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 Advanced Administrator

CODE:	LÄNGE:	PREIS:
VMW_VCBEDRAA	1 Tage	€750.00

Description

This one-day course teaches you how to use the advanced features of the VMware Carbon Black® EDR™ product. This usage includes gaining access to the Linux server for management and troubleshooting in addition to configuring integrations and using the API. This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs. This class focuses exclusively on advanced technical topics related to the technical back-end configuration and maintenance.
Product Alignment

- VMware Carbon Black EDR

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
- Identify the architecture for a cluster configuration and Carbon Black EDR cluster communication
- Describe the Carbon Black EDR server data types and data locations
- Use the API to interact with the Carbon Black EDR server without using the UI
- Create custom threat feeds for use in the Carbon Black EDR server
- Perform the integration with a syslog server
- Use different server-side scripts for troubleshooting
- Troubleshoot sensor-side configurations and communication

Zielgruppe

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

Voraussetzungen

This course requires completion of the following course:

- VMware Carbon Black EDR Administrator

Inhalt

Course Introduction

- Introductions and course logistics
- Course objectives

Architecture

- Data flows and channels
- Sizing considerations
- Communication channels and ports

Server Datastores

- SOLR database
- Storage configurations and data aging
- Partition states
- Postgres
- Modulestore

EDR API

- CBAPI overview
- Viewing API calls in the browser
- Utilizing the API to access data

Threat Intelligence Feeds

- Feed structure
- Report indicator types
- Custom threat feed creation and addition

Syslog Integration

- SIEM support
- Configuration

Troubleshooting

- Server-side scripts
- Server logs
- Sensor operations

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.