DUMPSARENA

VMware Carbon Black Cloud Endpoint Standard Skills

VMware 5V0-93.22

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, VMware Carbon Black Cloud Endpoint Standard - Architecture and Technologies	1
Topic 2, VMware Carbon Black Cloud Endpoint Standard - Products and Solutions	1
Topic 3, Planning and Designing	1
Topic 4, Installing, Configuring, and Setup	2
Topic 5, Troubleshooting and Repairing	4
Topic 6, Administrative and Operational Tasks	14
Total	23

QUESTION NO: 1

An investigation confirms that a specific executable hash is malicious. The administrator needs to prevent that exact file from executing on managed endpoints without creating a broad rule that affects files with similar names or paths.

Which action should the administrator take?

A. Create a ban for the confirmed file hash.

B. Create a process rule that matches the file name only.

C. Mark the file hash as approved.

D. Remove the affected endpoints from their device groups.

ANSWER: A

Explanation:

A ban for the confirmed malicious hash is the most targeted control. It prevents execution of the identified file regardless of the filename or location used on an endpoint. A process rule based only on a filename or path can be bypassed by renaming or relocating the file and can unintentionally affect legitimate software with a similar name.

QUESTION NO: 2

An administrator creates a narrowly scoped process rule to address a confirmed threat. Before enabling the rule, the administrator wants to determine whether its conditions would have matched recently observed legitimate activity.

Which action provides this validation without enforcing the rule?

A. Use the Test Rule link from within the rule.

B. Enable the rule with a deny action.

C. Restart the sensor service on a pilot endpoint.

D. Create an alert notification for the policy.

ANSWER: A

Explanation:

The **Test Rule** capability evaluates the proposed rule conditions against available historical event data and returns matching results. This allows the administrator to assess likely false positives before enabling enforcement. Enabling the rule would apply the configured action going forward, while alert notifications and sensor restarts do not validate the rule against prior events.