



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

CODE:	LÄNGE:	PREIS:
VMW_VCBEDRAAN	8 Hours (1 day)	€750.00

Description

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product during incident response. Using the SANS PICERL framework, you will configure the server and perform an investigation on a possible incident. This course provides guidance on using Carbon Black EDR capabilities throughout an incident with an in-depth, hands-on, scenariobased lab. Product Alignment

- VMware Carbon Black EDR

Lernziel

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

- Utilize Carbon Black EDR throughout an incident
- Implement a baseline configuration for Carbon Black EDR
- Determine if an alert is a true or false positive
- Fully scope out an attack from moment of compromise
- Describe Carbon Black EDR capabilities available to respond to an incident
- Create addition detection controls to increase security

Zielgruppe

Security operations personnel, including analysts and incident responders.

Voraussetzungen

This course requires completion of the following course:

- [VMware Carbon Black EDR Administrator](#)

Inhalt

Course Introduction

- Introductions and course logistics
- Course objectives

VMware Carbon Black EDR & Incident Response

- Framework identification and process

Preparation

- Implement the Carbon Black EDR instance according to organizational requirements

Identification

- Use initial detection mechanisms
- Process alerts

- Proactive threat hunting
- Incident determination

Containment

- Incident scoping
- Artifact collection
- Investigation

Eradication

- Hash banning
- Removing artifacts
- Continuous monitoring

Recovery

- Rebuilding endpoints
- Getting to a more secure state

Lessons Learned

- Tuning Carbon Black EDR
- Incident close out

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.](#)