NSE5_EDR-5.0$^{\text{Q\&As}}$

Fortinet NSE 5 - FortiEDR 5.0

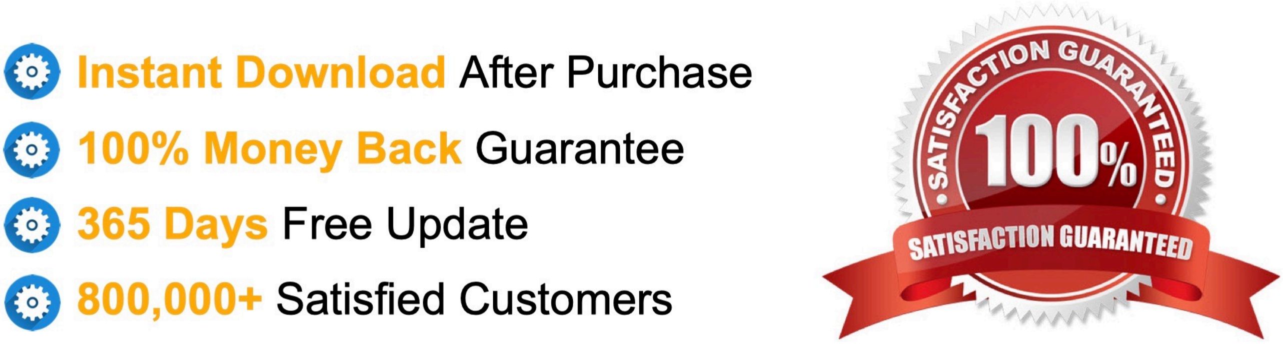
Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

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

https://www.geekcert.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

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


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

When installing a FortiEDR collector, why is a `Registration Password\\' for collectors needed?

A. To restrict installation and uninstallation of collectors

B. To verify Fortinet support request

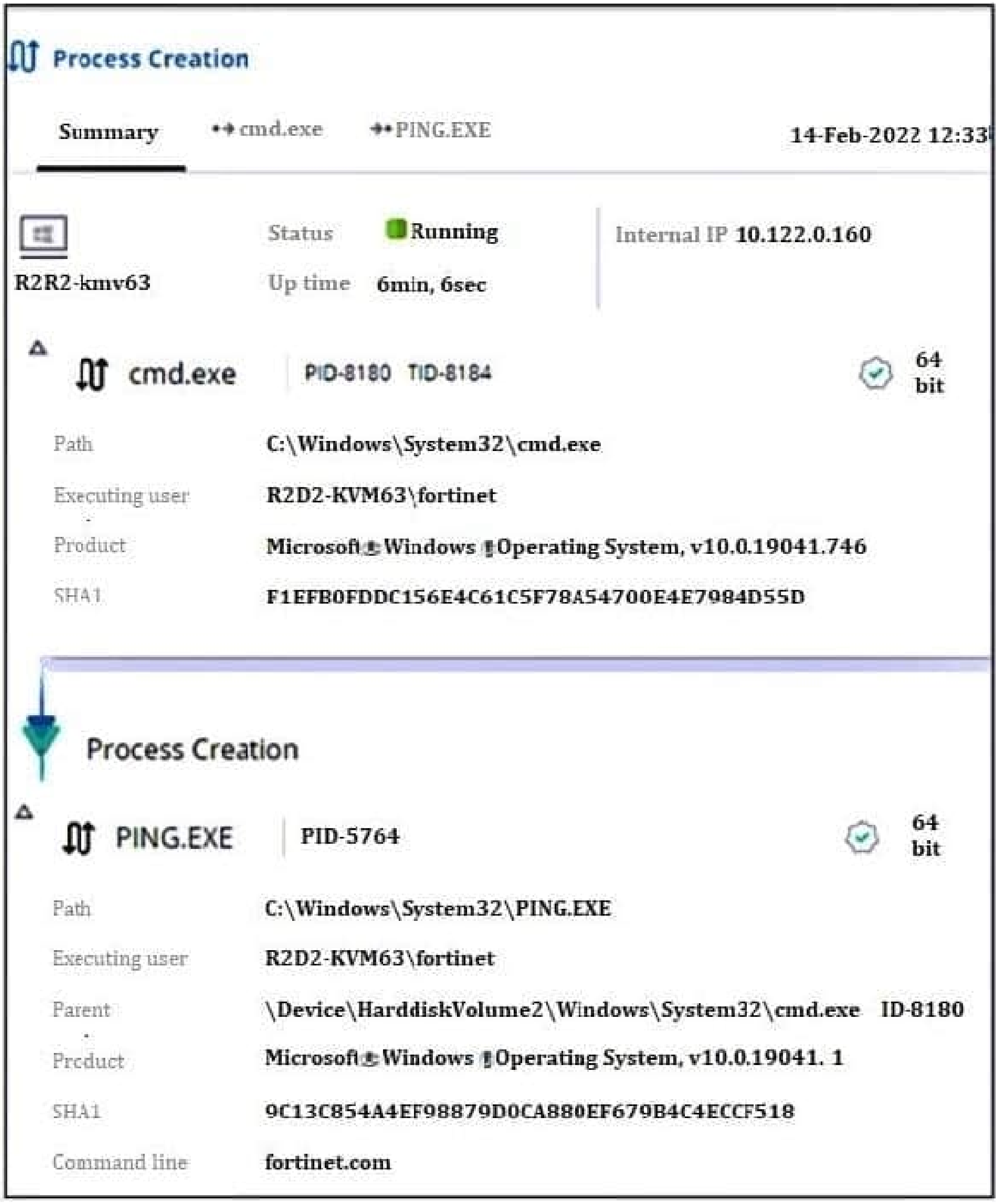
C. To restrict access to the management console

D. To verify new group assignment

Correct Answer: A

QUESTION 2

Refer to the exhibit.



Process Creation

Summary | cmd.exe | PING.EXE | 14-Feb-2022 12:33

R2R2-kmv63

Status	Running
Up time	6min, 6sec
Internal IP	10.122.0.160

cmd.exe | PID-8180 TID-8184 | 64 bit

Path	C:\Windows\System32\cmd.exe
Executing user	R2D2-KVM63\fortinet
Product	Microsoft® Windows® Operating System, v10.0.19041.746
SHA1	F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D

Process Creation

PING.EXE | PID-5764 | 64 bit

Path	C:\Windows\System32\PING.EXE
Executing user	R2D2-KVM63\fortinet
Parent	\Device\HarddiskVolume2\Windows\System32\cmd.exe ID-8180
Prcduct	Microsoft® Windows® Operating System, v10.0.19041. 1
SHA1	9C13C854A4EF98879D0CA880EF679B4C4ECCF518
Command line	fortinet.com

Based on the threat hunting event details shown in the exhibit, which two statements about the event are true? (Choose two.)

A. The PING EXE process was blocked

B. The user fortinet has executed a ping command

C. The activity event is associated with the file action

D. There are no MITRE details available for this event

Correct Answer: BD

QUESTION 3

What is the benefit of using file hash along with the file name in a threat hunting repository search?

A. It helps to make sure the hash is really a malware

B. It helps to check the malware even if the malware variant uses a different file name

C. It helps to find if some instances of the hash are actually associated with a different file

D. It helps locate a file as threat hunting only allows hash search

Correct Answer: B

QUESTION 4

What is the role of a collector in the communication control policy?

A. A collector blocks unsafe applications from running

B. A collector is used to change the reputation score of any application that collector runs

C. A collector records applications that communicate externally

D. A collector can quarantine unsafe applications from communicating

Correct Answer: C

QUESTION 5

What is the purpose of the Threat Hunting feature?

A. Delete any file from any collector in the organization

B. Find and delete all instances of a known malicious file or hash in the organization

C. Identify all instances of a known malicious file or hash and notify affected users

D. Execute playbooks to isolate affected collectors in the organization

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it\\'s a search and destroy operation."

Latest NSE5_EDR-5.0 Dumps | NSE5_EDR-5.0 PDF Dumps | NSE5_EDR-5.0 Study Guide