



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com

Phone: +46 8 555 188 00

CODE:	LENGTH:	PRICE:
VMW_VCBCEEDR	8 Hours (1 day)	kr11,000.00

Description

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.

Objectives

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

- Describe the components and capabilities of VMware Carbon Black Cloud Enterprise EDR
- Identify the architecture and data flows for VMware Carbon Black Cloud Enterprise EDR communication
- Perform searches across endpoint data to discover suspicious behavior
- Manage watchlists to augment the functionality of VMware Carbon Black Cloud Enterprise EDR
- Create custom watchlists to detect suspicious activity in your environment
- Describe the process for responding to alerts in VMware Carbon Black Cloud Enterprise EDR
- Discover malicious activity within VMware Carbon Black Cloud Enterprise EDR
- Describe the different response capabilities available from VMware Carbon Black Cloud

Audience

Security operations personnel, including analysts and managers

Prerequisites

This course requires completion of the following course:

- VMware Carbon Black Cloud Fundamentals

Programme

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

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
26 Apr 2024			English	Self Paced Training		kr7,800.00

Ytterligare information

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)