Free Questions for NSE5_EDR-5.0 by certsdeals

Shared by Camacho on 04-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements about the FortiEDR solution are true? (Choose two.)

Options:

A- It provides pre-infection and post-infection protection

B- It is Windows OS only

C- It provides central management

D- It provides pant-to-point protection

Answer:

A, D

Question 2

Question Type: MultipleChoice

Which security policy has all of its rules disabled by default?

Options:

A- Device Control

B- Ransomware Prevention

C- Execution Prevention

D- Exfiltration Prevention

Answer:

B

Question 3

Question Type: MultipleChoice

Which FortiEDR component is required to find malicious files on the entire network of an organization?

Options:

A- FortiEDR Aggregator

B- FortiEDR Central Manager

C- FortiEDR Threat Hunting Repository

D- FortiEDR Core

Answer:

A

Question 4

Question Type: **MultipleChoice**

Which scripting language is supported by the FortiEDR action managed?

Options:

A- TCL

B- Python

C- Perl

D- Bash

Answer:

A

Question 5

Question Type: MultipleChoice

A FortiEDR security event is causing a performance issue with a third-parry application. What must you do first about the event?

Options:

A- Contact Fortinet support

B- Terminate the process and uninstall the third-party application

C- Immediately create an exception

D- Investigate the event to verify whether or not the application is safe

Answer:

C

Question 6

Question Type: MultipleChoice

An administrator finds a third party free software on a user's computer mat does not appear in me application list in the communication control console

Which two statements are true about this situation? (Choose two)

Options:

A- The application is allowed in all communication control policies

B- The application is ignored as the reputation score is acceptable by the security policy

C- The application has not made any connection attempts

D- The application is blocked by the security policies

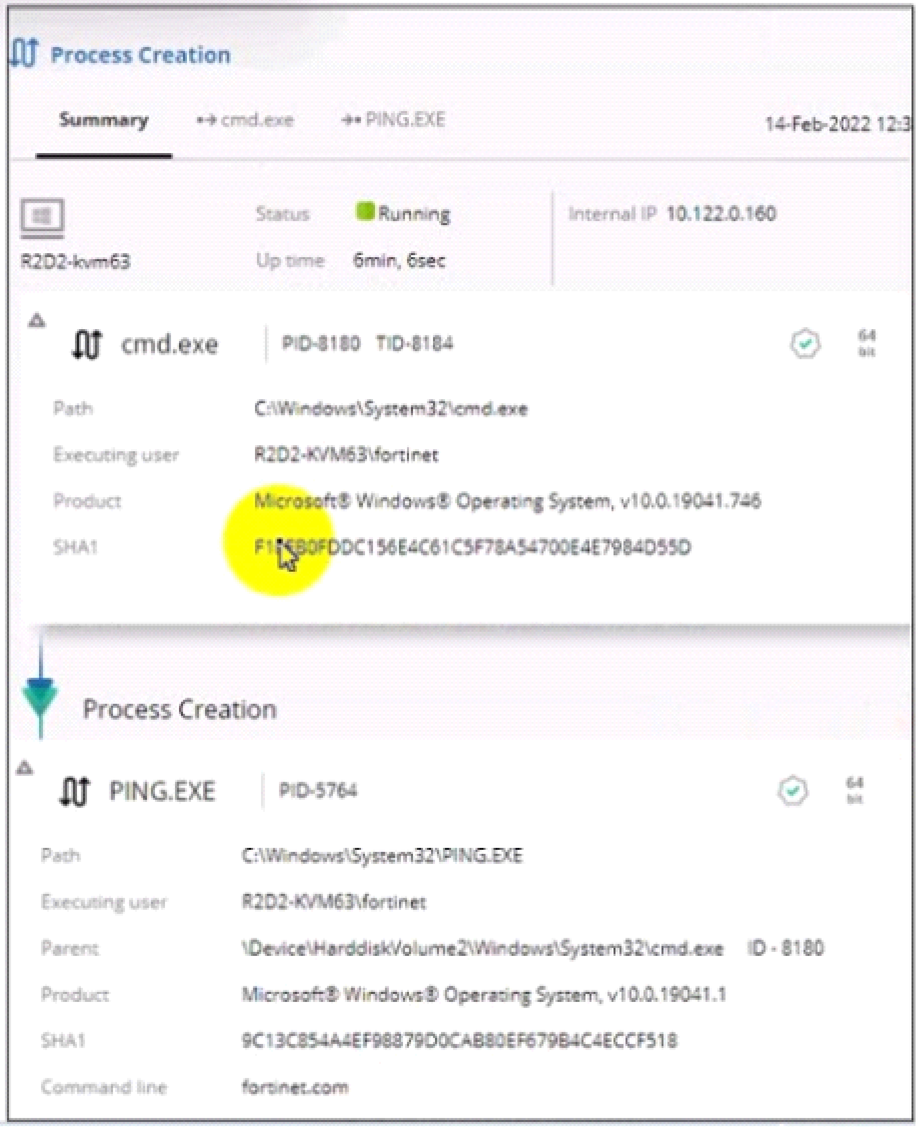
Answer:

A, D

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



Process Creation

Summary ↔ cmd.exe → PING.EXE 14-Feb-2022 12:3

R2D2-kvm63

Status 🟩 Running

Up time 6min, 6sec

Internal IP 10.122.0.160

cmd.exe | PID-8180 TID-8184

Path C:\Windows\System32\cmd.exe

Executing user R2D2-KVM63\fortinet

Product Microsoft® Windows® Operating System, v10.0.19041.746

SHA1 F1[illegible]B0FDDC156E4C61C5F78A54700E4E7984D55D

Process Creation

PING.EXE | PID-5764

Path C:\Windows\System32\PING.EXE

Executing user R2D2-KVM63\fortinet

Parent \Device\HarddiskVolume2\Windows\System32\cmd.exe ID - 8180

Product Microsoft® Windows® Operating System, v10.0.19041.1

SHA1 9C13C854A4EF98879D0CAB80EF679B4C4ECCF518

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.)

Options:

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

Answer:

A, D

Question 8

Question Type: **MultipleChoice**

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

Options:

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

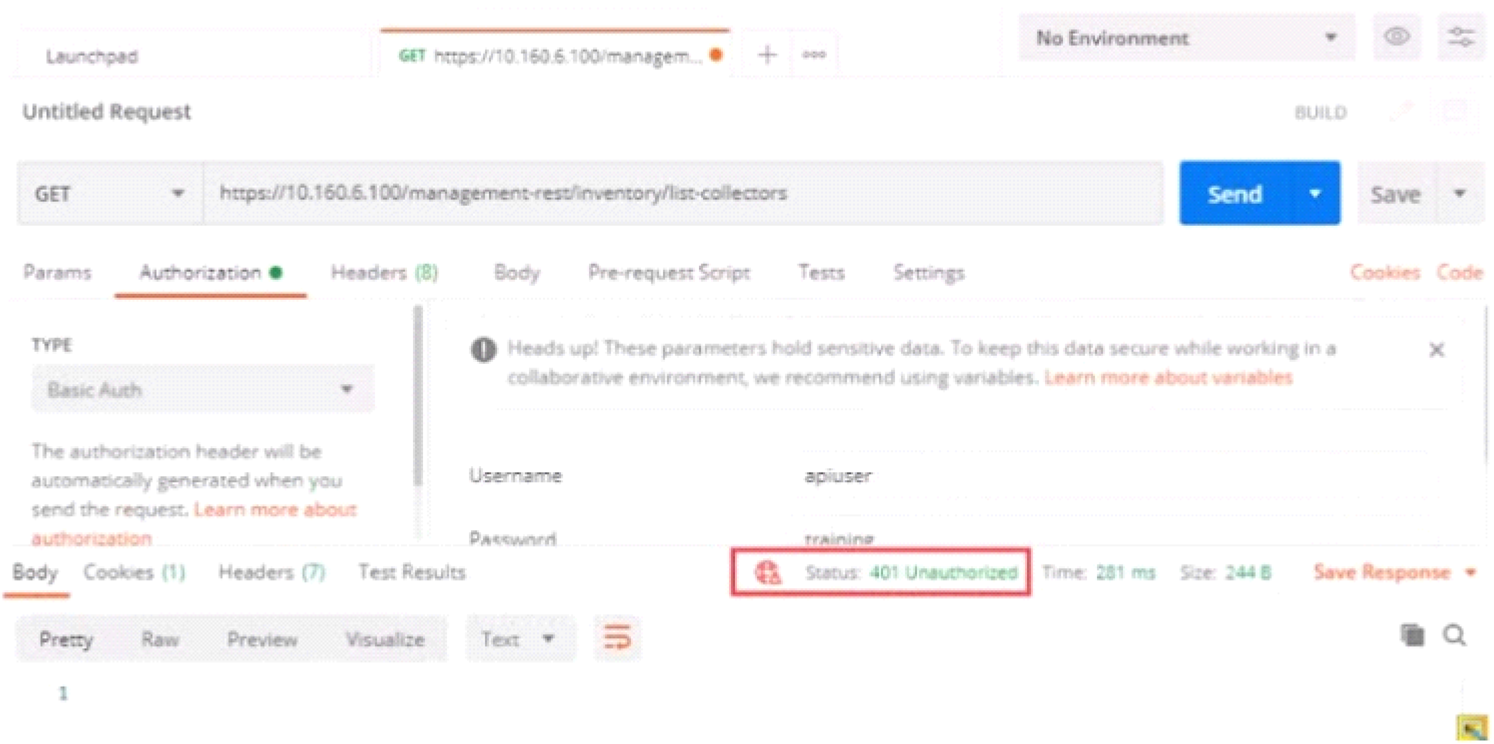
Answer:

A

Question 9

Question Type: **MultipleChoice**

Refer to the exhibit.



GET https://10.160.6.100/management-rest/inventory/list-collectors

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: apiuser

Password: training

Status: 401 Unauthorized Time: 281 ms Size: 244 B

```
1
```

Based on the postman output shown in the exhibit why is the user getting an unauthorized error?

Options:

A- The user has been assigned Admin and Rest API roles

B- FortiEDR requires a password reset the first time a user logs in

C- Postman cannot reach the central manager

D- API access is disabled on the central manager

Answer:

A

Question 10

Question Type: **MultipleChoice**

FortiXDR relies on which feature as part of its automated extended response?

Options:

A- Playbooks

B- Security Policies

C- Forensic

D- Communication Control

Answer:

B