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.pass4itsure.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

Which FortiEDR component must have JumpBox functionality to connect with FortiAnalyzer?

A. Collector

B. Core

C. Central manager

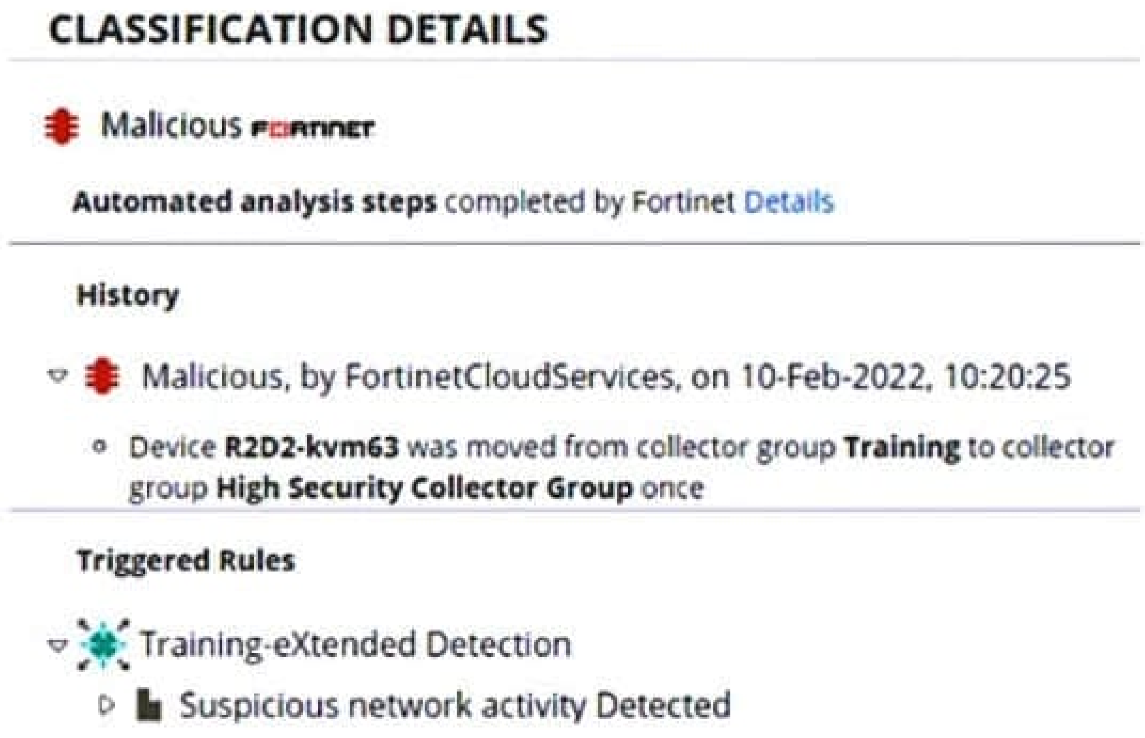
D. Aggregator

Correct Answer: B

You need an on premise CORE , with jump box functionality and valid API access, to Gate, Analyzer, NAC and or Sandbox.

QUESTION 2

Exhibit.



CLASSIFICATION DETAILS

Malicious FORTINET

Automated analysis steps completed by Fortinet Details

History

Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25

- Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

Training-eXtended Detection

Suspicious network activity Detected

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

A. The device is moved to isolation.

B. Playbooks is configured for this event.

C. The event has been blocked

D. The policy is in simulation mode

Correct Answer: BD

QUESTION 3

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

How can the administrator achieve this?

A. The local administrator can create a new exception and share it with other organizations.

B. A user account can create a new exception and share it with other organizations.

C. The administrator can create a new exception and assign it globally to all organizations.

D. The administrator can create a new exception policy for each organization hosted on FortiEDR.

Correct Answer: C

Fortiedr AdminGuide "For a multi-organization FortiEDR system, an Administrator who is assigned to All organizations (see Users) can also specify whether the exception applies to all organizations. The All organizations option applies the exception to all organizations, regardless of whether or not the security event already occurred."

QUESTION 4

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)

A. Radius

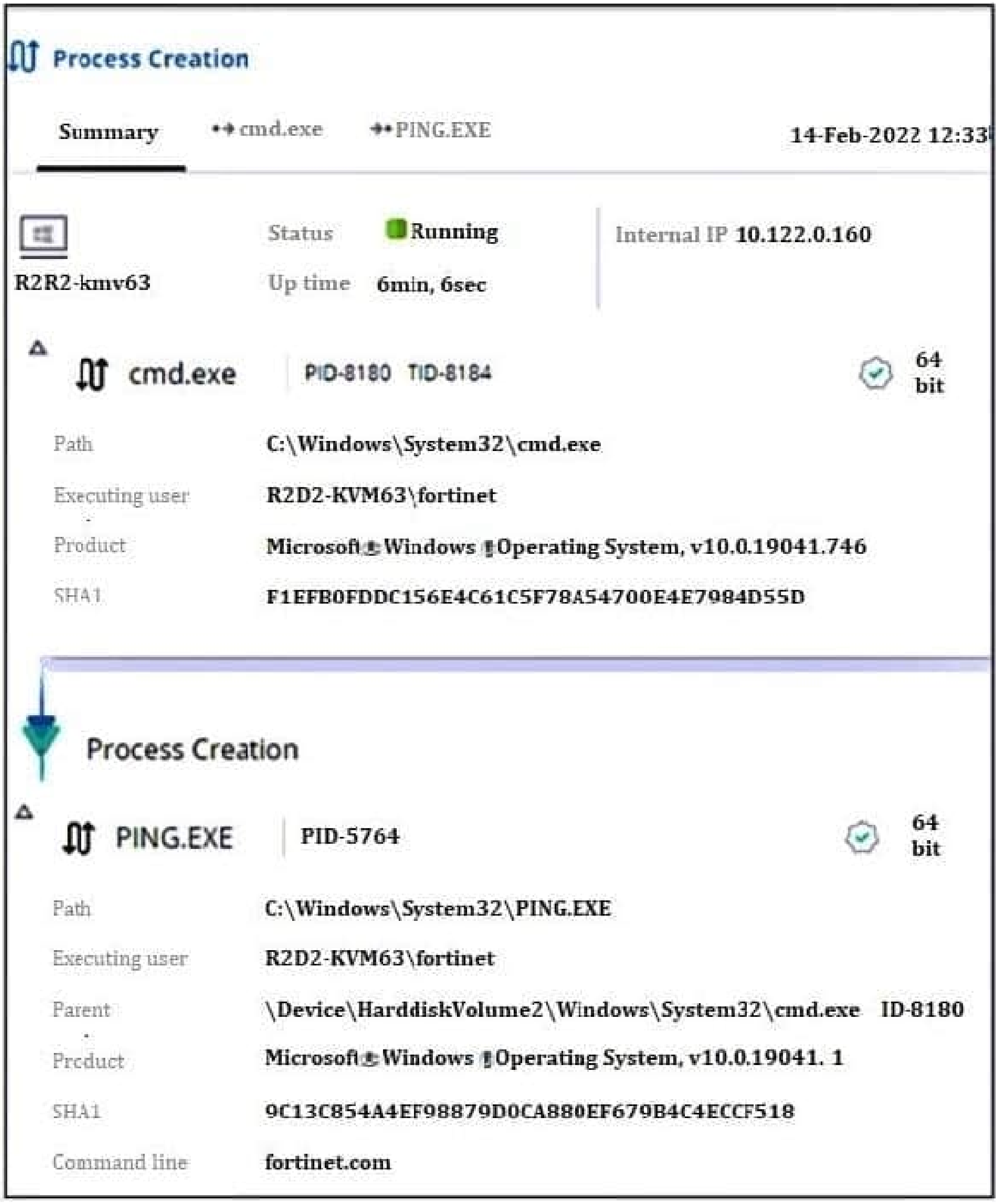
B. SAML

C. TACACS D. LDAP

Correct Answer: BD

QUESTION 5

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