

KillTest

質量更高 服務更好



練習題

<https://www.killtest.net>

一年免費更新服務

Exam : 5V0-91.20

**Title : VMware Carbon Black
Portfolio Skills**

Version : DEMO

1. 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

Answer: A

Explanation:

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

2. An analyst navigates to the alerts page in Endpoint Standard and sees the following:

STATUS	FIRST SEEN	REASON	DEVICE	ACTIONS
■	11:58:42 pm Aug 17, 2020	A known virus (Malware: EICAR) was detected.	Administrator Summit	[Icons]
■	11:58:42 pm Aug 17, 2020	The application explorer.exe dropped a known virus (Malware: EICAR) onto the device.	Administrator Summit	[Icons]
■	11:52:44 pm Aug 17, 2020	The application firefox.exe invoked another application (helper.exe).	Administrator Temple	[Icons]

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: A

3. An Enterprise EDR administrator sees the process in the graphic on the Investigate page but does not see an alert for this process:

PROCESS	DEVICE	DEVICE TIME	PID	USERNAME	REGMODS	FILEMODS	NETCONNS	MODLOADS	CHILDPROCS
cmdtask.exe	clientad	10:35:39 am Aug 12, 2020	1948	CBPNTEDRhe-induser					2
Scheduled Task Created	clientad	10:35:39 am Aug 12, 2020	1132	CBPNTEDRhe-induser					
cmdtask.exe	clientad	10:35:39 am Aug 12, 2020	5744	CBPNTEDRhe-induser					

How can the administrator generate an alert for future hits against this watchlist?

- A. select the watchlist on the watchlists page, select the Scheduled Task Created report, and use Take Action to select Alert on hit for the report.
- B. Select the watchlist on the watchlists page, select the Scheduled Task Created report, and use Take Action to toggle Alert on hit to On.
- C. Select the watchlist on the watchlists page and click on Alerts: Off to toggle the alerts to On.
- D. Select the watchlist on the watchlists page, use Take Action to select Edit, and select Alert on hit.

Answer: D

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

Answer: A

5.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)

Answer: A