



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Skontaktuj się z nami

Email: szkolenia.ecs.pl@arrow.com
Phone: 12 616 43 00

VMware Carbon Black Cloud: Advanced Operations and Troubleshooting

Kod: **Czas trwania:** **Cena netto:**

VMW_CBCAOT 16 Hours (2 days) zł4,200.00

Description

This two-day, hands-on training course provides you with the advanced knowledge, skills, and tools to achieve competency in performing advanced operations and troubleshooting of VMware Carbon Black Cloud. This course will go into integrating VMware Carbon Black Cloud with other third-party components and utilizing the API and the SDK to automate operations within the product and your security stack. This course will also enable you to troubleshoot common problems during sensor installation, operations, and within the VMware Carbon Black Cloud console with hands-on lab problems.

Cel szkolenia

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

- Describe and determine use cases for integrating with Carbon Black Cloud
- Configure, automate, and troubleshoot the Carbon Black Cloud Syslog integration
- Use Carbon Black Cloud APIs to pull data with Postman
- Install and use the Carbon Black Cloud Python SDK
- Automate operations using the Carbon Black Cloud SDK and APIs
- Identify and troubleshoot Carbon Black Cloud sensor installations
- Gather troubleshooting data within the browser to remediate or escalate issues
- Identify and resolve sensor usage, networking, and performance issues with the Carbon Black Cloud sensor

Uczestnicy

Experienced security administrators and security analysts who are already familiar with VMware Carbon Black Cloud

Wymagania wstępne

Before taking this course, you should have completed the VMware Carbon Black Cloud: Plan and Deploy course. You should also have the following understanding or knowledge:

- Good understanding of managing and working with various Linux and Windows operating systems
- Knowledge and working experience of security operations

Program szkolenia

- | | |
|---|---|
| 1 Course Introduction | 2 Carbon Black Cloud Integrations |
| • Introductions and course logistics | • Describe the integration capabilities with Carbon Black Cloud |
| • Course objectives | • Determine integration use cases |
| | • Identify required components for integrating Carbon Black Cloud |
| | • Differentiate Carbon Black Cloud integration vendors |
| | 4 Using Postman |
| 3 Carbon Black Cloud Syslog Integration | • Explain the concept and purpose of an API |
| • Describe the function of the Syslog Connector | • Interpret common REST API Status codes |
| • Generate API and SIEM keys from the Cloud console | • Recognize the difference between platform and product APIs |
| • Validate a successful Syslog integration | • Using the Postman Client to initiate API calls |
| • Describe how to automate the Syslog Connector | • Create a custom access level and respective API key |
| • Troubleshoot issues with the Syslog integration | • Create a valid API request |

5 Using the VMware Carbon Black Cloud Python SDK

- Install the VMware Carbon Black Cloud Python SDK
- Describe the different authentication methods
- Evaluate the best authentication method for a given task

6 Automating Operations

- Automate basic Incident Response tasks using the VMware Carbon Black Cloud SDK and API
- Automate basic watchlist interactions using the VMware carbon Black Cloud SDK and API

7 Sensor Installation Troubleshooting

- Describe sensor install log collection process
 - Identify sensor install log parameters
 - Create a detailed sensor install log
 - Locate sensor install logs on an endpoint
 - Interpret sensor install success from an install log
 - Determine likely cause for install failure using sensor logs
 - Propose resolution steps for a given sensor install failure
- 8 VMware Carbon Black Cloud Console Troubleshooting
 - Identify sensor bypass status reasons
 - Simplify console data exports using search
 - Describe differences in Audit Log detail levels
 - Locate built-in browser tools
 - Gather console diagnostics logs from a browser
 - Review console diagnostics logs

9 Sensor Operations Troubleshooting

- Identify available types of diagnostic logs
- Gather appropriate diagnostic logs for a given issue
- Identify steps for resolving software interoperability issues
- Identify steps for resolving resource issues
- Identify steps for resolving network issues

Więcej informacji

Terminy

Na żądanie. [Prosimy o kontakt](#)

Dodatkowe informacje

Jeśli interesują Cię inne szkolenia tego producenta - skontaktuj się z nami.