



VMware Carbon Black Cloud Enterprise EDR

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.

Kursinhalt

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

E-Book Sie erhalten englischsprachige Unterlagen von VMware als E-Book.

Zielgruppe

Security operations personnel, including analysts and managers

Voraussetzungen

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.ch/go/VBED

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 der Schweiz	1 Tag
Online Training	1 Tag CHF 875,-
Termine auf Anfrage	

Stand 27.04.2024



Inhaltsverzeichnis

VMware Carbon Black Cloud Enterprise EDR

1 Course Introduction

- Introductions and course logistics
- Course objectives

2 Data Flows and Communication

- Hardware and software requirements
- Architecture
- Data flows

3 Searching Data

- Creating searches
- Search operators
- Analyzing processes
- Analyzing binaries
- Advanced queries

4 Managing Watchlists

- Subscribing
- Alerting
- Custom watchlists

5 Alert Processing

- Alert creation
- Analyzing alert data
- Alert actions

6 Threat Hunting in Enterprise EDR

- Cognitive Attack Loop
- Malicious behaviors

7 Response Capabilities

- Using quarantine
- Using live response

