NSE5_EDR-5.0 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:

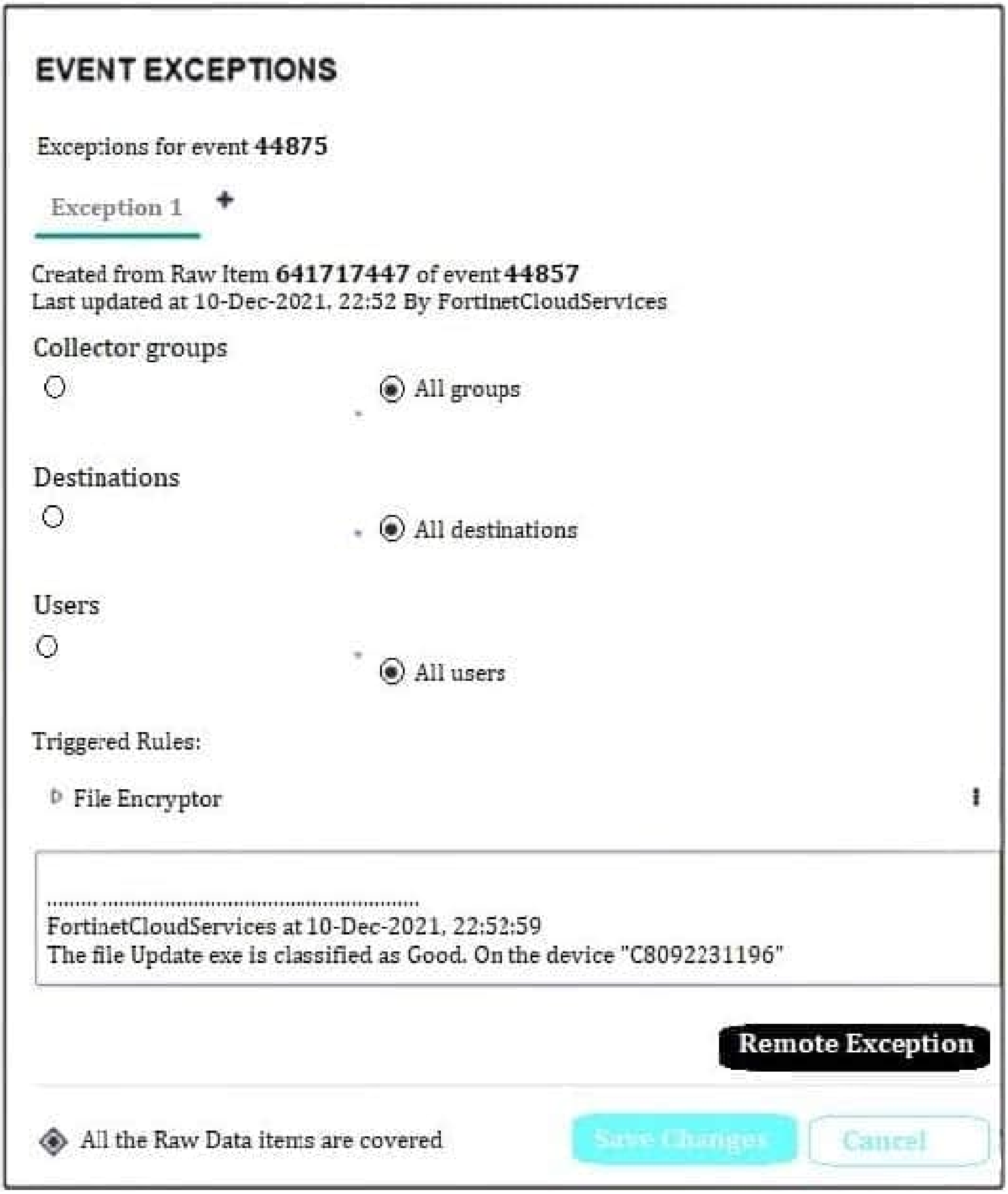
https://www.leads4pass.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.



EVENT EXCEPTIONS

Exceptions for event 44875

Exception 1 +

Created from Raw Item 641717447 of event 44857
Last updated at 10-Dec-2021, 22:52 By FortinetCloudServices

Collector groups
○ ● All groups

Destinations
○ ● All destinations

Users
○ ● All users

Triggered Rules:

File Encryptor

FortinetCloudServices at 10-Dec-2021, 22:52:59
The file Update exe is classified as Good. On the device "C8092231196"

Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

A. A partial exception is applied to this event

B. FCS playbooks is enabled by Fortinet support

C. The exception is applied only on device C8092231196

D. The system owner can modify the trigger rules parameters

Correct Answer: AC

QUESTION 2

Which two criteria are requirements of integrating FortiEDR into the Fortinet Security Fabric? (Choose two.)

A. Core with Core only functionality

B. A Forensics add-on license

C. Central Manager connected to FCS

D. A valid API user with access to connectors

Correct Answer: CD

QUESTION 3

Which statement is true about the flow analyzer view in forensics?

A. It displays a graphic flow diagram.

B. Two events can be compared side-by-side.

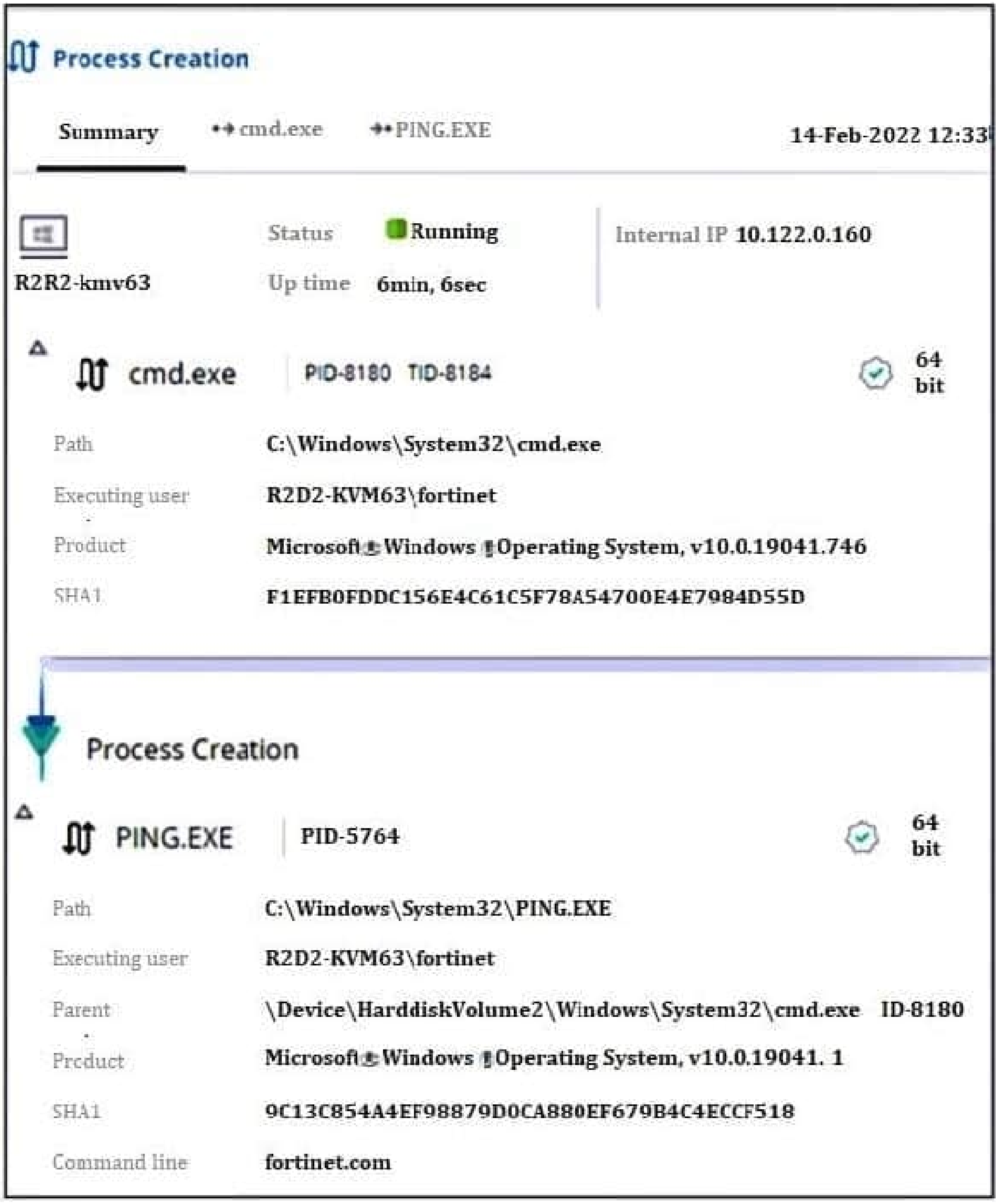
C. It shows details about processes and sub processes.

D. The stack memory of a specific device can be retrieved

Correct Answer: A

QUESTION 4

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 5

A company requires a global communication policy for a FortiEDR multi-tenant environment.

How can the administrator achieve this?

A. An administrator creates a new communication control policy and shares it with other organizations

B. A local administrator creates new a communication control policy and shares it with other organizations

C. A local administrator creates a new communication control policy and assigns it globally to all organizations

D. An administrator creates a new communication control policy for each organization

Correct Answer: C