vmware EDUCATION SERVICES

5V0-91.20 VMware Carbon Black Portfolio Skills

Exam Details

The VMware Carbon Black Portfolio Skils (5V0-91.20), which leads to VMware Carbon Black EndPoint Protection 2021 is a 60-item exam, with a passing score of 300 using a scaled method. Exam time is 150 minutes.

Exam Delivery

This is a proctored exam delivered through Pearson VUE. For more information, visit the Pearson VUE website.

Certification Information

For details and a complete list of requirements and recommendations for attainment, please reference the VMware Education Services – Certification website.

Minimally Qualified Candidate

The minimally qualified candidate (MQC) has experience with VMware Carbon Black and Is able to administrate and operationalize, manage and configure the product to meet their organization's goals. The MQC also uses the capability of the product and leverages the tool's capabilities to achieve the organization's security goals.

The MQC should have all the knowledge contained in the associated pre-requisite courses and exam sections listed below.

Exam Sections

If a section is missing from the list below, please note it is because the exam has no testable objectives for that section. The objective numbering may be referenced in your score report at the end of your testing event for further preparation should a retake of the exam be necessary.

Section 1 – Introduction – There are no testable objectives for this section

Section 2 - VMware Products and Solutions

- Objective 2.1: Given a scenario about App Control user accounts with privileges, identify how they should be assigned.
- Objective 2.2: Identify the characteristics of enforcement levels in App Control.

Objective 2.3: Given an App Control use case, identify the enforcement level that should be used.

Objective 2.4: Given an App Control use case, identify computers that meet the specified state or condition.

Objective 2.5: Give a scenario about managing an endpoint, identify how to accomplish this with App Control.

Objective 2.6: Given an App Control use case, identify the required rule type that should be used.

Objective 2.7: Given a scenario where alerting is needed, identify the criterion that should be configured in App Control.

Objective 2.8: Given an event in App Control, identify the components, the event type, or the meaning of the event.

Section 3 - VMware Carbon Black EDR

Objective 3.1: Identify the EDR components and dataflows.

Objective 3.2: Given a scenario, identify how to manage and configure EDR Sensor groups.

Objective 3.3: Given a scenario including a search in EDR, identify what is being searched for.

Objective 3.4: Given a scenario including a graphic in EDR, analyze the data given.

Objective 3.5: Identify the characteristic of a binary search and banning binaries in EDR.

Objective 3.6: Identify characteristics that impact search performance in EDR.

Objective 3.7: Identify how and when to use and configure feeds in EDR.

Objective 3.8: Identify how to create and review watchlists I EDR.

Objective 3.9: Given a scenario about an alert, identify the proper response mechanism in EDR.

Section 4 - VMware Carbon Black Cloud Endpoint Standard

Objective 4.1: Identify the communication process and requirements for Sensor to server comms in Endpoint Standard.

Objective 4.2: Given a scenario including a search in Cloud Endpoint including results, analyze the results.

Objective 4.3: Identify characteristics of policy-centered components and sensor options in Cloud Endpoint.

Objective 4.4: Identify the characteristics of permissions and blocking and isolation rules for Cloud Endpoint.

Objective 4.5: Identify the impact of reputation on rules in Cloud Endpoint.

Objective 4.6: Identify the structure of an alert in Cloud Endpoint.

Objective 4.7: Given a scenario about an alert including the investigation and triage pages, identify the components of the alert in Cloud Endpoint.

Objective 4.8: Given a scenario about an alert, identify how to respond using a Cloud Endpoint response option.

Section 5 - VMware Carbon Black Cloud Enterprise EDR

Objective 5.1: Given a scenario including a watchlist, identify the components of the watchlist in Cloud Enterprise EDR.

Objective 5.2: Identify the structure of an alert in Cloud Enterprise EDR.

Objective 5.3: Given a scenario about an alert including the process and binary analysis pages, identify the components of the alert in Cloud Enterprise EDR.

Objective 5.4: Given a scenario about an environment, and an example and a goal, identify the query that should be created to accomplish the goal.

Objective 5.5: Given a scenario about an alert, identify how to respond using a Cloud Enterprise EDR response option.

Section 6 - VMware Carbon Black Cloud Audit and Remediation

Objective 6.1: Identify how to perform basic queries with OSQuery in Cloud Audit and Remediation.

Objective 6.2: Given a query, identify the framework or structure of the query in Cloud Audit and Remediation.

Objective 6.3: Given a query from the UI, identify its function and interpret the results for Cloud Audit and Remediation.

Objective 6.4: Given a scenario about Cloud Audit and Remediation, identify the components in OS query statements.

Objective 6.5: Identify how to exclude data from results using Where statements in Cloud Audit and Remediation.

Objective 6.6: Given a scenario, identify the type of query that should be used for Cloud Audit and Remediation.

Objective 6.7: Given a scenario including the requirement for a specific result, identify how to use Advanced SQL components to achieve the results.

Objective 6.8: Identify Cloud Audit Live Response capabilities, limitations, and features.

Recommended Courses

VMware Carbon Black Portfolio: Configure and Manage

References

http://www.vmware.com

http://kb.vmware.com

https://blogs.vmware.com

https://docs.vmware.com

https://pubs.vmware.com

https://www.vmware.com/techpapers.html

https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=94400

Advanced Search Guide: https://community.carbonblack.com/t5/Carbon-Black-Cloud-Knowledge/Advanced-search-tips-for-Carbon-Black-Cloud-Platform-Search/ta-p/93230?attachment-id=15334

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Endpoint-Detection-and-Response/Ban-Hash-Limit/m-p/20769

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-to-Disable-Enable-Tamper-Protection-on-an-Agent/ta-p/37220

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-Alert-ID-vs-Threat-ID/ta-p/42859

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-Reputation-Priority/ta-p/51797

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/CB-Response-Cloud-How-to-Enable-Live-Response/ta-p/68555

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/CB-Response-How-to-Mark-and-Purge-Inactive-Banned-Hashes-from/ta-p/69732

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/CB-ThreatHunter-How-to-build-a-custom-watchlist-from-the/ta-p/85882

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/CB-ThreatHunter-How-to-subscribe-to-curated-watchlists/ta-p/71974

Carbon Black Knowledge Base: https://community.carbonblack.com/t5/Knowledge-Base/EDR-How-to-upgrade-a-sensor/ta-p/90378

OS Query Read the Docs Page: https://osquery.readthedocs.io/en/stable/introduction/sql/

OS Query Read the Docs Page: https://osquery.readthedocs.io/en/stable/introduction/sql/#your-first-query

Exam Content Contributors

Ben Tedesco
Bob Ekstrom
Christopher Garcia
Jason Lim
John McReynolds
Jon Lymath
Justin Scarpaci
Lauren Harrington
Ryan Hendricks

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

REV. 10/2020