BROADCOM®

250-602: Carbon Black Cloud Technical Specialist

Exam Study Guide v. 1.0

Exam Description

Candidates can validate technical knowledge and competency by becoming a Certified Technical Specialist based on your specific area of technology expertise. To achieve this level of certification, candidates must pass this proctored exam that is based on a combination of training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Carbon Black Cloud product in an Operations role. This certification exam tests the candidate's knowledge on how to how to install, configure and administer Carbon Black Cloud.

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with Carbon Black Cloud in a production or lab environment.

Study References

Instructor-Led https://www.broadcom.com/support/education/software

Carbon Black Cloud Endpoint Standard (1 Day Instructor-Led)

- Module 1: Course Introduction and Objectives
- Module 2: Data Flows and Communication ▪ Hardware and software requirements ▪ Architecture ▪ Data flows
- Module 3: Searching Data ▪ Creating searches ▪ Analyzing events ▪ Search operators ▪ Advanced queries
- Module 4: Policy Components ▪ Rules ▪ Local scanner ▪ Sensor capabilities
- Module 5: Prevention Capabilities Using Rules ▪ Rule types ▪ Rule creation ▪ Reputation priority ▪ Configuring rules ▪ Evaluating rule impact
- Module 6: Processing Alerts ▪ Alert triage
- Module 7: Response Capabilities ▪ Using quarantine ▪ Using live response ▪ Hash banning

Carbon Black Cloud Audit & Remediation (1 Day Instructor-Led)

- Module 1: Course Introduction and Objectives
- Module 2: Data Flows and Communication ▪ Hardware and software requirements ▪ Architecture
- Module 3: Query Basics ▪ Osquery ▪ Available tables ▪ Query scope ▪ Running versus scheduling
- Module 4: Recommended Queries ▪ Use cases ▪ Inspecting the SQL query
- Module 5: SQL Basics ▪ Components ▪ Tables ▪ Select statements ▪ Where clause ▪ Creating basic queries
- Module 6: Filtering Results ▪ Where clause ▪ Exporting and filtering
- Module 7: Basic SQL Queries ▪ Query creation ▪ Running queries ▪ Viewing results
- Module 8: Advanced Search Capabilities ▪ Advanced SQL options ▪ Threat hunting
- Module 9: Response Capabilities ▪ Using live response

Carbon Black Cloud Enterprise EDR (1 Day Instructor-Led)

- Module 1: Course Introduction and Objectives
- Module 2: Data Flows and Communication ▪ Hardware and software requirements ▪ Architecture ▪ Data flows
- Module 3: Searching Data ▪ Creating searches ▪ Search operators ▪ Analyzing processes ▪ Analyzing binaries ▪ Advanced queries
- Module 4: Managing Watchlists ▪ Subscribing ▪ Alerting ▪ Custom watchlists
- Module 5: Alert Processing ▪ Alert creation ▪ Analyzing alert data ▪ Alert actions
- Module 6: Threat Hunting in Enterprise EDR ▪ Cognitive Attack Loop ▪ Malicious behaviors
- Module 7: Response Capabilities ▪ Using quarantine ▪ Using live response

Carbon Black Cloud Plan and Deploy (1 Day Instructor-Led)

- Module 1: Course Introduction and Objectives
- Module 2: Introduction to Carbon Black Cloud
- Module 3: Managing Carbon Black Cloud Roles and Users
- Module 4: Carbon Black Cloud Sensor Requirements
- Module 5: Preparing for Deployment
- Module 6: Installing Sensors
- Module 7: Deploying Workloads
- Module 8: Managing Sensors
- Module 9: Post-Deployment Validation

Documentation

https://support.broadcom.com/security

- Carbon Black Cloud User Guide <Link>
- Carbon Black Cloud Sensor <Link>
- Carbon Black Cloud Workload <Link>

Product Websites

- **Carbon Black Cloud Landing Page**

Exam Objectives

The following tables list the Certification exam objectives for the exam and how these objectives align to the corresponding course topics and their associated lab exercises as well as the referenced product documentation.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

For more information on the Certification Program, visit
https://www.broadcom.com/support/education/software/certification/all-exams

Carbon Black Cloud Administration

Exam Objectives	Applicable Course Content
Describe the components and capabilities of Carbon Black Cloud Endpoint Standard	**Carbon Black Cloud: Endpoint Standard** • Module 2: Data Flows and Communication • Module 3: Searching Data • Module 6: Processing Alerts • Module 7: Response Capabilities **Carbon Black Cloud: Plan and Deploy** • Module 3: Managing VMware Carbon Black Cloud Roles and Users **Carbon Black Cloud: User Guide**
Manage Carbon Black Cloud roles and users	
Describe the different alert and response capabilities available from Carbon Black Cloud	

Carbon Black Cloud Policies

Exam Objectives	Applicable Course Content
Manage the Carbon Black Cloud rules based on organizational requirements	**Carbon Black Cloud: Endpoint Standard** • Module 4: Policy Components • Module 3: Searching Data **Carbon Black Cloud: Plan and Deploy** • Module 5: Preparing for Deployment **Carbon Black Cloud: User Guide**
Configure rules to address common threats and evaluate the impact of rules on endpoints	

Carbon Black Cloud Sensors

Exam Objectives	Applicable Course Content
Describe the requirements, installation and management of Carbon Black Cloud Sensors	**Carbon Black Cloud: Plan and Deploy** • Module 4: VMware Carbon Black Cloud Sensor Requirements • Module 6: Installing Sensors • Module 8: Managing Sensors • Module 9: Post-Deployment Validation **Carbon Black Cloud Sensor Documentation**

Carbon Black Cloud Live Query

Exam Objectives	Applicable Course Content
Describe the use case and functionality of Live Query	**Carbon Black Cloud Audit and Remediation** • Module 2: Data Flows and Communication • Module 3: Query Basics • Module 4: Recommended Queries

Carbon Black Cloud Enterprise EDR

Exam Objectives	Applicable Course Content
Describe the capabilities and functions of Carbon Black Cloud EEDR.	**Carbon Black Cloud Enterprise EDR** • Module 2: Data Flows and Communication • Module 3: Searching Data • Module 4: Managing Watchlists • Module 6: Threat Hunting in Enterprise EDR

Carbon Black Cloud Workload

Exam Objectives	Applicable Course Content
Describe the capabilities and functions of Carbon Black Cloud Workload.	**Carbon Black Cloud: Plan and Deploy** • Module 7: Deploying Workloads **Carbon Black Cloud Workload: User Guide**

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. **Which of the following features are offered by the Carbon Black Cloud Platform?(Chose 2)**

   A. Real-time endpoint protection
   B. Automated cloud backup
   C. Threat hunting and incident response
   D. Rapid Rules Engine

2. **Carbon Black Cloud can collect data on which of the following?**

   A. Clipboard history
   B. Process Executions
   C. Keyboard inputs
   D. Mouse movements

3. **Which operating systems are supported by Carbon Black Cloud sensors? (Chose 2)**

   A. Windows
   B. Chrome
   C. macOS
   D. Android

4. **How do sensors in Carbon Black Cloud contribute to its security capabilities?**

   A. By encrypting data stored on the endpoint
   B. By monitoring and reporting on endpoint activities
   C. By increasing the network bandwidth for faster data transfer
   D. By physically securing the endpoint device

5. **How can an administrator verify that a Carbon Black Cloud sensor is communicating properly with the cloud?**

   A. Within the Carbon Black Cloud console under the sensor's health status
   B. By checking the sensor's status in the system tray
   C. Reviewing the local event viewer on the endpoint
   D. Sending a test malware file to the endpoint

6. **What effect does changing a policy in VMware Carbon Black Cloud have on associated sensors??**

   A. Updates the sensors' configuration according to the new policy settings
   B. Immediately disconnects the sensors from the network
   C. Requires a manual restart of sensors to apply the new policy
   D. No effect until the sensor is reinstalled

7. **What module within the Carbon Black Cloud platform would gather IT compliance information?**

   A. Live Response
   B. Enterprise EDR
   C. Live Query
   D. Live Remediation

8. **What integration is required for Carbon Black Cloud Workload?**

   A. Vmware vCenter
   B. Hyper-V
   C. Containers
   D. Cloud provider

9. **Which is default Carbon Black Cloud policy?**

   A. Protected
   B. High Enforcement
   C. Standard
   D. Secured

10. **Which is a valid Carbon Black Cloud response action?**

   A. Live Query
   B. Quarentine
   C. Reboot
   D. Upgrade

Sample Exam Answers:

1. A,C
2. B
3. A,C
4. B
5. A
6. A
7. C
8. A
9. C
10. B