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

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

QUESTION 1

Refer to the exhibit.

TestApplication.exe.exe (3 events)
Malicious
15-Feb-2022, 13:31:39
5894314
R2D2-kvm63
TestApplication.exe.exe
Malicious
8.8.8.8
15-Feb-2022, 13:31:39
15-Feb-2022, 13:31:39
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc
CLASSIFICATION DETAILS
Malicious
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown
History
Malicious, by Fortinet, on 15-Feb-2022, 13:31:41
Triggered Rules
Exfiltration Prevention
Invalid Checksum - Connection Attempt from Application wi...
Malicious File Detected
Suspicious Packer - Activity by an Application packed by a S...
Writeable Code - Identified an Executable with Writable Code

TestApplication.exe.exe (3 events)
Malicious
5894314
R2D2-kvm63
TestApplication.exe.exe
Malicious
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc

15-Feb-2022, 13:31:39
8.8.8.8
15-Feb-2022, 13:31:39
15-Feb-2022, 13:31:39
CLASSIFICATION DETAILS
Malicious
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown
History
Malicious, by Fortinet, on 15-Feb-2022, 13:31:41
Triggered Rules
Exfiltration Prevention
Invalid Checksum - Connection Attempt from Application wi...
Malicious File Detected
Suspicious Packer - Activity by an Application packed by a S...
Writeable Code - Identified an Executable with Writable Code

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

A. The NGAV policy has blocked TestApplication exe

B. TestApplication exe is sophisticated malware

C. The user was able to launch TestApplication exe

D. FCS classified the event as malicious

Correct Answer: BC

QUESTION 2

An administrator finds that a newly installed collector does not display on the INVENTORY tab in the central manager.

What two troubleshooting steps must the administrator perform? (Choose two.)

A. Export the collector logs from the central manager.

B. Verify the central manager has connectivity to FCS.

C. Verify TCP ports 8081 and 555 are open.

D. Check if the FortiEDR services are running on the collector device.

Correct Answer: CD

QUESTION 3

Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

A. FortiNAC

B. FortiGate

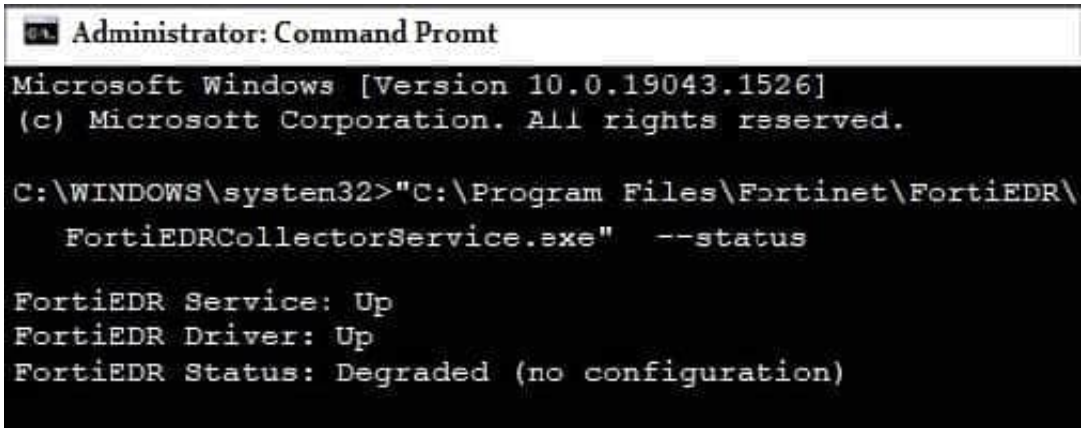
C. FortiSiem

D. FortiSandbox

Correct Answer: AB

QUESTION 4

Refer to the exhibit.



Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

A. The collector device has windows firewall enabled

B. The collector has been installed with an incorrect port number

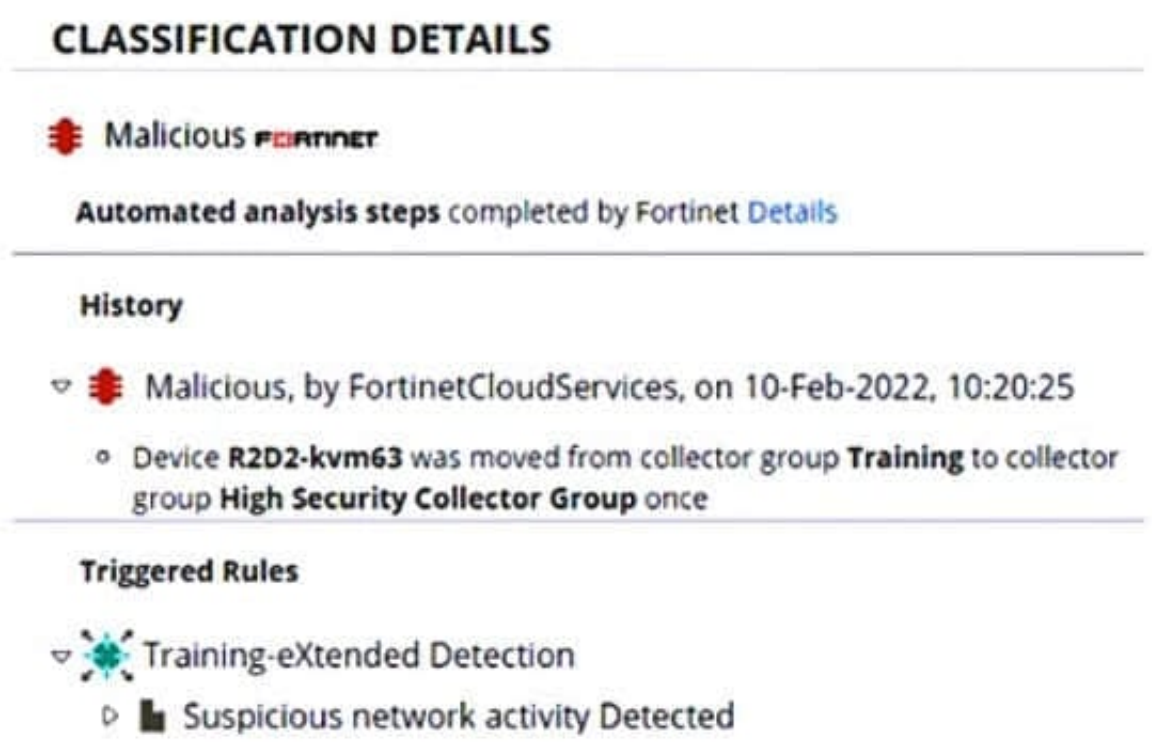
C. The collector has been installed with an incorrect registration password

D. The collector device cannot reach the central manager

Correct Answer: BC

QUESTION 5

Exhibit.



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

NSE5_EDR-5.0 VCE Dumps NSE5_EDR-5.0 Exam Questions NSE5_EDR-5.0 Braindumps