# VMware Carbon Black Portfolio Skills

**1.** 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 endpoints on the query by selecting the check box for each device.

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 the policy for the endpoints on the query, and then select the check box for each device.

D. 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.

**Answer(s):** D

---

**2.** A process wrote an executable file as detailed in the following event:
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. Trusted Path

B. File Creation Control

C. Advances (Write-Ignore)

D. Trusted Publisher

**Answer(s):** B

---

**3.** Which enforcement level does not block unapproved files but will block files that have been specifically banned?

A. Medium Enforcement

B. Disabled

C. Visibility

D. Low Enforcement

**Answer(s):** B

---

**4.** An administrator has updated a Threat Intelligence Report by turning it into a watchlist and needs to disable (Ignore) the old Threat Intelligence Report.
Where in the UI is this action not possible to perform?

A. Search Threat Reports Page

B. Threat Intelligence Feeds Page

C. Threat Report Page

D. Triage Alerts Page

**Answer(s):** B

---

**5.** An analyst navigates to the alerts page in Endpoint Standard and sees the following:
What does the yellow color represent on the left side of the row?

A. It is an alert from a watchlist rather than the analytics engine.

B. It is a threat alert and warrants immediate investigation.

C. It is an observed alert and may indicate suspicious behavior.

D. It is a dismissed alert within the user interface.

**Answer(s):** A

---

**6.** 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. Sensor Management

B. Investigate

C. Policies

D. Alerts

**Answer(s):** A

---

**7.** 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. **/java.exe --> Invokes an untrusted process --> Terminate process

B. **/Program Files/*/java.exe--> Invokes an untrusted process --> Deny operation

C. **\Program Files*\java.exe --> Invokes a command interpreter --> Terminate process

D. **\java.exe --> Invokes a command interpreter --> Deny operation

**Answer(s):** C

---

**8.** Review the following query:
path:c:\program\ files\ \(x86\)\microsoft
How would this query input term be interpreted?

A. c:\program files x86\microsoft

B. c:rogram files (x86)icrosoft

C. c:rogramfilesx86icrosoft

D. c:\program files (x86)\microsoft

**Answer(s):** D

---

**9.** 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(s):** D

---

**10.** An administrator ran the following query.
SELECT name, VERSION, install_location, install_source, publisher, install_date, uninstall_string FROM programs WHERE publisher = "Microsoft Corporation"; The administrator notices a lot of installed programs are not returned. How can the administrator alter the query to see all results?

A. Edit the WHERE clause to remove the quotes

B. Remove the WHERE clause

C. Replace the = with LIKE

D. Change the WHERE clause to = "*"

**Answer(s):** A

**11.** Which actions are available for Permissions?

A. Approve, Upload, No Upload

B. Deny Operation, Terminate Process

C. Allow, Allow & Log, Bypass

D. Performs any Operation, Runs or is running

**Answer(s):** C

---

**12.** Refer to the exhibit, noting the circled red dot:
What is the meaning of the red dot under Hits in the Process Search page?

A. Whether the execution of the process resulted in a syslog hit

B. Whether the execution of the process resulted in a sensor hit

C. Whether the execution of the process resulted in matching hits for different users

D. Whether the execution of the process resulted in a feed hit

**Answer(s):** C

---

**13.** An Endpoint Standard administrator is working with an IT team to explicitly permit specific applications from the environment using both the IT Tools and Certs Approved List features. Once applied, which reputation would these applications be classified under for processing?

A. Trusted White

B. Company White

C. Local White

D. Common White

**Answer(s):** A

---

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

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

**Answer(s):** A B D

---

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

A. Schedule an add-hoc cron job to remove

B. Use a pre-configured system cron job daily to remove them

C. Run the cbbannlng script on the EDR server

D. Go to the hashes page on the web console and remove them

**Answer(s):** C

---

**16.** 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. 1 day

B. 7 days

C. 14 days

D. 30 days

**Answer(s):** D

---

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

A. Move all computers to the original Enforcement level

B. Move all computers to High Enforcement level

C. Move all computers to Low Enforcement level

D. Move all computers to Medium Enforcement level

**Answer(s):** A

---

**18.** 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 established.
- [ ] C. CBLR is disabled.
- [ ] D. A CBLR session is not attached.
- [ ] E. A CBLR session already exists.

**Answer(s):** D E

---

**19.** What occurs when an administrator selects "Enable private logging level" in Sensor Settings under Policy?

A. Delay execute for cloud scan is disabled.

B. Script Files that have unknown reputations are not uploaded.

C. Live Response is disabled.

D. Domain names are obfuscated.

**Answer(s):** B

---

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

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

**Answer(s):** A E

---