

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. The alert is tied to an unusual process name. When navigating to the binary details page, for the binary used in the alert, the analyst sees the following:

BINARY DETAILS
Get detailed information about a binary

1EE3D7C80D075D64F97D04D036E558043F2F6BC959C87CD580A6D53896B96A0F Download Add to

MD5: 83762e18db29b51a804a9e312d0ed99c
First seen as: powershell.exe
First seen: 11:05:06 am Mar 8, 2020
signature status: signed, verified, trusted, os, catalog, signed
Publisher name: Microsoft Windows ADD
Reputation: TRUSTED_WHITE_LIST

General	
OS:	WINDOWS
Architecture:	x86
Size:	421KB

Digital Signature	
Signature Status:	signed, verified, trusted, os, catalog, signed
Publisher name:	Microsoft Windows
Signed time:	1:22:00 am Sep 15, 2018
Issuer:	Microsoft Windows Production PCA 2011

Paths	
c:\windows\system64\windowspowershell\v1.0\powershell.exe	

File Details	
File description:	Windows PowerShell
File Version:	10.0.17763.1 (WinBuild.160101.0800)
Original filename:	Powershell.exe
Internal filename:	POWERSHELL
Company name:	Microsoft Corporation
Product name:	Microsoft Windows Operating System
Product version:	10.0.17763.1
Legal copyright:	© Microsoft Corporation. All rights reserved.

Endpoints	
First seen:	CBENT-WKSH at 11:05:06 am Mar 8, 2020
Last seen:	CBENT-WKSH at 11:05:06 am Mar 8, 2020
Seen on:	1 Devices

The analyst wants to find any instances of this process executing regardless of the process name used.

Which two details from the binary can be used to search for the application regardless of the seen name? (Choose two.)

- A. The binary's hash
- B. The path
- C. The original filename
- D. The product version
- E. The publisher name

Correct Answer: BD

QUESTION 2

How often do watchlists run?

- A. Every 10 minutes
- B. Every 5 minutes
- C. Watchlists can be configured to run at scheduled intervals

D. Every 30 minutes

Correct Answer: C

QUESTION 3

When dismissing alerts, when should an administrator select "If alert occurs in the future, automatically dismiss it from all devices"?

- A. When the administrator wishes to mark the alert instance as a false positive
- B. When the administrator wishes to be notified again to this behavior
- C. When the administrator wishes to apply this action to all future alerts from the device
- D. When the administrator wishes to remove the alert

Correct Answer: C

QUESTION 4

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 5

Management has directed that the SOC team be enabled to create global file bans via the App Control API.

How would this be configured in the App Control Console?

- A. Create a Role, map to corresponding SOC group, and add permission "Manage files" to Role.
- B. Add permission "Manage files" and create an API token for each SOC user.
- C. Create a Role, map to the corresponding SOC group, add permission "Manage files", and create API token for the Role.
- D. Create a Role, map it to the corresponding SOC group, add permission "Manage files" to Role, and create an API token for each user in group.

Correct Answer: C

[5V0-91.20 PDF Dumps](#)

[5V0-91.20 Practice Test](#)

[5V0-91.20 Exam Questions](#)