



Arrow ECS Finland Oy - Education Services

## TRAINING OFFERING

---

**You can reach us at:**

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: [education.ecs.fi@arrow.com](mailto:education.ecs.fi@arrow.com)

Phone: 0870 251 1000



## VMware Carbon Black Portfolio: Configure and Manage

CODE:	LENGTH:	PRICE:
VMW_CBCM	5 day(s)	€3,850.00

### Description

This 5-day course teaches you how to install, configure, and manage the VMware Carbon Black® Portfolio suite of products, which include:

- VMware Carbon Black® App Control™ Administrator
- VMware Carbon Black® EDR™ Administrator
- VMware Carbon Black Cloud Endpoint™ Standard
- VMware Carbon Black® Cloud Audit and Remediation
- VMware Carbon Black® Cloud Enterprise EDR™

You learn how to use the capabilities of the products according to the organization's security posture and organizational policies. This course provides an in-depth, technical understanding of the Carbon Black Portfolio through comprehensive coursework, hands-on labs, and scenario-based exercises.

### Objectives

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

- Describe the components and capabilities of Carbon Black App Control
  - Manage and configure the Carbon Black App Control server based on organizational requirements
  - Create policies to control enforcement levels and agent functionality
  - Implement rules to support the organization's security posture
  - Use the Carbon Black App Control tools to understand agent and server data
  - 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 server 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
  - Describe the components and capabilities of Carbon Black Cloud Endpoint Standard
  - Identify the architecture and data flows for VMware Carbon Black Cloud products
  - Perform searches across endpoint data to discover suspicious behavior
  - Manage the Carbon Black Cloud Endpoint Standard rules based on organizational requirements
  - Configure rules to address common threats
- 
- Evaluate the impact of rules on endpoints
  - Process and respond to alerts
  - Describe the different response capabilities available from VMware Carbon Black Cloud
  - Describe the components and capabilities of Carbon Black Cloud Enterprise EDR
  - Perform searches across endpoint data to discover suspicious behavior
  - Manage watchlists to augment the functionality of Carbon Black Cloud Enterprise EDR
  - Create custom watchlists to detect suspicious activity in your environment
  - Describe the process for responding to alerts in Carbon Black Cloud Enterprise EDR
  - Discover malicious activity within Carbon Black Cloud Enterprise EDR

- • Describe the different response capabilities available from VMware Carbon Black Cloud
- • Describe the components and capabilities of Carbon Black Cloud Audit and Remediation
- • Describe the use case and functionality of recommended queries
- • Achieve a basic knowledge of SQL
- • Describe the elements of a SQL query
- • Evaluate the filtering options for queries
- • Perform basic SQL queries on endpoints
- • Describe the different response capabilities available from VMware Carbon Black Cloud

## Audience

System administrators and security operations personnel (including analysts and managers)

## Prerequisites

System administration experience on Microsoft Windows or Linux operating systems

## Programme

### 1 Course Introduction

- • Introductions and course logistics
- • Course objectives

### 2 VMware Carbon Black App Control Administrator

- • Login Accounts and Groups
- • Policies
- • Computer Details
- • Custom Rules
- • Tools
- • Events
- • Baseline Drift

### 3 VMware Carbon Black EDR

- • Planning and Architecture
- • Server Installation & Administration
- • Process Search and Analysis
- • Binary Search and Banning Binaries
- • Search best practices
- • Threat Intelligence
- • Watchlists
- • Alerts / Investigations / Responses

### 4 VMware Carbon Black Cloud Endpoint Standard

- • Data Flows and Communication
- • Searching Data
- • Policy Components
- • Prevention Capabilities Using Rules
- • Processing Alerts
- • Response Capabilities

### 5 VMware Carbon Black Cloud Enterprise EDR

- • Managing Watchlists
- • Alert Processing
- • Threat Hunting in Enterprise EDR
- • Response Capabilities

### 6 VMware Carbon Black Cloud Audit and Remediation

- • Query Basics
- • Recommended Queries
- • SQL Basics
- • Filtering Results

- • Basic SQL Queries
- • Advanced Search Capabilities
- • Response Capabilities

## Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
29 Sep 2022			English	Self Paced Training		€3,440.00

## Additional Information

This training is also available as onsite training. [Please contact us to find out more.](#)