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:

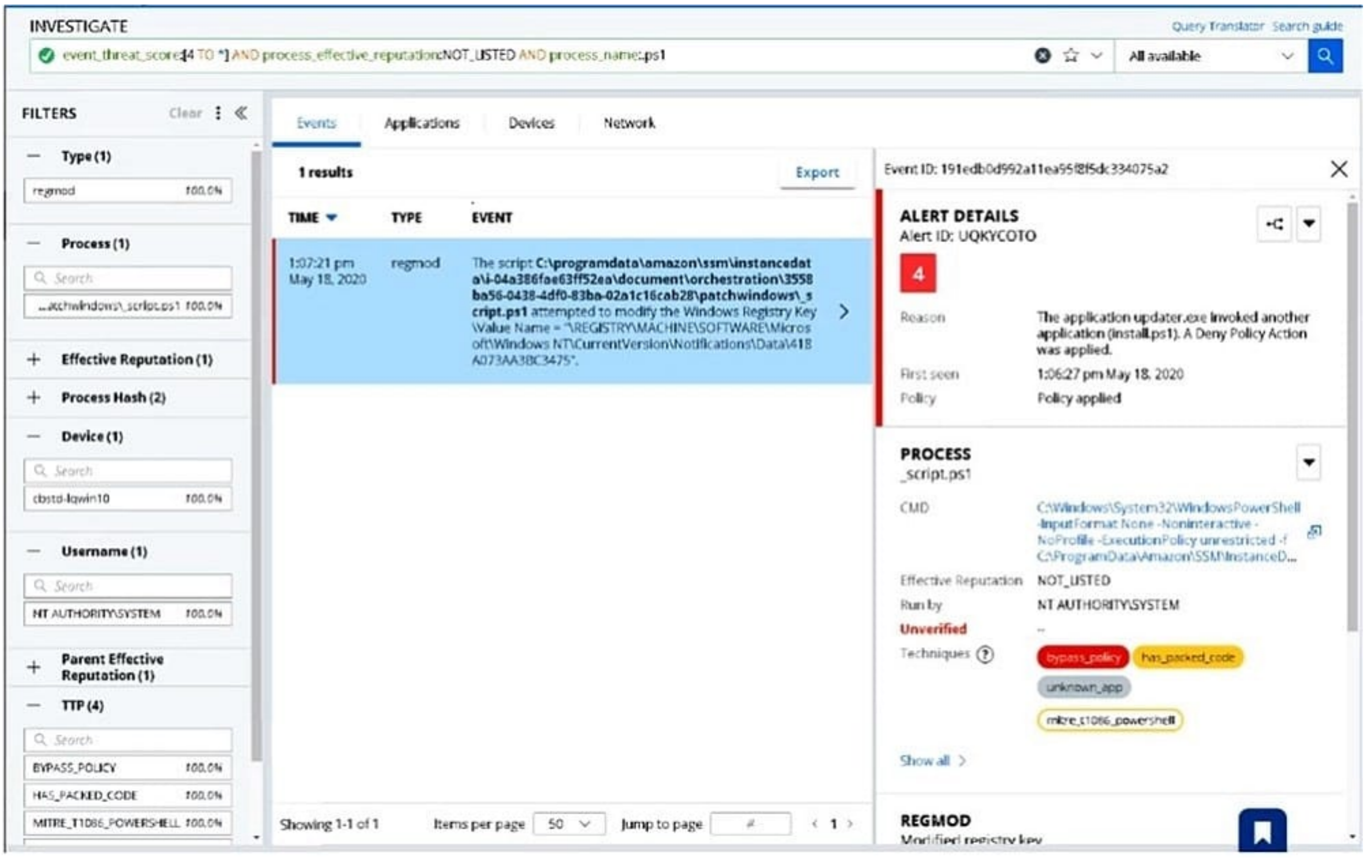
https://www.passapply.com/5v0-91-20.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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



event_threat_score:[4 TO *] AND process_effective_reputation:NOT_LISTED AND process_name:_ps1

Filters:

- Type (1): regmod 100.0%
- Process (1): ...atchwindows_script.ps1 100.0%
- Effective Reputation (1)
- Process Hash (2)
- Device (1): cbstd-lqwin10 100.0%
- Username (1): NT AUTHORITY\SYSTEM 100.0%
- Parent Effective Reputation (1)
- TTP (4): BYPASS_POLICY 100.0%; HAS_PACKED_CODE 100.0%; MITRE_T1086_POWERSHELL 100.0%

1 results

TIME	TYPE	EVENT
1:07:21 pm May 18, 2020	regmod	The script **C:\programdata\amazon\ssm\instancedata\i-04a386fae63ff52ea\document\orchestration\3558ba56-0438-4df0-83ba-02a1c16cab28\patchwindows_script.ps1** attempted to modify the Windows Registry Key \Value Name = "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475".

Event ID: 191edb0d992a11ea95f8f5dc334075a2

ALERT DETAILS
Alert ID: UQKYCOTO

4

Reason	The application updater.exe invoked another application (install.ps1). A Deny Policy Action was applied.
First seen	1:06:27 pm May 18, 2020
Policy	Policy applied

PROCESS
_script.ps1

CMD	C:\Windows\System32\WindowsPowerShell -InputFormat None -Noninteractive -NoProfile -ExecutionPolicy unrestricted -f C:\ProgramData\Amazon\SSM\InstanceD...
Effective Reputation	NOT_LISTED
Run by	NT AUTHORITY\SYSTEM
Unverified	--
Techniques	bypass_policy has_packed_code unknown_app mitre_t1086_powershell

REGMOD
Modified registry key

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 2

An administrator receives an alert with the TTP DATA_TO_ENCRYPTION.

What is known about the alert based on this TTP even if other parts of the alert are unknown?

A. A process attempted to delete encrypted data on the disk.

B. A process attempted to write a file to the disk.

C. A process attempted to modify a monitored file written by the sensor.

D. A process attempted to transfer encrypted data on the disk over the network.

Correct Answer: B

QUESTION 3

An analyst has investigated multiple alerts on a number of HR workstations and found that java.exe is attempting to PowerShell. Of the Windows workstations in question, the analyst has also found that Java is installed in multiple locations.

The analyst needs to block java.exe from this type of operation.

Which rule meets this need?

A. **/java.exe --> Invokes an untrusted process --> Terminate process

B. **/Program Files/*/java.exe--> Invokes an untrusted process --> Deny operation

C. **\Program Files*\java.exe --> Invokes a command interpreter --> Terminate process

D. **\java.exe --> Invokes a command interpreter --> Deny operation

Correct Answer: C

QUESTION 4

An active compromise is detected on an endpoint. Due to current policies, the compromise was detected but not terminated.

What would be an appropriate action to end the current communication between the device and the attacker?

A. Uninstall the sensor

B. Place the system into bypass mode

C. Place the system into Quarantine D. Remotely scan the endpoint

Correct Answer: B

QUESTION 5

Carbon Black App Control maintains an inventory of all interesting (executable) files on endpoints where the agent is installed.

What is the initial inventory procedure called, and how can this process be triggered?

A. Inventorying; enable Discovery mode

B. Baselining; install the agent

C. Discovery; place agent into Disabled mode

D. Initialization; move agent out of Disabled mode

Correct Answer: A