

VMware.5V0-91.20.v2022-05-09.q46

Exam Code:	5V0-91.20
Exam Name:	VMware Carbon Black Portfolio Skills
Certification Provider:	VMware
Free Question Number:	46
Version:	v2022-05-09
# of views:	1085
# of Questions views:	460
https://www.exam-tests.com/5V0-91.20-exam/VMware.5V0-91.20.v2022-05-09.q46.html	

NEW QUESTION: 1

An administrator needs to manage a group of sensors from within the console.

Which three actions are available for sensors within the Sensor Group? (Choose three.)

- A. Restart
- B. Move to group
- C. Disable
- D. Share Settings
- E. Uninstall
- F. Ban

Answer: A,B,E ([LEAVE A REPLY](#))

NEW QUESTION: 2

How can an analyst disregard alerts on multiple devices with the least amount of administrative effort?

- A. Select the "Dismiss on all devices" option.
- B. Make a note in the Notes/Tags option.
- C. Search by hash and dismiss.
- D. Turn off the Group Alerts option.

Answer: D ([LEAVE A REPLY](#))

Reference:

sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjv6pryl4XvAhWagVwKHTCMDTEQFjAAegQIARAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Ft5%2FKnowledge-Base%2FCarbon-Black-Cloud-How-to-Dismiss-Alerts%2Fta-p%2F51766&usq=AOvVaw2x1mST1tWpuASUMLmFhyul (80)

NEW QUESTION: 3

An administrator is interested in upgrading endpoints to the latest release in VMware Carbon Black App Control (V8.1.4+).

What is the first step to make a new agent available for installation or upgrade?

- A. Download from the Carbon Black User Exchange
- B. Download from the Carbon Black Cloud Back End
- C. Download from the Carbon Black App Control Server
- D. Download from the Carbon Black Software Reputation Service (SRS)

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 4

Level 3 service desk personnel have been approved to modify computer enforcement levels by security governance.

Which set of steps is required to implement this change?

- A. Create new user role, map AD group to role, assign permission "Manage computers" to role.
- B. Create new user role, map AD group to role, assign permission "Temporary assign computers" to role.
- C. Assign permission "Temporary assign computers" to each user.
- D. Create new user role, assign permission "Manage computers" to role.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 5

An administrator needs to check configurations using Audit across several policies and locations within the organization.

How can the administrator run the query to only these specific devices?

- A. Specify the policy for the endpoints on the query, and then type the sensor name into the text box, selecting the devices. Repeat as necessary for all devices.
- B. Specify endpoints on the query by typing the sensor name into the text box, selecting the device. Repeat as necessary for all devices.
- C. Specify endpoints on the query by selecting the check box for each device.
- D. Specify the policy for the endpoints on the query, and then select the check box for each device.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 6

Carbon Black App Control maintains an inventory of all interesting (executable) files on endpoints where the agent is installed.

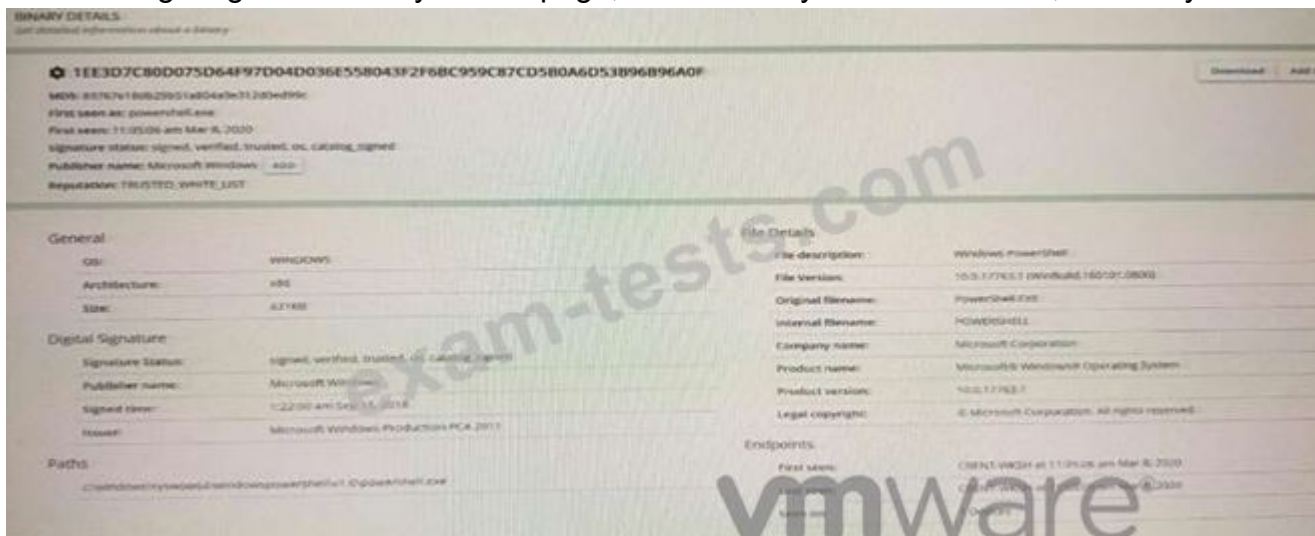
What is the initial inventory procedure called, and how can this process be triggered?

- A. Discovery; place agent into Disabled mode
- B. Baselining; install the agent
- C. Inventorying; enable Discovery mode
- D. Initialization; move agent out of Disabled mode

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

An analyst is investigating an alert within Enterprise EDR. The alert is tied to an unusual process name. When navigating to the binary details page, for the binary used in the alert, the analyst sees the following:



The analyst wants to find any instances of this process executing regardless of the process name used. Which two details from the binary can be used to search for the application regardless of the seen name? (Choose two.)

- A. The path
- B. The product version
- C. The binary's hash
- D. The original filename
- E. The publisher name

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 8

What is the meaning, if any, of the event Report write (removable media)?

- A. This event would never occur. App Control does not report activity on removable media.
- B. A Policy's device control setting 'Block writes to unapproved removable media' is set to Enabled. The event details show the process, file name, and hash modified or deleted on the removable media.
- C. A Policy's device control setting 'Block writes to unapproved removable media' is set to Report Only. The event details show the process and file name modified or deleted on the unapproved removable media.
- D. A Policy's device control setting 'Block writes to unapproved removable media' is set to Report Only. The event details show the process, file name, and hash modified or deleted on the removable media.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 9

An administrator viewed and filtered the results of a completed query within the User Interface for Audit and Remediation. The administrator exported the results to create charts and other visuals for reporting. When viewing the exported results, the administrator noticed some results were missing from the data set.

Why did the administrator not have the full data set from the query?

- A. Export applies to the data visible in the UI; filtering will impact the viewable data.
- B. Export is limited to the first hundred rows, and the query had more rows than supported.

- C. Export was used prior to the query completing, and some data is missing.
- D. Export pulls all results; the query must not have covered all data required.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

A Carbon Black Cloud Endpoint Standard analyst is testing different search operator combinations. Which two queries produce the same result? (Choose two.)

- A. process_name:chrome.exe netconn_domain:google.com
- B. process_name:chrome.exe AND NOT netconn_domain:google.com
- C. process_name:chrome.exe OR netconn_domain:google.com
- D. process_name:chrome.exe OR NOT netconn_domain:google.com
- E. process_name:chrome.exe NOT netconn_domain:google.com

Answer: D,E ([LEAVE A REPLY](#))

NEW QUESTION: 11

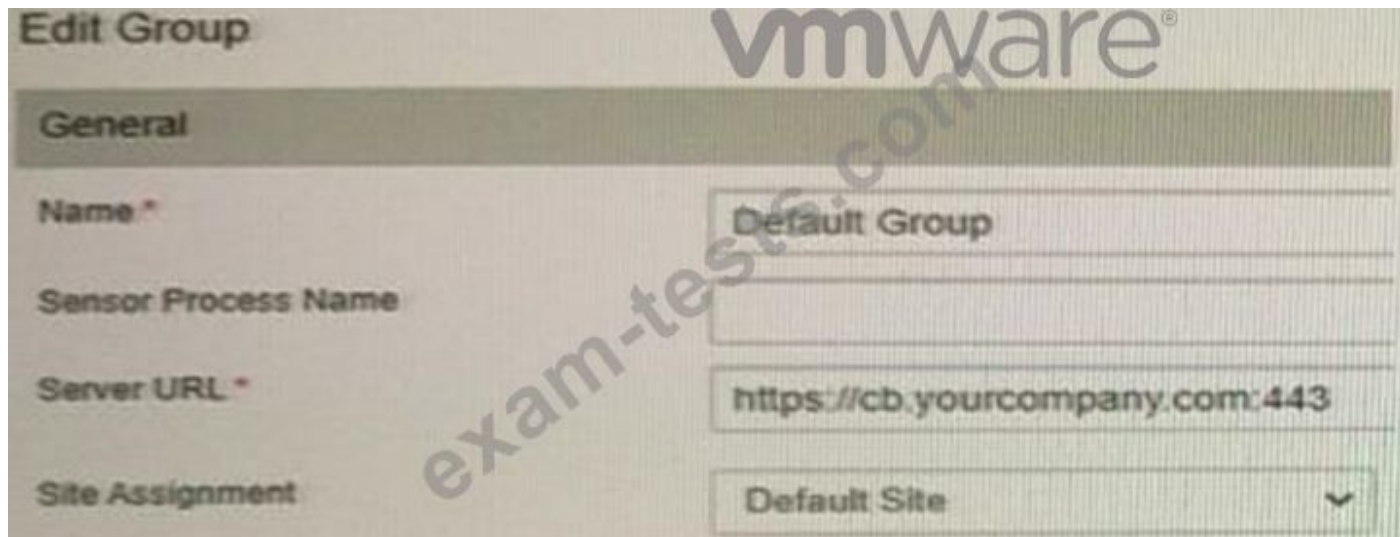
After an emergency, what does the Restore computer button do on the App Control Home page?

- A. Move all computers to Medium Enforcement level
- B. Move all computers to Low Enforcement level
- C. Move all computers to High Enforcement level
- D. Move all computers to the original Enforcement level

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

Refer to the exhibit:



Which two statements are true about Carbon Black Live Response (CBLR)? (Choose two.)

- A. CBLR is disabled.
- B. CBLR is enabled.
- C. A CBLR session is established.
- D. A CBLR session already exists.
- E. A CBLR session is not attached.

Answer: D,E ([LEAVE A REPLY](#))

NEW QUESTION: 13

A process wrote an executable file as detailed in the following event:

Timestamp: Jan 10, 2020 16:40:32	Source: USWIN-MGMT2	Subtype: New Unapproved File To
Computer:	File Path: c:\windows\temp	File Name: sysmgmtask.vbs
Process: c:\program files\sysmgr\sysmgr.exe	User: Local System	

Which rule type should be used to ensure that files of the same name and path, written by that process in the future, will not be blocked when they execute?

- A. Advances (Write-Ignore)
- B. File Creation Control
- C. Trusted Path
- D. Trusted Publisher

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

An administrator is creating a query per policy for Audit and Remediation. The administrator ran several recommended queries already but notices they are unable to run the same recommended query for one of their policies. The run button is grayed out.

Which statement correctly explains why the run button is unavailable?

- A. The sensors in the policy do not support the table or query.
- B. The query or table is not supported within osquery.
- C. The administrator needs the use live query permission.
- D. The number of consecutive running queries is limited.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 15

An administrator is concerned that someone may be using unauthorized commands from cmd.exe. These commands are not considered suspicious or malicious, and there is no policy based around them.

Which page should the administrator use to find these commands?

- A. Investigate
- B. Alerts
- C. Sensor Management
- D. Policies

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 16

App Control System Health email alerts for excessive agent backlog are occurring hourly. This is overwhelming the analysts, and they would like to reduce the notifications.

How can the analyst reduce the unneeded alerts?

- A. Set the email address for subscribers to an invalid email.

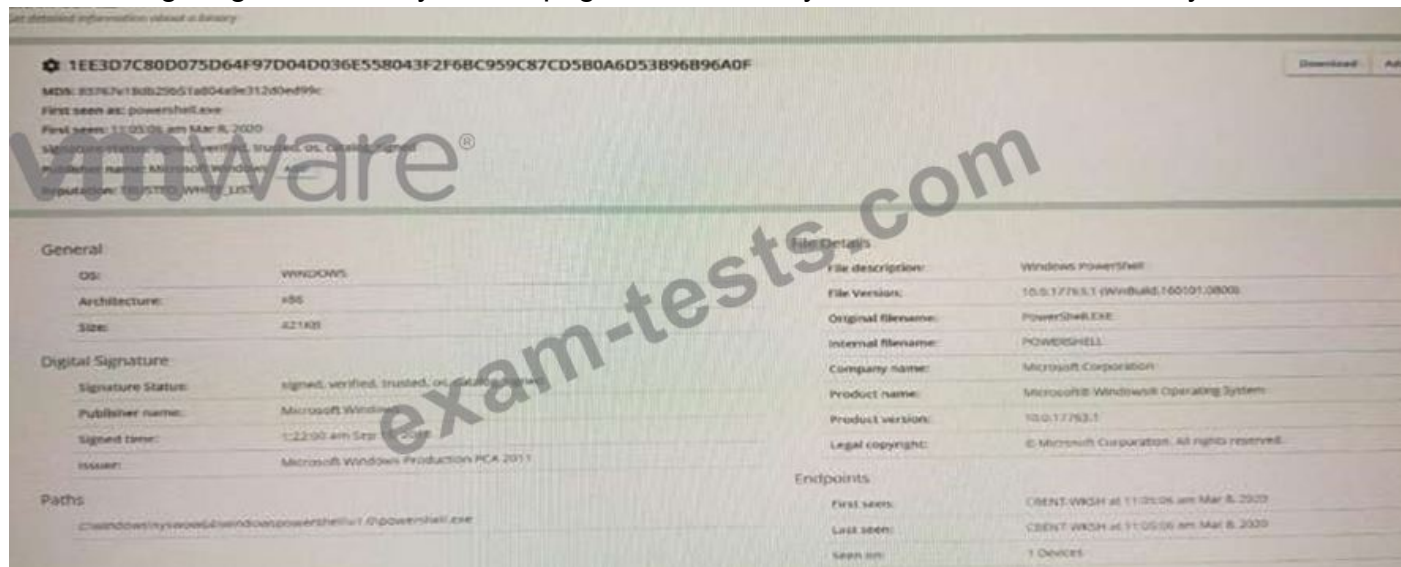
- B. Change reminder email to daily or disabled.
- C. Delete the alert.
- D. Disable the alert.

Answer: ([SHOW ANSWER](#))

Valid 5V0-91.20 Dumps shared by BraindumpsPass.com for Helping Passing 5V0-91.20 Exam! BraindumpsPass.com now offer the **newest 5V0-91.20 exam dumps**, the BraindumpsPass.com 5V0-91.20 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 5V0-91.20 dumps with Test Engine here:
<https://www.braindumpsPass.com/VMware/5V0-91.20-practice-exam-dumps.html> (115 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17

An analyst is investigating an alert within Enterprise EDR. The alert is tied to an unusual process name. When navigating to the binary details page, for the binary used in the alert, the analyst sees the following:



The analyst wants to find any instances of this process executing regardless of the process name used. Which two details from the binary can be used to search for the application regardless of the seen name? (Choose two.)

- A. The product version
- B. The original filename
- C. The path
- D. The publisher name
- E. The binary's hash

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

Which Sensor Status under Endpoint Health indicates that a system's policy enforcement is disabled, and the sensor is not sending security event data to the cloud?

- A. Quarantined
- B. Deregistered
- C. Inactive
- D. Bypass

Answer: (SHOW ANSWER)

Reference:

Bypass-has-been-Enabled-on-the/ta-p/74905

NEW QUESTION: 19

Which two statements are true regarding Live Response? (Choose two.)

- A. Live Response opens an SSH session with the remote device.
- B. Live Response requires both view and manage permissions to use.
- C. Live Response utilizes the same channel for sensor-server communications.
- D. Live Response supports one user per session on an endpoint.
- E. Live Response can only be initiated through the user interface.

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 20

Which strategy should be used to purge inactive bans from the web console?

- A. Run the cbbanning script on the EDR server
- B. Use a pre-configured system cron job daily to remove them
- C. Go to the hashes page on the web console and remove them
- D. Schedule an add-hoc cron job to remove

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

How long will Live Queries in Carbon Black Audit and Remediation run before timing out?

- A. 14 days
- B. 30 days
- C. 180 days
- D. 7 days

Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

Which identifier is shared by all events when an alert is investigated?

- A. Priority Score
- B. Event ID
- C. Process ID
- D. Alert ID

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 23

An Enterprise EDR administrator is reviewing the Investigate page and believes they are receiving false positive hits from specific watchlist.

Which three options reduce future false positive hits from this watchlist? (Choose three.)

- A. Modify policy rules to exclude the false positive directory.
- B. Disable/remove the report associated with the false positives.
- C. Dismiss the watchlist hit.
- D. Disable the watchlist associated with the false positives.
- E. Select edit watchlist and uncheck alert on hits.
- F. Disable/remove the IOC associated with the false positives.

Answer: B,E,F ([LEAVE A REPLY](#))

NEW QUESTION: 24

An analyst has investigated multiple alerts on a number of HR workstations and found that java.exe is attempting to PowerShell. Of the Windows workstations in question, the analyst has also found that Java is installed in multiple locations. The analyst needs to block java.exe from this type of operation.

Which rule meets this need?

- A. **/Program Files/*/java.exe-> Invokes an untrusted process -> Deny operation
- B. **/java.exe -> Invokes an untrusted process -> Terminate process
- C. **\Program Files*java.exe -> Invokes a command interpreter -> Terminate process
- D. **\java.exe -> Invokes a command interpreter -> Deny operation

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 25

What information does the Alert Details panel provide on the Alert Triage page in Endpoint Standard?

- A. Device ID
- B. Alert ID
- C. Threat ID
- D. Process ID

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 26

Which ID in Endpoint Standard is associated with one specific action, involves up to three different hashes (Parent, Process, Target), and occurs on a single device at a specific time?

- A. Alert ID
- B. Process ID
- C. Event ID
- D. Threat ID

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 27

Which strategy is used to create an exclusion in Endpoint Standard for another AV/security product?

- A. Bypass Mode
- B. Permission Rule
- C. Isolation Rule
- D. Approved List

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 28

The security operations group is complaining that they are getting multiple App Control alerts for specific malicious files after they have banned the file.

Which step is necessary to prevent future alerts on these files?

- A. Disable the Reminder Mail.
- B. Edit the Malicious File Detected Alert. Select the criteria: Ignore already banned files and Ignore already approved files.
- C. Edit the Malicious File Detected Alert. Select the criteria: Ignore already banned files.
- D. Set the Alert Status to Disabled.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 29

Management has directed that the SOC team be enabled to create global file bans via the App Control API. How would this be configured in the App Control Console?

- A. Create a Role, map to the corresponding SOC group, add permission "Manage files", and create API token for the Role.
- B. Create a Role, map to corresponding SOC group, and add permission "Manage files" to Role.
- C. Add permission "Manage files" and create an API token for each SOC user.
- D. Create a Role, map it to the corresponding SOC group, add permission "Manage files" to Role, and create an API token for each user in group.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 30

Refer to the exhibit:

Which two statements are true about Carbon Black Live Response (CBLR)? (Choose two.)

- A. CBLR is enabled.
- B. A CBLR session is not attached.
- C. A CBLR session already exists.
- D. A CBLR session is established.
- E. CBLR is disabled.

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 31

Which wildcard configuration applies a policy to all files and subfolders in a specific folder in Endpoint Standard?

- A. C:\Program Files\example\\$\$
- B. C:\Program Files\example*
- C. C:\Program Files\example\\$
- D. C:\Program Files\example**

Answer: D ([LEAVE A REPLY](#))

Valid 5V0-91.20 Dumps shared by BraindumpsPass.com for Helping Passing 5V0-91.20 Exam! BraindumpsPass.com now offer the **newest 5V0-91.20 exam dumps**, the BraindumpsPass.com 5V0-91.20 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 5V0-91.20 dumps with Test Engine here:
<https://www.braindumpsPass.com/VMware/5V0-91.20-practice-exam-dumps.html> (115 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32

What does the Aggressive setting do when configured in Local Scan Settings?

- A. It enables signature updates for the scanner.
- B. It scans new files on first execution.
- C. It scans all files on execution.
- D. It adds a temporary reputation.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 33

A security policy states to enable Live Response by default across the enterprise. However, the team identified critical systems which should not support Live Response due to risk. The team needs to disable Live Response on selected systems.

From which page can this goal be accomplished?

- A. API Access
- B. Roles
- C. Policy
- D. Endpoints

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 34

Given the following query:

```
SELECT * FROM users WHERE UID >= 500;
```

Which statement is correct?

- A. This query filters results sent to the cloud.
- B. This query returns all accounts found on systems.
- C. This query limits the number of columns to display in the results.
- D. This query is missing a parameter for validity.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

An organization leverages a commonly used software distribution tool to manage deployment of enterprise software and updates. Custom rules are a suitable option to ensure the approval of files delivered by this tool.

Which other trust mechanism could the organization configure for large-scale approval of these files?

- A. Trusted Distributor
- B. Windows Update
- C. Local Approval Mode
- D. Rapid Config

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 36

How is a new Alert of type Event Alert created whenever an endpoint is added or deleted and send emails for the App Control admin whenever these events occur?

- A. Add filter in Event Properties for Subtype Computer modified. Add the App Control admin email, and then click Create & Exit.
- B. Add filter in Event Properties for Subtype Computer added and Computer deleted. Add the App Control admin email, and then click Create & Exit.
- C. Add filter in Event Properties for Subtype Endpoint added and Endpoint deleted. Click Create and add the App Control admin email, and then click Create & Exit.
- D. Add filter in Event Properties for Subtype Computer added and Computer deleted. Click Create and add the App Control admin email, and then click Create & Exit.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 37

An administrator wants to find instances where the binary is unsigned.

Which term will accomplish this search?

- A. process_publisher_state:FILE_SIGNATURE_STATE_NOT_SIGNED
- B. NOT process_publisher:FILE_SIGNATURE_STATE_SIGNED
- C. NOT process_publisher_state:FILE_SIGNATURE_STATE_SIGNED
- D. process_publisher:FILE_SIGNATURE_STATE_NOT_SIGNED

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 38

An administrator needs to query all endpoints in the HR group for instances of an obfuscated copy of cmd.exe.

Given this Enterprise EDR query:

process_name:cmd.exe AND device_group:HR AND NOT enriched:true

Which example could be added to the query to provide the desired results?

- A. NOT process_name:cmd.exe
- B. NOT process_original_filename:cmd.exe
- C. NOT process_company_name:cmd.exe
- D. NOT process_internal_name:cmd.exe

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 39

At which three frequencies may a Carbon Black Audit and Remediation administrator schedule the run of Live Queries? (Choose three.)

- A. Any frequency
- B. Bi-Weekly
- C. Monthly
- D. Weekly
- E. Hourly
- F. Daily

Answer: C,D,F ([LEAVE A REPLY](#))

NEW QUESTION: 40

Which Live Query statement is properly constructed?

- A. SELECT * FROM 'users'
- B. select from users;
- C. select * from *;
- D. SELECT * FROM users;

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 41

Which statement is true about Carbon Black Live Response (CBLR)?

- A. CBLR sessions do not need to wait for the next sensor check-in.
- B. CBLR cannot be accessed through the API.
- C. CBLR is only available on Windows Endpoints.
- D. CBLR is disabled by default.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 42

Refer to the exhibit:

Which statement is true in regards to communication between the sensor and server?

- A. The sensor must be able to resolve the name cb.yourcompany.com.
- B. The sensor will communicate on a non-default port.
- C. The server must have an entry in the host file for cb.yourcompany.com.
- D. The communication is unencrypted.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 43

How often do watchlists run?

- A. Every 30 minutes
- B. Watchlists can be configured to run at scheduled intervals
- C. Every 10 minutes
- D. Every 5 minutes

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 44

An administrator receives an alert with the TTP DATA_TO_ENCRYPTION.

What is known about the alert based on this TTP even if other parts of the alert are unknown?

- A. A process attempted to delete encrypted data on the disk.
- B. A process attempted to modify a monitored file written by the sensor.
- C. A process attempted to write a file to the disk.
- D. A process attempted to transfer encrypted data on the disk over the network.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 45

A process is writing numerous interesting files that never actually execute.

Which rule type can the administrator define that will prevent reporting these file creations?

- A. Performance Optimization
- B. File Creation Control (Suppress)
- C. Expert (Tag Process, Terminate Process)
- D. Execute Ignore

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

Which statement filters data to only return rows where the publisher of the software includes VMware anywhere in the name?

- A. WHERE publisher = "%VMware%"
- B. WHERE publisher = "VMware"
- C. WHERE publisher LIKE "VMware%"
- D. WHERE publisher LIKE "%VMware%"

Answer: D ([LEAVE A REPLY](#))

Valid 5V0-91.20 Dumps shared by BraindumpsPass.com for Helping Passing 5V0-91.20 Exam! BraindumpsPass.com now offer the **newest 5V0-91.20 exam dumps**, the BraindumpsPass.com 5V0-91.20 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 5V0-91.20 dumps with Test Engine here:
<https://www.braindumpspass.com/VMware/5V0-91.20-practice-exam-dumps.html> (115 Q&As Dumps,
40%OFF Special Discount: Exam-Tests)

Valid 5V0-91.20 Dumps shared by BraindumpsPass.com for Helping Passing 5V0-91.20 Exam! BraindumpsPass.com now offer the **newest 5V0-91.20 exam dumps**, the BraindumpsPass.com 5V0-91.20 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 5V0-91.20 dumps with Test Engine here:
<https://www.braindumpspass.com/VMware/5V0-91.20-practice-exam-dumps.html> (115 Q&As Dumps,
40%OFF Special Discount: Exam-Tests)