

5V0-91.20.VCEplus.premium.exam.56q

Number: 5V0-91.20
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

5V0-91.20

VMware Carbon Black Portfolio Skills



Exam A

QUESTION 1

An administrator is troubleshooting App Control agent issues. When navigating to the Computer Details page, the administrator sees the following:

Computers

Computers connected: 1 Total computers: 2 Current CL version: 1156 CL version for upgrade: 1155

Saved Views: (none) Add

Group By: (none) Ascending

Days Disconnected: (none)

Show Filters | Show Columns | Export to CSV | Refresh Page

Action Search: Go Clear

	Computer Name ▲	Connected	Policy Status	Upgrade Status	Connected Enforcement	Disconnected Enforcement	IP Address	Policy
<input type="checkbox"/>	WORKGROUP\APPCONTROL	●	Up to date	Up to date	None (Visibility)	None (Visibility)	::1	Initial Install
<input type="checkbox"/>	WORKGROUP\WINDOWS-CLIENT	●	Up to date	Up to date	None (Visibility)	None (Visibility)	10.100.10.101	Initial Install

2 items
Page 1/1
25 rows per page

What is the status of the WINDOWS-CLIENT agent?

- A. Connected and Up to date
- B. Disconnected and Up to date
- C. Connected but unsupported
- D. Connected but health check failed

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2 There is a need to ignore all activity at an application path. Which rule definition should be used to address this need?

- A. Application at Path, Performs any operation, Bypass
- B. Application at Path, Runs or is Running, Bypass
- C. Application at Path, Runs or is Running, Allow & Log
- D. Application at Path, Performs any operation, Allow & Log

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-Console-How-to-Set-up-Exclusions-in-the/ta-p/42334>

QUESTION 3 An analyst is investigating an alert within the Enterprise EDR console and needs to take action on it.

Which three actions are available to take on the alert? (Choose three.)

- A. Ignore alert
- B. Dismiss
- C. Dismiss on all devices if grouping is enabled

- D. Edit watchlist
- E. Save report
- F. Notifications history

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-How-to-Dismiss-Alerts/ta-p/51766>

QUESTION 4 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. Move to group
- B. Disable
- C. Restart
- D. Ban
- E. Uninstall
- F. Share Settings

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjttoeA3lLvAhU6QhUIHZaND-YQFjAAegQIARAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F3020%2F1%2FCB_EDR_7.3_User_Guide.pdf&usg=AOvVaw23smt4s66MWHdv9jM2PYF- (86)

QUESTION 5

An analyst has investigated two alerts on two separate HR workstations and found that notepad.exe has established communication to another IP address.

Which rule will kill notepad.exe entirely if this activity is detected in the future?

- A. **\system32\notepad.exe --> Communicates over the network --> Terminate process
- B. **\system32\notepad.exe --> Runs or is Running --> Deny operation
- C. **/system32/notepad.exe --> Runs or is Running --> Terminate process
- D. **/system32/notepad.exe--> Communicates over the network --> Deny operation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj88fL33YLvAhVQRhUIHYbdDxAQFjABegQIARAD&url=https%3A%2F%2Fwww.carbonblack.com%2Fblog%2Fcb-threatsightinvestigation-reveals-retadup-worm-leverages-autoit-launch-monero-cryptomining-campaign%2F&usg=AOvVaw0De3tmD7FIQSS8VNMVsH7u>

QUESTION 6

A Carbon Black administrator received an alert for an untrusted hash executing in the environment.

Which two information items are found in the alert pane? (Choose two.)

- A. Launch Live Query
- B. Launch process analysis
- C. User quarantine
- D. Add hash to banned list

E. IOC short name

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

An administrator observes the following event detail in the Investigate tab for an application with an unknown reputation making network connections:

Process name: hxtsr.exe Process ID: 6720 App reputation: NOT_LISTED App reputation (applied, cloud): UNKNOWN App MD5: 1bd0d798a5a7f7e975d9ee59572a4012 App SHA: 16f7ddaa4944632505f557
Event ID: 010f7551b35a11ea9b3c9f3f7b58d4d8 Category: Monitored Alert ID: 5DWLGij9 Alert severity: 3 TTPs: INTERNATIONAL_SITE, NETWORK_ACCESS, ADAPTIVE_WHITE_APP, ACTIVE_CLIENT

Upon further review of the event details returned, the reputation is observed as NOT_LISTED, and the applied (cloud) reputation is UNKNOWN.

Why is the applied (cloud) reputation UNKNOWN and not NOT_LISTED?

- A. The sensor demoted the local reputation from UNKNOWN to NOT_LISTED based on the cloud reputation.
- B. NOT_LISTED was applied by the sensor after observing no cloud reputation, as evidenced by the applied cloud reputation UNKNOWN.
- C. The application was UNKNOWN at the time of the event but then later determined to be NOT_LISTED.
- D. The sensor demoted the local reputation from NOT_LISTED to UNKNOWN based on the cloud reputation.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 8

In which two ways can the tamper protection on an App Control agent be disabled when diagnosing agent issues or removing the agent? (Choose two.)

- A. From the Computer Details page on the web console
- B. From the Files on Computers page on the web console
- C. Run authenticated DasCLI on Windows command prompt
- D. Run RepCLI on Windows command prompt
- E. From the File Catalog page on the web console

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-to-Disable-Enable-Tamper-Protection/ta-p/37220>

QUESTION 9

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-What-Happens-When-Bypass-has-been-Enabled-on-the/ta-p/74905>

QUESTION 10

An Enterprise EDR administrator has created a custom Watchlist and wants to add a custom query to a report in the custom Watchlist.

From which page can the administrator add this custom query?

- A. Policies
- B. Watchlists
- C. Investigate
- D. Cloud Analysis

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwih0bWU4oLvAhX-UBUIHVBDDSUQFjAAegQIAhAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1913%2F18%2FEnterprise%2520EDR%2520Getting%2520Started.pdf&usg=AOvVaw2_M7opfEgUallfutBZChvk

QUESTION 11

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



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**QUESTION 12**

An analyst is investigating a specific alert in Endpoint Standard. The analyst selects the investigate button from the alert triage page and sees the following:

INVESTIGATE

alert_id ASAHBNJV

Enriched Events | Processes

FILTERS Clear

Type (3)

filemod	50.0%
crossproc	25.0%
netconn	25.0%

Process (2)

Search

...c26\patchwindows_script.ps1	75.0%
...wershell\v1.0\powershell.exe	25.0%

Effective Reputation (2)

Process Hash (5)

Device (1)

Search

tbent.wksh2	100.0%
-------------	--------

Events Applications Devices Network

4 results

TIME	TYPE	EVENT
10:59:16 am Jun 24, 2020	netconn	The script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbc8f4cc86\patchwindows_script.ps1 attempted to establish a TCP/80 connection to 169.254.169.254:80 (169.254.169.254) from 172.15.0.120:60155. The device was off the corporate network using the public address 34.225.43.220 (CBENT-WKSH2.ec2.internal, located in Ashburn VA, United States). The operation was blocked and the application terminated by Cb Defense. Policy Terminate Alert
10:59:15 am Jun 24, 2020	filemod	The file C:\windows\temp_psscriptpolicytest_bol00uen.5x4.ps1 was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbc8f4cc86\patchwindows_script.ps1 Alert
10:59:15 am Jun 24, 2020	crossproc	The script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbc8f4cc86\patchwindows_script.ps1 attempted to create a viewable window by calling the function 'CreateWindowExW'. The operation was successful. Alert
10:59:14 am Jun 24, 2020	filemod	The file C:\windows\temp_psscriptpolicytest_wnul40pe.wzg.ps1 was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the application C:\windows\system32\windowspowershell\v1.0\powershell.exe. Alert

Which statement accurately characterizes this situation?

- A. These events are tied to an observed alert within the user interface.
- B. The policy had no blocking and isolation rules set.
- C. The events shown will all have the same event ID, correlating them to the alert.
- D. Each event listed contributed to the overall alert score and severity.



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13 Examine the following EDR query:

file_desc:"Windows Command Processor" AND -process_name:cmd.exe

Which process will show in the query results?

- A. Any process named something other than cmd.exe with the file description of "Windows Command Processor"
- B. Any process with the binary file description "Windows Command Processor"
- C. Any process with the binary file description "Windows Command Processor" named cmd.exe
- D. Any process named cmd.exe

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwic3bDN5YLvAhX3QEEAHd2MDIQQFjAAegQIBRAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F2961%2F1%2FMware%2520Carbon%2520Black%2520App%2520Control%25208.5.0%2520User%2520Guide.pdf&usg=AOvVaw3es_0JTc8-BifNR4iFiGl (7)

QUESTION 15 This search is entered into the process search

page: notepad.exe Which three statements about this query are

true? (Choose three.)

- A. Only processes named notepad.exe will be returned.
- B. Since a field name is not selected, query performance will be impacted.
- C. A field identifier is required for all criteria within a process search.
- D. The search will fail with an error.
- E. All processes containing the text notepad.exe in any default field.
- F. Processes with registry modifications containing notepad.exe would be returned.

Correct Answer: BEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A company wants to implement the strictest security controls for computers on which the software seldom changes (i.e., servers or single-purpose systems).

Which Enforcement Level is the most fitting?

- A. Low Enforcement
- B. Medium Enforcement
- C. High Enforcement
- D. None (Visibility)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjapqGLiYXvAhUwQxUIHRn2BHYQFjALegQILxAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1001%2F1%2Fbit9-userguide.pdf&usg=AOvVaw23gKIZGFcZ4y9AKAalm9Oj>

QUESTION 17

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

- A. It adds a temporary reputation.
- B. It scans all files on execution.

- C. It scans new files on first execution.
- D. It enables signature updates for the scanner.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-To-Configure-Local-AV-Scan/ta-p/89051>

QUESTION 18 Review the following search:

childproc_name:"rundll32.exe" AND -digsig_result:"Signed" AND path:c:\windows*

What is this search looking for?

- A. Processes being launched by rundll32.exe running out of the windows directory that are not signed
- B. Instances of rundll32.exe running out of the windows directory that are not signed
- C. Instances of rundll32.exe running out of the windows directory that are signed
- D. Processes launching rundll32.exe running out of the windows directory that are not signed

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.carbonblack.com/blog/hunting-the-white-rabbit-detecting-metasploit-meterpreter-using-carbon-black/>

QUESTION 19 Which reputation is processed with the lowest priority for Endpoint Standard?

- A. Local White
- B. Known MalwareC. Trusted White
- D. Common White

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20 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 is disabled by default.
- C. CBLR is only available on Windows Endpoints.
- D. CBLR cannot be accessed through the API.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Cb-Response-Go-Live-Button-is-Grayed-Out/ta-p/41205>

QUESTION 21

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

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 administrator needs the use live query permission.
- C. The number of consecutive running queries is limited.
- D. The query or table is not supported within osquery.

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjZ_N65jIXvAhUFYcAKHbu4ChUQFjAAegQIAhAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F3142%2F25%2FCarbon%2520Black%2520Cloud%2520-%2520Endpoint%2520Advanced%2520User%2520Guide.pdf&usg=AOvVaw2N-B7YFQA_I7hj-HvB5Hf6 (47)

QUESTION 23

An Endpoint Standard administrator finds a binary in the environment and decides to manually add the file hash to the Banned List.

Which reputation does the file now have?

- A. Suspect/Heuristic Malware
- B. Company Black
- C. Adware/PUP Malware
- D. Known Malware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Given an event rule: Approve nVidia Drivers, changes the local state to Approved for file writes or execution blocks when the publisher is NVIDIA Corporation.

How is an alert created that is triggered whenever an nVidia driver is approved by the event rule?

- A. Add a new Alert of type Event Alert. Set Subtype to New unapproved file to computer and Execution block (unapproved file) and Publisher to NVIDIA Corporation. Click Create and add email recipients.
- B. Click Create Alert on the event rule Approve nVidia Drivers details page. Click Create and add email recipients. Create and Exit.
- C. Click Create Alert on the event rule Approve nVidia Drivers details page. Add email recipients. Create and Exit.

D. Create a custom rule name Approve nVidia that approves writes or blocks when the publisher is NVIDIA Corporation. Create an alert for rule name Approve nVidia. Click Create and add email recipients.

Correct Answer: B

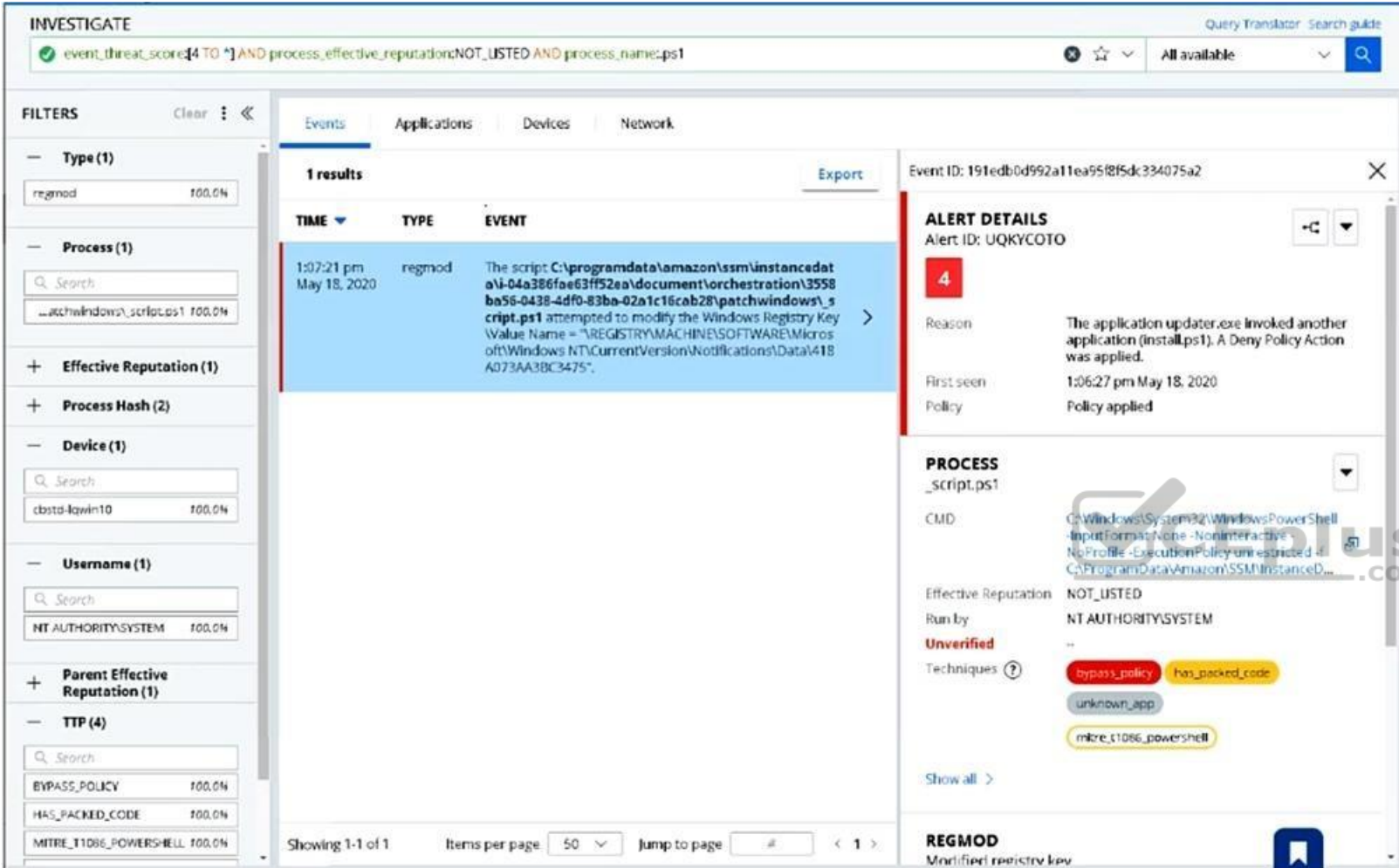
Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

An Endpoint Standard analyst runs the query in the graphic below:



The screenshot shows the Microsoft Defender for Endpoint Investigate interface. The query bar contains the query: `event_threat_score[4 TO *] AND process_effective_reputation:NOT_LISTED AND process_name:ps1`. The left sidebar shows filters for Type (1), Process (1), Effective Reputation (1), Process Hash (2), Device (1), Username (1), Parent Effective Reputation (1), and TTP (4). The main pane shows 1 result for the query. The result is a regmod event from May 18, 2020, at 1:07:21 pm. The event description states: "The script C:\programdata\amazon\ssm\instancedat... attempted to modify the Windows Registry Key Value Name = 'REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475'." The right pane shows alert details for Alert ID: UQKYCOTO, with a reason of "The application updater.exe invoked another application (install.ps1). A Deny Policy Action was applied." The process details show the process name as _script.ps1, running under NT AUTHORITY\SYSTEM, with an effective reputation of NOT_LISTED. The techniques listed are bypass_policy, has_packed_code, unknown_app, and mitre_t1086_powershell.

Which three statements are true from the results shown? (Choose three.)

- A. The process is a PowerShell process running a script with a .ps1 extension.
- B. The process has a threat score greater than 4.
- C. The process made a network connection to another system.
- D. The process had a NOT_LISTED reputation at the time the event occurred.
- E. The process was run under the NT_AUTHORITY\SYSTEM user context.
- F. The process was able to inject code into another process.

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.google.com/url?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)

QUESTION 28 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 Report Only. 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 Enabled. The event details show the process, file name, and hash modified or deleted on the removable media.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

Which action is only available for the “Performs any operation” and “Performs any API Operation” operation attempts?

- A. Bypass
- B. Allow & Log
- C. Runs or is Running
- D. Allow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjCIN7SwoXvAhVignEKHbXpChUQFjAAegQIARAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1413%2F3%2Fcbd-userguide.pdf&usg=AOvVaw1CU0_RmjfwbwAh68luEKAd
(90)

QUESTION 30 Review

this EDR query:

childproc_name:whoami.exe AND childproc_name:hostname.exe AND childproc_name:tasklist.exe AND childproc_name:ipconfig.exe

Which process would show in the query results?

- A. Any process invoked by whoami.exe, hostname.exe, tasklist.exe, and ipconfig.exe
- B. Any process invoked by whoami.exe, hostname.exe, tasklist.exe, or ipconfig.exe
- C. Any process invoking whoami.exe, hostname.exe, tasklist.exe, or ipconfig.exe
- D. Any process invoking whoami.exe, hostname.exe, tasklist.exe, and ipconfig.exe

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

A Carbon Black Cloud analyst needs to identify the Internet Explorer extensions installed on Windows endpoints.

Which Live Query statement will successfully query these items?

- A. SELECT * FROM registry JOIN ie_extensions;
- B. SELECT * FROM registry WHERE ie_extensions;
- C. SELECT * FROM ie_extensions;
- D. SELECT * FROM ie_extensions WHERE enabled=true;

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which statement is true about configuring VMware Carbon Black Application Control for use on non-persistent virtual machines (VM's)?

- A. The endpoint housing the agent template must always be on/running except when updating the image.
- B. The gold image housing the agent template must be digitally signed to ensure the integrity of the agent cache.
- C. The endpoint housing the agent template must always be off except when updating the image.
- D. The agent running on the template machine must not be initialized before deploying clones.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33 An administrator runs the following query in Audit and Remediation:

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

How long will this query stay active and accept data from the sensors?

- A. 14 days
- B. 30 days
- C. 7 days
- D. 1 day

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-Audit-and-Remediation-How-long-does-a-query/ta-p/34817>

QUESTION 34

An administrator uses the following Enterprise EDR search query to show web browsers spawning non-browser child processes that connect over the network:

(parent_name:chrome.exe OR parent_name:iexplore.exe OR parent_name:firefox.exe) AND (NOT process_name:chrome.exe OR NOT process_name:iexplore.exe OR NOT process_name:firefox.exe) Which field can be added to this query to filter the results by signature status?

- A. childproc_publisher_state
- B. process_publisher
- C. childproc_reputation
- D. process_publisher_state

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35 Given the following query:

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

Which statement is correct?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36 What are three ways to ignore a feed report within the EDR user interface? (Choose three.)

- A. Threat Reports Details page
- B. Threat Intelligence Feeds page



- C. Investigations page
- D. Search Threat Reports page
- E. Alert Dashboard page
- F. After marking a feed alert as a false positive

Correct Answer: ABF

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/EDR-How-to-Customize-a-Feed-to-Prevent-False-Positives/ta-p/64413>

QUESTION 37 What is the maximum number of binaries (hashes) that can be banned using the web console?

- A. 500
- B. 600
- C. 300
- D. 400

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38 An administrator wants to allow files to run from a network share.

Which rule type should the administrator configure?

- A. Execute Prompt (Shared Path)
- B. Trusted Path
- C. Network Execute (Allow)
- D. Write Approve (Network)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39 An analyst is reviewing an alert in Enterprise EDR from a custom watchlist. The analyst disagrees with the alert severity rating.

How can the analyst change the alert severity value, if this is possible?

- A. The alert severity is assigned by the backend analytics.
- B. The alert severity is not configurable.
- C. Change the alert severity on the watchlist.
- D. Change the alert severity on the report.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 40 What information does the Alert Details panel provide on the Alert Triage page in Endpoint Standard?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

An analyst on the security team noticed that several alerts are false positives within Enterprise EDR. The analyst disables the IOC within the report from those alerts.

Which statement correctly explains what disabling the IOC will accomplish?

- A. That specific IOC in the report will no longer generate hits or alerts on the device from the alert.
- B. The report will no longer generate hits or alerts on the device from the alert.
- C. That specific IOC in the report will no longer generate hits or alerts.
- D. The report will no longer generate hits or alerts.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 42 Which identifier is shared by all events when an alert is investigated?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43 An Enterprise EDR administrator wants to use Watchlists curated by VMware Carbon Black and other threat intelligence specialists.

How should the administrator add these curated Watchlists from the Watchlists page?

- A. Click Add Watchlists, and input the URL(s) for the desired Watchlists.
- B. Click Take Action, select Edit, and select the desired Watchlists.
- C. Click Take Action, and select Subscribe for the desired Watchlists.
- D. Click Add Watchlists, on the Subscribe tab select the desired Watchlists, and click Subscribe.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj1tW404XvAhWZRhUIHSygB74QFjADegQIExAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1913%2F18%2FEnterprise%2520EDR%2520Getting%2520Started.pdf&usq=AOvVaw2_M7opfEgUallfutBZChvk (5)

QUESTION 44 An incorrectly constructed watchlist generates 10,000 incorrect alerts.

How should an administrator resolve this issue?

- A. Delete the watchlist to automatically clear the alerts, and then create a new watchlist with the correct criteria.
- B. From the Triage Alerts Page, use the facets to select the watchlist, click the Wrench button to “Mark all as Resolved False Positive”, and then update the watchlist with the correct criteria.
- C. Update the Triage Alerts Page to show 200 alerts, click the Select All Checkbox, click the “Dismiss Alert(s)” button for each page, and then update the watchlist with the correct criteria.
- D. From the Watchlists Page, select the offending watchlist, click “Clear Alerts” from the Action menu, and then update the watchlist with the correct criteria.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45 Which list below captures all Enforcement Levels for App Control policies?

- A. Critical, Lockdown, Monitored, Tracking, Banning
- B. High Enforcement, Medium Enforcement, Low Enforcement
- C. High Enforcement, Medium Enforcement, Low Enforcement, None (Visibility), None (Disabled)
- D. Control, Local Approval, Disabled

Correct Answer: C

Section: (none)

Explanation

**Explanation/Reference:**

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiFsPPz04XvAhWRsnEKHV4lBukQFjABegQIAhAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F2961%2F1%2FVMware%2520Carbon%2520Black%2520App%2520Control%25208.5.0%2520User%2520Guide.pdf&usq=AOvVaw3es_0JTc8-BifNR4iFiGl (6)

QUESTION 46

A company uses Audit and Remediation to check configurations and adhere to compliance regulations. The regulations require monthly reporting and twelve months of data retained.

How can an administrator accomplish this requirement with Audit and Remediation?

- A. Schedule the query to run monthly, and set the data retention to 12 months for the query.
- B. Schedule the query to run monthly, and configure the audit log retention to 12 months.
- C. Schedule the query to run monthly, and no further action is required.
- D. Schedule the query to run monthly, and export the results for each run to an external location.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiE-87R1IXvAhVQRhUIHbkOCHUQFjAAegQIARAD&url=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F3142%2F24%2FCarbon%2520Black%2520Cloud%2520-%2520Audit%2520and%2520Remediation%2520User%2520Guide.pdf&usq=AOvVaw0kK6mNGRW_8wvc65hQxHE0 (6)

QUESTION 47

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

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. Disable the alert.
- D. Delete the alert.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 49

An analyst wants to block an application's specific behavior but does not want to kill the process entirely as it is heavily used on workstations. The analyst needs to use a Blocking and Isolation Action to ensure that the process is kept alive while blocking further unwanted activity.

Which Blocking and Isolation Action should the analyst use to accomplish this goal?

- A. Log Operation
- B. Deny Operation
- C. Terminate Process
- D. Block Process

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50 An administrator wants to query the status of the firewall for all endpoints. The administrator will query the registry key found here

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile.

To make the results easier to understand, the administrator wants to return either enabled or disabled for the results, rather than the value from the registry key.

Which SQL statement will rewrite the output based on a specific result set returned from the system?

- A. CASE
- B. AS
- C. ALTER

D. SELECT

Correct Answer: A

Section: (none)

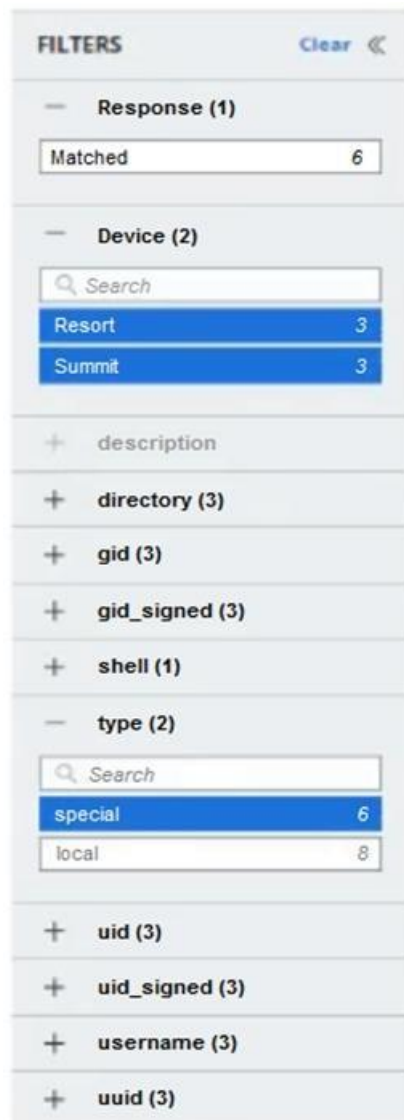
Explanation

Explanation/Reference:

Reference: <https://www.carbonblack.com/blog/8-live-queries-that-will-speed-up-your-next-pci-audit/>

QUESTION 51

Refer to the exhibit:



The screenshot shows a 'FILTERS' sidebar with a 'Clear' button and a back arrow. It contains several filter sections:

- Response (1)**: A dropdown menu showing 'Matched' with a count of 6.
- Device (2)**: A search bar and a list of devices: 'Resort' (3) and 'Summit' (3).
- description**: A plus sign icon.
- directory (3)**: A plus sign icon.
- gid (3)**: A plus sign icon.
- gid_signed (3)**: A plus sign icon.
- shell (1)**: A plus sign icon.
- type (2)**: A search bar and a list of types: 'special' (6) and 'local' (8).
- uid (3)**: A plus sign icon.
- uid_signed (3)**: A plus sign icon.
- username (3)**: A plus sign icon.
- uuid (3)**: A plus sign icon.



Which two logic statements correctly explain filtering within the UI? (Choose two.)

- A. Filtering between fields is a logical OR
- B. Filtering within the same field is a logical AND
- C. Filtering between fields is a logical AND
- D. Filtering between fields is a logical XOR
- E. Filtering within the same field is a logical OR

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://uit.stanford.edu/service/cbprotect/approval-mechanisms>

QUESTION 53 How often do watchlists run?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 54**

Which statement should be used when constructing queries in Carbon Black Audit and Remediation, Live Query?

- A. ALTER
- B. UPDATE
- C. REMOVE
- D. SELECT

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55 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*

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-to-Create-Policy-Blocking-Isolation-and/ta-p/65941>

QUESTION 56 An alert for a device running a proprietary application is tied to a vital business operation.

Which action is appropriate to take?

- A. Add the application to the Approved List.
- B. Terminate the process.
- C. Deny the operation.
- D. Quarantine the device.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference: