vmware LEARNING

VMware Security Technical Associate

Exam Details (Last Updated: 8/15/2022)

The VMware Security Technical Associate exam (1V0-91.22) which leads to VMware Certified Technical Associate - Security 2023 certification is a 50-item exam, with a passing score of 300 using a scaled method. Candidates are given an appointment time of 120 minutes,which includes adequate time to complete the exam for non-native English speakers. This exam may contain a variety of item types including multiple-choice, multiple-selection multiple-choice, matching, drag-and-drop, and hot area. Additional item types may be used but will appear less frequently than those previously mentioned.

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 candidate can describe and explain endpoint security concepts and can explain VMware Carbon Black Cloud components, features, and capabilities, but occasionally needs to research topics. The candidate can clearly perform navigation of the VMware Carbon Black Cloud user interface and make configuration changes, but occasionally needs to research topics. The candidate occasionally requires assistance or supervision with security related tasks. The candidate occasionally needs to research security related topics. The candidate possesses most, but perhaps not all the knowledge shown in the exam sections (blueprint).

Exam Sections

VMware exam blueprint sections are now standardized to the seven sections below, some of which may NOT be included in the final exam blueprint depending on the exam objectives.

Section 1 – Architecture and Technologies

Section 2 – Products and Solutions

Section 3 – Planning and Designing

Section 4 – Installing, Configuring, and Setup

Section 5 – Performance-tuning, Optimization, and Upgrades

Section 6 – Troubleshooting and Repairing

Section 7 – Administrative and Operational Tasks

If a section does not have testable objectives in this version of the exam, it will be noted below, accordingly. 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.

Sections Included in this Exam

Section 1 – Architectures and Technologies

Objective 1.1 - Define the term cybersecurity

Objective 1.2 - Identify types of cybersecurity vulnerabilities

Objective 1.3 - Recognize attack mitigation strategies

Objective 1.4 - Describe the stages of an attack from the point of view of the attacker

Objective 1.5 - Identify different types of cybersecurity attacks

Objective 1.6 - Identify examples of behaviors associated with security tactics, techniques, and procedures

Objective 1.7 - Identify examples of indicators of compromise

Objective 1.8 - Identify the pillars of a zero-trust approach to security

Objective 1.9 - Describe a defense-in-depth security approach

Objective 1.10 - Identify the functions of basic security controls

Objective 1.11 - Distinguish between antivirus and next-generation antivirus solutions

Objective 1.12 - Explain the purpose of a watchlist

Section 2 – VMware Products and Solutions

Objective 2.1 - Recognize the central concepts in the intrinsic approach to security developed by VMware

Objective 2.2 - Identify the control points in the VMware approach to security

Objective 2.3 - Recognize VMware products that support the implementation of a zero-trust approach to security

Objective 2.4 - Identify features of VMware Carbon Black Cloud solutions

Objective 2.5 - Identify the priority of different reputations in VMware Carbon Black Cloud

Objective 2.6 - Recognize when and how to assign reputations in VMware Carbon Black Cloud

Objective 2.7 - Identify use cases for Carbon Black Cloud Endpoint Standard

Objective 2.8 - Identify use cases for Carbon Black Cloud Audit and Remediation

Objective 2.9 - Identify use cases for Carbon Black Cloud Enterprise EDR

Objective 2.10 - Identify tasks that can be performed in the VMware Carbon Black Cloud console

Objective 2.11 - Describe the term unknown file in the context of VMware Carbon Black Cloud

Objective 2.12 - Describe how cloud analysis helps prevent malware

- Objective 2.13 - Describe how to remove malware from endpoints
- Objective 2.14 - Describe when and how to use the Inbox in the VMware Carbon Black Cloud console
- Objective 2.15 - Describe when and how to use audit logs in the VMware Carbon Black Cloud console
- Objective 2.16 - Determine the appropriate VMware Carbon Black Cloud sensor installation method for given use cases
- Objective 2.17 - Recognize the steps for performing an attended installation of a VMware Carbon Black Cloud sensor
- Objective 2.18 - Recognize the steps for performing an unattended installation of a VMware Carbon Black Cloud sensor
- Objective 2.19 - Identify types of data collected in VMware Carbon Black Cloud
- Objective 2.20 - Recognize the search capabilities in VMware Carbon Black Cloud
- Objective 2.21 - Describe the use cases for watchlists in VMware Carbon Black Cloud
- Objective 2.22 - Recognize different alert types
- Objective 2.23 - Identify ways to respond to and dismiss alerts in VMware Carbon Black Cloud
- Objective 2.24 - Describe the purpose of using recommended queries in VMware Carbon Black Cloud
- Objective 2.25 - Identify categories of recommended queries
- Objective 2.26 - Describe when and how to use Live Response
- Objective 2.27 - Recognize the purpose of built-in policies
- Objective 2.28 - Recognize how to modify settings on the Policy page in VMware Carbon Black Cloud
- Objective 2.29 - Describe the benefits to integrating security solutions
- Objective 2.30 - Identify the integration capabilities of VMware Carbon Black Cloud

Section 3 – Not Applicable

Section 4 – Not Applicable

Section 5 – Not Applicable

Section 6 – Not Applicable

Section 7 – Not Applicable

Courses used to develop this exam and strongly recommended to you for exam preparation:

VMware Endpoint Security: Core Technical Skills

Certification

VMware Certified Technical Associate - Security 2023

References

No additional references

Exam Content Contributors

Allan Solomon
Brett Ford
Cian Muldoon
Isabella Rocha
Joe Thoming
Tom Houpt
Kevin Evans
Ryan Hendricks