collection to Postman
- Initiate an API request from Postman
- Perform operations manually using Postman
- Analyze the use cases for Postman
- Show basic automation tasks using the API and curl
- Compare the usage of curl with Postman

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at