Question 1

An 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 path?

Options:

A- All executable files in the 'Program Files' folder and subfolders will be ignored, including malware files.

B- No Files will be ignored from the 'Program Files' director/, but Malware in the 'Program Files' directory will continue to be blocked.

C- Executable files in the 'Program Files' folder will be blocked.

D- Only executable files in the 'Program Files' folder will be ignored, including malware files.

Answer:

A

Question 2

An administrator is tasked to create a reputation override for a company-critical application based on the highest available priority in the reputation list. The company-critical application is already known by VMware Carbon Black.

Which method of reputation override must the administrator use?

Options:

A- Signing Certificate

B- Hash

C- Local Approved

D- IT Tool

Answer:

A

Question 3

An organization has found application.exe running on some machines in their Workstations policy. Application.exe has a SUSPECT_MALWARE reputation and runs from C:\Program Files\IT\Tools. The Workstations policy has the following rules which could apply:

Blocking and Isolation Rule

Permissions Rule

Which action, if any, should an administrator take to ensure application.exe cannot run?

Options:

A- Change the reputation to KNOWN MALWARE to a higher priority.

B- No action needs to be taken as the file will be blocked based on reputation alone.

C- Remove the Permissions rule for C:\Program FilesMTVToolsV.

D- Add the hash to the company banned list at a higher priority.

Answer:

C

Question 4

An administrator needs to make sure all files are scanned locally upon execution.

Which setting is necessary to complete this task?

Options:

A- On-Access File Scan Mode must be set to Aggressive.

B- Signature Update frequency must be set to 2 hours.

C- Allow Signature Updates must be enabled.

D- Run Background Scan must be set to Expedited.

Answer:

A

Question 5

What is a security benefit of VMware Carbon Black Cloud Endpoint Standard?

Options:

A- Events and alerts are tagged with Carbon Black TTPs to provide context around attacks.

B- Firewall rule configuration are provided in the environment.

C- Data leakage protection (DLP) is enforced on endpoints or subsets of endpoints.

D- Customized threat feeds can be combined with other outside threat intelligence sources.

Answer:

A