Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

VMware Carbon Black EDR Administrator

CODE:	LÄNGE:	PREIS:
VMW_VCBEDRA	8 Hours (1 day)	€690.00

Description

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

Lernziel

By the end of the course, you should be able to meet the following objectives:

- Describe the components and capabilities of the Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Describe the Carbon Black EDR server installation process
- Manage and configure the Carbon Black EDR sever based on organizational requirements
- Perform searches across process and binary information
- Implement threat intelligence feeds and create watchlists for automated notifications
- Describe the different response capabilities available from the Carbon Black EDR server
- Use investigations to correlate data between multiple processes

Zielgruppe

System administrators and security operations personnel, including analysts and managers.

Voraussetzungen

There are no prerequisites for this course.

Inhalt

Course Introduction

- Introductions and course logistics
- Course objectives

Planning and Architecture

- Hardware and software requirements
- Architecture
- Data flows
- Server installation review
- Installing sensors

Server Installation & Administration

- Configuration and settings
- Carbon Black EDR users and groups

Process Search and Analysis

- Filtering options
- Creating searches
- Process analysis and events

Binary Search and Banning Binaries

- Filtering options
- Creating searches
- Hash banning

Search best practices

- Search operators
- Advanced queries

Threat Intelligence

- Enabling alliance feeds
- Threat reports details
- Use and functionality

Watchlists

- Creating watchlists
- Use and functionality

Alerts / Investigations / Response

- Using the HUD
- Alerts workflow
- Using network isolation
- Using live response

Weiterführende Kurse

- VMware Carbon Black EDR Advanced Administrator
- VMware Carbon Black EDR Advanced Analyst

Weitere Informationen

- Dieses Training wird direkt vom/beim Hersteller durchgeführt.
- Dieser Kurs ist nicht rabatt- und prämienprogrammfähig !

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.