

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.pass2lead.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

Given the following query:

SELECT hostname, cpu_type, cpu_brand, cpu_physical_cores, cpu_logical_cores, cpu_microcode, (1.0 * physical_memory / (1000*1000*1000)) AS physical_mem_gb, hardware_vendor, hardware_model, hardware_version, hardware_serial FROM system_info;

Which statement Is correct?

- A. This query combines data from several different tables.
- B. This query customizes the results returned by the system.
- C. This query is missing a filter option.
- D. This query shows data from the physical_mem_gb column.

Correct Answer: C

QUESTION 2

A process has created a number of interesting (executable) files in one sequence.

In addition to the event Subtype \\'New Unapproved File to Computer\\', what other event subtype is likely to be associated with this sequence?

- A. File Upload Completed
- B. New File Discovered on Startup
- C. File Group Created
- D. File Properties Modified

Correct Answer: B

QUESTION 3

Which statement correctly defines the results of ignoring a feed report?

- A. Ignoring a feed report will ignore future instances of that report.
- B. Ignoring a feed report will ignore all indicators in other threat reports.
- C. Ignoring a feed report will also ignore the threat intelligence feed.



D. Ignoring a feed report will remove all instances of the report.

Correct Answer: C

QUESTION 4

How can an analyst disregard alerts on multiple devices with the least amount of administrative effort?

- A. Select the "Dismiss on all devices" option.
- B. Make a note in the Notes/Tags option.
- C. Search by hash and dismiss.
- D. Turn off the Group Alerts option.

Correct Answer: D

Reference: https://www.google.com/url? sa=tandrct=jandq=andesrc=sandsource=webandcd=andcad=rjaanduact=8andved=2ahUKEwjv6pryl4XvAhW agVwKHTCMDTEQFjAAegQIARADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Ft5% 2FKnowled ge-Base%2FCarbon-Black-Cloud-How-to-Dismiss-Alerts%2Fta-p% 2F51766andusg=AOvVaw2x1mST1tWpuASUMLmFhyul (80)

QUESTION 5

What is the maximum number of binaries (hashes) that can be banned using the web console?

A. 500

B. 600

C. 300

- D. 400
- Correct Answer: C

QUESTION 6

App Control System Health email alerts for excessive agent backlog are occurring hourly.

This is overwhelming the analysts, and they would like to reduce the notifications.

How can the analyst reduce the unneeded alerts?

- A. Set the email address for subscribers to an invalid email.
- B. Change reminder email to daily or disabled.



- C. Disable the alert.
- D. Delete the alert.
- Correct Answer: B

QUESTION 7

This search is entered into the process search page: notepad.exe Which three statements about this query are true? (Choose three.)

- A. Only processes named notepad.exe will be returned.
- B. Since a field name is not selected, query performance will be impacted.
- C. A field identifier is required for all criteria within a process search.
- D. The search will fail with an error.
- E. All processes containing the text notepad.exe in any default field.
- F. Processes with registry modifications containing notepad.exe would be retuned.

Correct Answer: BEF

QUESTION 8

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

Correct Answer: A

QUESTION 9

An Endpoint Standard analyst runs the query in the graphic below:



C, Serrich	event_threat_score: 4 TO *] AND	process_effective_	reputation	OT_USTED AND process_name:.ps1			0 4 ~	All available	~
- Type (1) I results Export - Type (1) I results Export - Process (1) I make * Type EVENT - Make * Type EVENT ALERT DETAILS - Make * Type <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>									
Treamed Tenuits Export Export Export Tesuits Tesuits Export Export Export ALEXT DETAILS	ILTERS Clear : «	Events	Application	s Devices Network					
rrgmd 160.6% - Process (1) Q. Scroth Laker V DPF is VKNT 157.21 pm 157.21 pm <td< td=""><td>- Type (1)</td><td>Lensuite</td><td></td><td></td><td>Export</td><td>Event ID: 191edb0d992a</td><td>11ea551815dc3</td><td>34075a2</td><td></td></td<>	- Type (1)	Lensuite			Export	Event ID: 191edb0d992a	11ea551815dc3	34075a2	
 Process (1) Sorth Sorth	regmod f00,0%	11490419			export				
Jordan (1) List2:21 pm regmod The script C:\programdata\amazon\smi\instancedat abi-04a3E6feedBf32a+ddocument/orchestration\355 Reason The application updater.ese invoked anothe application (instan_ps1). A Deny Policy Action was applied. + Effective Reputation (1) - The script C:\programdata\amazon\smi\instancedat abi-04a3E6feedBf32a+ddocument/orchestration\355 - The application updater.ese invoked anothe application (instan_ps1). A Deny Policy Action was applied. + Process Hash (2) - Device (1) - - 0. Search tistst-laquin10 100.5% - To0.5% - - - Username (1) C.\Windows\System32\WindowsNottications\Data4418 C.Windows\System32\WindowsNottications\Data4418 PROCESS script.ps1 - - Username (1) C.Soroth Tr AUTHORITYSYSTEM To0.5% - - - - Soroth Tr TP (4) - - - - - - - TTP (4) - - - - - - - TTP (4) - - - - - - TTP (4) - - - - - <		TIME 💌	TYPE	EVENT					•c •
Q. Sorch May 18, 2020 al-04.26366fa626ff32a-udocument/orchestration/3558	Process (1)	1				Alert ID: UQKYCOT	0		
	Q. Search		regmod	a\i-04a3E6fae63ff52ea\document\orchestration\	3558	4			
Wale Name - TacGGTTYNARCHINESSOFTWARCHINESSOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOFTWARCHINessOfTWARCHINessOfTWARCHINessOfTWARCHINessOfTWARCHINessOfTWARCHINessOfTWARCHINessOfTWARCHINessOfTwarchines + Effective Reputation (1) A373AA3BC3475". + Process Hash (2) - Devke (1) Q. Search - Scorth - Usemame (1) C.Wandows/System32/Windows/System32/W	atchwindows_script.ps1_f00.0N			ba56-0438-4df0-83ba-02a1c16cab28\patchwindov	15/ 5				
 Effective Reputation (1) A073AA38C3475* Process Hash (2) Device (1) Rest seen 1:0627 pm May 18:2020 Policy Policy applied PROCESS				\Value Name = "\REGISTRY\MACHINE\SOFTWARE\MI	cros	Reason	application (i		
 Process Hash (2) Device (1) Search Converting Search Converting Converting	- Effective Reputation (1)			A073AA38C3475°.		First seen		ay 18. 2020	
Q. Search	- Process Hash (2)					Policy		Se metalasi an	
Q. Search	- Device (1)								
CMD C:Windows/System:2/Wi Stowid: Stowid: Sto	Q. Search								-
Username (1) Scorch TAUTHORITYSYSTEM 100.0H Scorch TTP (4) Scorch NPASS_POLICY 100.0H HS_PACHLD_CODE 100.0H HS_	bstd-lqwin10 roo.on					CUD	Cattandows	Sustem 320 Mindows Pou	erShell
RStorch Effective Reputation NOT_USTED RT_AUTHORITYSYSTEMF00.0% Run by NT_AUTHORITYSYSTEM • Parent Effective Reputation (1) - • TTP (4) - Techniques (*) (*) Rstorch	Username (1)					Carto	-InputFormat NoProfile -Ex	None -Noninteractive ecutionPolicy unrestrict	ted of d
IT AUTHORITYSYSTEM 100.0N T AUTHORITYSYSTEM 100.0N Parent Effective Reputation (1) TTP(4) C, Storich NPASS_POLICY 100.0N Show all > Techniques	0 fuert					Effective Reputation	10.000		
 Parent Effective Reputation (1) TTP (4) Reputation (1) TTP (4) TTP (4)						 Contraction and a second se second second se		IY\SYSTEM	
- TTP (4)	IT AUTOMITICITIEM TOLON					Unverified			
Keputation (1) urknown,app - TTP (4) (mkre_t1066_powershell) Q. Skorch Show all > Strow all > Show all >						Techniques 🕐	bypass_polic	has_packed_code	
Q. Storch: Inter_titles_powershell NPASS_POLICY 100.0H HAS_PACHED_CODE 100.0H	Reputation (1)						unknown_ap	P	
Q. Storth: SYPASS_POLICY 100.0% H45_PACNED_CODE 100.0%	- TTP (4)						(mkre_t1066)	powershell	
HYX-55_POLICY 100.0M HS_PACNED_CODE 100.0N	Q. Storch					100 - 100 - 20			
	EVPASS_POLICY FOD.04					Show all >			
	AS_PACKED_CODE 100.0%								
MITRE_TID86_POWERSHELL f00.0N Showing 1-1 of 1 Items per page 50 V jump to page # < 1 > REGMOD	MITRE_T1086_POWERSHELL #00.0%	Showing 1-1 of 1	Iter	ms per page 50 V Jump to page #] < 1>	REGMOD			

Which three statements are true from the results shown? (Choose three.)

- A. The process is a PowerShell process running a script with a .ps1 extension.
- B. The process has a threat score greater than 4.
- C. The process made a network connection to another system.
- D. The process had a NOT_LISTED reputation at the time the event occurred.
- E. The process was run under the NT_AUTHORITY\SYSTEM user context.
- F. The process was able to inject code into another process.

Correct Answer: ADF

QUESTION 10

An administrator is creating a query per policy for Audit and Remediation. The administrator ran several recommended queries already but notices they are unable to run the same recommended query for one of their policies. The run button is grayed out.

Which statement correctly explains why the run button is unavailable?

A. The sensors in the policy do not support the table or query.



- B. The administrator needs the use live query permission.
- C. The number of consecutive running queries is limited.
- D. The query or table is not supported within osquery.

Correct Answer: B

QUESTION 11

An Enterprise EDR administrator has created a custom Watchlist and wants to add a custom query to a report in the custom Watchlist.

From which page can the administrator add this custom query?

- A. Policies
- B. Watchlists
- C. Investigate
- D. Cloud Analysis
- Correct Answer: C

QUESTION 12

What does the Aggressive setting do when configured in Local Scan Settings?

- A. It adds a temporary reputation.
- B. It scans all files on execution.
- C. It scans new files on first execution.
- D. It enables signature updates for the scanner.

Correct Answer: C

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-ToConfigure-Local-AV-Scan/ta-p/89051

QUESTION 13

Given the following query:

SELECT * FROM users WHERE UID >= 500;



- Which statement is correct?
- A. This query limits the number of columns to display in the results.
- B. This query filters results sent to the cloud.
- C. This query is missing a parameter for validity.
- D. This query returns all accounts found on systems.

Correct Answer: A

QUESTION 14

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 15

Which value should an administrator use when reviewing an alert to determine the file reputation at the time the event occurred?

- A. Cloud Reputation (Initial)
- B. Effective Reputation



- C. Local Reputation
- D. Cloud Reputation (Current)

Correct Answer: A

Latest 5V0-91.20 Dumps 5V0-91.20 Exam Questions

5V0-91.20 Braindumps