5V0-91.20^{Q&As}

VMware Carbon Black Portfolio Skills

Pass VMware 5V0-91.20 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/5v0-91-20.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware
Official Exam Center

🛠 **Instant Download** After Purchase

🛠 **100% Money Back** Guarantee

🛠 **365 Days** Free Update

🛠 **800,000+** Satisfied Customers

QUESTION 1

An analyst is investigating an alert within Enterprise EDR on the process analysis page. The process tree can be seen below:

Which statement accurately characterizes this situation?

A. Conhost.exe has one or more child processes.

B. The solid line between the nodes denotes a process was injected into by another process.

C. Several nodes in this process tree have watchlist hits.

D. The analyst navigated to this process analysis page from the wscrlpt.exe process.
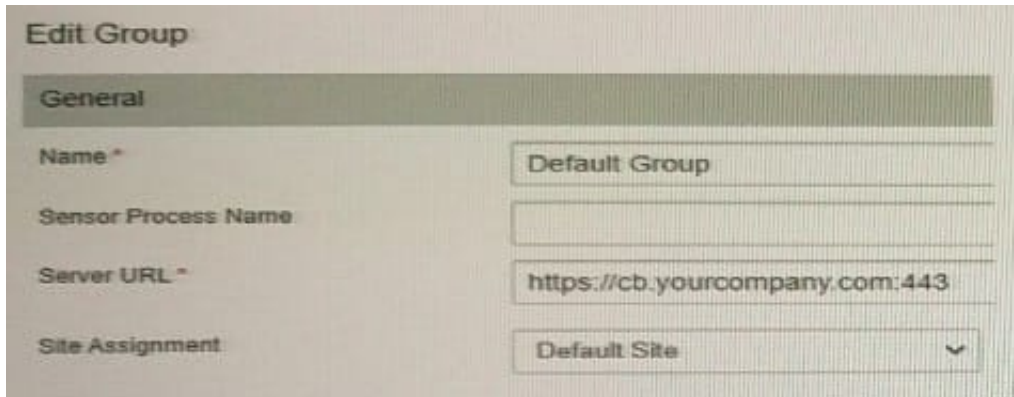
Correct Answer: B

QUESTION 2

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

QUESTION 3

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 server must have an entry in the host file for cb.yourcompany.com.

C. The communication is unencrypted.

D. The sensor will communicate on a non-default port.

Correct Answer: C

QUESTION 4

An administrator runs multiple queries on tables and combines the results after the fact to correlate data. The administrator needs to combine rows from multiple tables based on data from a related column in each table.

Which SQL statement should be used to achieve this goal?

A. JOIN

B. WHERE

C. AS

D. COMBINE

Correct Answer: A

QUESTION 5

An administrator wants to find instances where the binary Is unsigned. Which term will accomplish this search?

A. NOT process_publisher:FILE_SIGNATURE_STATE_SIGNED

B. NOT process_publisher_state:FILE_SIGNATURE_STATE_SIGNED

C. process_publisher_state:FILE_SIGNATURE_STATE_NOT_SIGNED

D. process_publisher:FILE_SIGNATURE_STATE_NOT_SIGNED

Correct Answer: B