Number: 5V0-93.22
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 5V0-93.22

Exam Name: VMware Carbon Black Cloud Endpoint Standard Skills

Exam A

QUESTION 1
An administrator has determined that the following rule was the cause for an unexpected block:
[Suspected malware] [Invokes a command interpreter] [Terminate process]
All reputations for the process which was blocked show SUSPECT_MALWARE.
Which reputation was used by the sensor for the decision to terminate the process?

A. Initial Cloud reputation
B. Actioned reputation
C. Current Cloud reputation
D. Effective reputation

Correct Answer: D
Section:

QUESTION 2
What is a capability of VMware Carbon Black Cloud?

A. Continuous and decentralized recording
B. Attack chain visualization and search
C. Real-time view of attackers
D. Automation via closed SOAP APIs

Correct Answer: B
Section:

QUESTION 3
A security administrator needs to remediate a security vulnerability that may affect the sensors. The administrator decides to use a tool that can provide interaction and remote access for further investigation.
Which tool is being used by the administrator?

A. CBLauncher
B. Live Response
C. PowerCLI
D. IRepCLI

Correct Answer: B
Section:

QUESTION 4
A security administrator notices an unusual software behavior on an endpoint. The administrator immediately used the search query to collect data and start analyzing indicators to find the solution.
What is a pre-requisite step in gathering specific vulnerability data to export it as a CSV file for analysis?

A. Perform a custom search on the Endpoint Page.

B. Access the Audit Log content to see associated events.
C. Search for specific malware by hash or filename.
D. Enable cloud analysis.

Correct Answer: A
Section:

QUESTION 5
A VMware Carbon Black managed endpoint is showing up as an inactive device in the console.
What is the threshold, in days, before a machine shows as inactive?

A. 7 days
B. 90 days
C. 60 days
D. 30 days

Correct Answer: D
Section:

QUESTION 6
Which statement is true regarding Blocking/Isolation rules and Permission rules?

A. Blocking & Isolation rules are overridden by Upload Rules.
B. Permission Rules are overridden by Blocking & Isolation rules
C. Upload Rules are overridden by Blocking & Isolation rules.
D. Blocking & Isolation rules are overridden by Permission Rules

Correct Answer: B
Section:

QUESTION 7
The VMware Carbon Black Cloud Sensor is not able to establish connectivity to the VMware Carbon Black Cloud Content Management URL over the standard SSL port TCP/443.
Which port, if any, will be the tailback?

A. TCP/54443
B. TCP/80
C. TCP/8443
D. It will not fallback and fail.

Correct Answer: C
Section:

QUESTION 8
An administrator has been tasked with preventing the use of unauthorized USB storage devices from being used in the environment.
Which item needs to be enabled in order to enforce this requirement?

A. Enable the Block access to all unapproved USB devices within the policies option.

B. Choose to disable USB device access on each endpoint from the Inventory page.
C. Select the option to block USB devices from the Reputation page.
D. Elect to approve only allowed USB devices from the USB Devices page.

Correct Answer: A
Section:

QUESTION 9
An administrator needs to create a search, but it must exclude 'system.exe'.
How should this task be completed?

A. #process_name:system.exe
B. *process_name:system.exe
C. -process_name:system.exe

Correct Answer: C
Section:

QUESTION 10
An administrator needs to use an ID to search and investigate security incidents in Carbon Black Cloud.
Which three IDs may be used for this purpose? (Choose three.)

A. Threat
B. Hash
C. Sensor
D. Event
E. User
F. Alert

Correct Answer: B, D, F
Section:

QUESTION 11
Which VMware Carbon Black Cloud integration is supported for SIEM?

A. SolarWinds
B. LogRhythm
C. Splunk App
D. Datadog

Correct Answer: C
Section:

QUESTION 12
What connectivity is required for VMware Carbon Black Cloud Endpoint Standard to perform Sensor Certificate Validation?

A. TCP/443 to GoDaddy OCSP and CRL URLs (crl.godaddy.com and ocsp.godaddy.com)

B. TCP/80 to GoDaddy OCSP and CRL URLs (crl.godaddy.com and ocsp.godaddy.com)
C. TCP/443 to GoDaddy CRL URL (crl.godaddy.com and ocsp.godaddy.com)
D. TCP/80 to GoDaddy CRL URL (crl.godaddy.com and ocsp.godaddy.com)

Correct Answer: A
Section:

QUESTION 13
An administrator wants to block an application by its path instead of reputation. The following steps have already been taken:
Go to Enforce > Policies > Select the desired policy >
Which additional steps must be taken to complete the task?

A. Click Enforce > Add application path name
B. Scroll down to the Permissions section > Click Add application path > Enter the path of the desired application
C. Scroll down to the Blocking and Isolation section > Click Edit (pencil icon) for the desired Reputation
D. Scroll down to the Blocking and Isolation section > Click Add application path > Enter the path of the desired application

Correct Answer: D
Section:

QUESTION 14
An administrator is investigating an alert and reads a summary that says:
The application powershell.exe was leveraged to make a potentially malicious network connection.
Which action should the administrator take immediately to block that connection?

A. Click Delete Application
B. Click Quarantine Asset
C. Click Export Alert
D. Click Drop Connection

Correct Answer: D
Section:

QUESTION 15
Which command is used to immediately terminate a current Live Response session?

A. kill
B. detach -q
C. delete
D. execfg

Correct Answer: B
Section:

QUESTION 16
A user downloaded and executed malware on a system. The malware is actively exfiltrating data.
Which immediate action is recommended to prevent further exfiltration?

A. Check Security Advisories and Threat Research contents.
B. Place the device in quarantine.
C. Run a background scan.
D. Request upload of the file for analysis.

Correct Answer: B
Section:

QUESTION 17
What are the highest and lowest file reputation priorities, respectively, in VMware Carbon Black Cloud?

A. Priority 1: Ignore, Priority 11: Unknown
B. Priority 1: Unknown, Priority 11: Ignore
C. Priority 1: Known Malware, Priority 11: Common White
D. Priority 1: Company Allowed, Priority 11: Not Listed/Adaptive White

Correct Answer: A
Section:

QUESTION 18
An administrator wants to find information about real-world prevention rules that can be used in VMware Carbon Black Cloud Endpoint Standard.
How can the administrator obtain this information?

A. Refer to an external report from other security vendors to obtain solutions.
B. Refer to the TAU-TIN's on the VMware Carbon Black community page.
C. Refer to the VMware Carbon Black Cloud sensor install guide.
D. Refer to VMware Carbon Black Cloud user guide.

Correct Answer: B
Section:

QUESTION 19
Is it possible to search for unsigned files in the console?

A. Yes, by using the search: NOT process_publisher_state:FILE_SIGNATURE_STATE_SIGNED
B. No, it is not possible to return a query for unsigned files.
C. Yes, by using the search: process_publisher_state:FILE_SIGNATURE_STATE_UNSIGNED
D. Yes, by looking at signed and unsigned executables in the environment and seeing if another difference can be found, thus locating unsigned files in the environment.

Correct Answer: C
Section:

QUESTION 20
The administrator has configured a permission rule with the following options selected:
Application at path: C:\Program Files**
Operation Attempt: Performs any operation

Action: Bypass
What is the impact, if any, of using the wildcards in the application at path field?

A. Executable files in the 'Program Files' directory and subdirectories will be ignored.
B. Executable files in the 'Program Files' directory will be blocked.
C. Executable files in the 'Program Files' directory will be logged.
D. Executable files in the 'Program Files' directory will be subject to blocking rules.

Correct Answer: A
Section:

QUESTION 21
A script-based attack has been identified that inflicted damage to the corporate systems. The security administrator found out that the malware was coded into Excel VBA and would like to perform a search to further inspect the incident.
Where in the VMware Carbon Black Cloud Endpoint Standard console can this action be completed?

A. Endpoints
B. Settings
C. Investigate
D. Alerts

Correct Answer: C
Section:

QUESTION 22
An administrator would like to proactively know that something may get blocked when putting a policy rule in the environment.
How can this information be obtained?

A. Search the data using the test rule functionality.
B. Examine log files to see what would be impacted
C. Put the rules in and see what happens to the endpoints.
D. Determine what would happen based on previously used antivirus software

Correct Answer: A
Section:

QUESTION 23
An administrator has just placed an endpoint into bypass.
What type of protection, if any, will VMware Carbon Black provide this device?

A. VMware Carbon Black will be uninstalled from the endpoint.
B. VMware Carbon Black will place the machine in quarantine.
C. VMware Carbon Black will not provide any protection to the endpoint.
D. VMware Carbon Black will apply policy rules.

Correct Answer: C
Section:

QUESTION 24
A security administrator needs to review the Live Response activities and commands that have been executed while performing a remediation process to the sensors.
Where can the administrator view this information in the console?

A. Users
B. Audit Log
C. Notifications
D. Inbox

Correct Answer: B
Section:

QUESTION 25
Which statement accurately characterizes Alerts that are categorized as a 'Threat' versus those categorized as 'Observed'?

A. 'Threat' indicates an ongoing attack. 'Observed' indicates the attack is over and is being watched.
B. 'Threat' indicates a more likely malicious event. 'Observed' are less likely to be malicious.
C. 'Threat' indicates a block (Deny or Terminate) has occurred. 'Observed' indicates that there is no block.
D. 'Threat' indicates that no block (Deny or Terminate) has occurred. 'Observed' indicates a block.

Correct Answer: B
Section:

QUESTION 26
An administrator is working in a development environment that has a policy rule applied and notices that there are too many blocks. The administrator takes action on the policy rule to troubleshoot the issue until the blocks are fixed.
Which action should the administrator take?

A. Unenforce
B. Disable
C. Recall
D. Delete

Correct Answer: B
Section:

QUESTION 27
An organization has the following requirements for allowing application.exe:
For example, on one user's machine, the path is C:\Users\Lorie\Temp\Allowed\application.exe.
Which path meets this criteria using wildcards?

A. C:\Users\?\Temp\Allowed\application.exe
B. C:\Users*\Temp\Allowed\application.exe
C. *:\Users**\Temp\Allowed\application.exe
D. *:\Users*\Temp\Allowed\application.exe

Correct Answer: B

Section:

QUESTION 28
The use of leading wildcards in a query is not recommended unless absolutely necessary because they carry a significant performance penalty for the search.
What is an example of a leading wildcard?

A. filemod:system32/ntdll.dll
B. filemod:system32/*ntdll.dll
C. filemod:*/system32/ntdll.dll
D. filemod:system32/ntdll.dll*

Correct Answer: C
Section:

QUESTION 29
Where can a user identify whether a sensor's signature pack is out-of-date in VMware Carbon Black Cloud?

A. Enforce > Investigate > Sensors > Details
B. Enforce > Inventory > Endpoints > Policy
C. Inventory > Endpoints > Sensor Update Status
D. Inventory > Endpoints > Device Name

Correct Answer: C
Section:

QUESTION 30
A security administrator is tasked to investigate an alert about a suspicious running process trying to modify a system registry.
Which components can be checked to further inspect the cause of the alert?

A. Command lines. Device ID, and priority score
B. Event details, command lines, and TTPs involved
C. TTPs involved, network connections, and child path
D. Priority score, file reputation, and timestamp

Correct Answer: B
Section:

QUESTION 31
An administrator wants to be notified when particular Tactics, Techniques, or Procedures (TTPs) are observed on a managed endpoint.
Which notification option must the administrator configure to receive this notification?

A. Alert that crosses a threshold with the 'observed' option selected
B. Alert that includes specific TTPs
C. Alert for a Watchlist hit
D. Policy action that is enforced with the 'deny' opt ion selected

Correct Answer: C

Section:

QUESTION 32
An administrator needs to configure a policy for macOS and Linux Sensors, not enabling settings which are only applicable to Windows.
Which three settings are only applicable to Sensors on the Windows operating system? (Choose three.)

A. Delay execute for cloud scan
B. Allow user to disable protection
C. Submit unknown binaries for analysis
D. Expedited background scan
E. Scan execute on network drives
F. Require code to uninstall sensor

Correct Answer: A, E, F
Section:

QUESTION 33
An administrator has configured a terminate rule to prevent an application from running. The administrator wants to confirm that the new rule would have prevented a previous execution that had been observed.
Which feature should the administrator leverage for this purpose?

A. Setup a notification based on a policy action, and then select Terminate.
B. Utilize the Test rule link from within the rule.
C. Configure the rule to terminate the process.
D. Configure the rule to deny operation of the process.

Correct Answer: B
Section: