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

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

QUESTION 1

Which threat hunting profile is the most resource intensive?

A. Comprehensive

B. Inventory

C. Default

D. Standard Collection

Correct Answer: A

QUESTION 2

Refer to the exhibit.

Based on the threat hunting query shown in the exhibit which of the following is true?

A. RDP connections will be blocked and classified as suspicious

B. A security event will be triggered when the device attempts a RDP connection

C. This query is included in other organizations

D. The query will only check for network category

Correct Answer: B

QUESTION 3

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 4

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 5

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 6

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

A. FortiEDR Aggregator

B. FortiEDR Central Manager

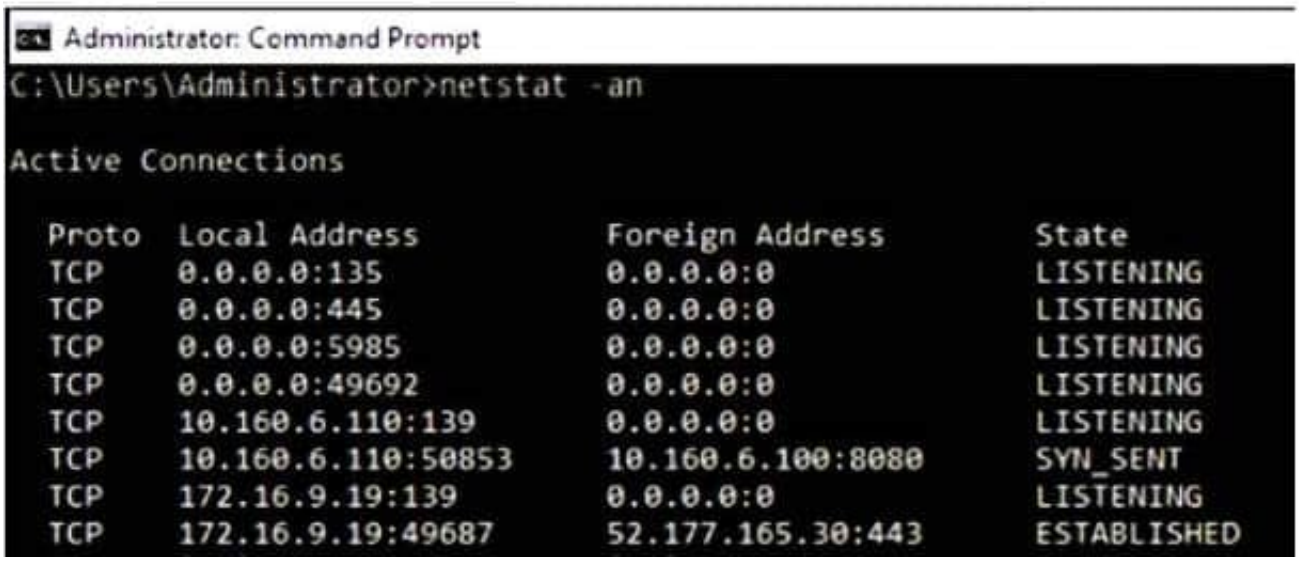
C. FortiEDR Threat Hunting Repository

D. FortiEDR Core

Correct Answer: C

QUESTION 7

Refer to the exhibits.



The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP

address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

A. Reinstall collector agent and use port 443

B. Reinstall collector agent and use port 8081

C. Reinstall collector agent and use port 555

D. Reinstall collector agent and use port 6514

Correct Answer: B

QUESTION 8

How does FortiEDR implement post-infection protection?

A. By preventing data exfiltration or encryption even after a breach occurs

B. By using methods used by traditional EDR

C. By insurance against ransomware

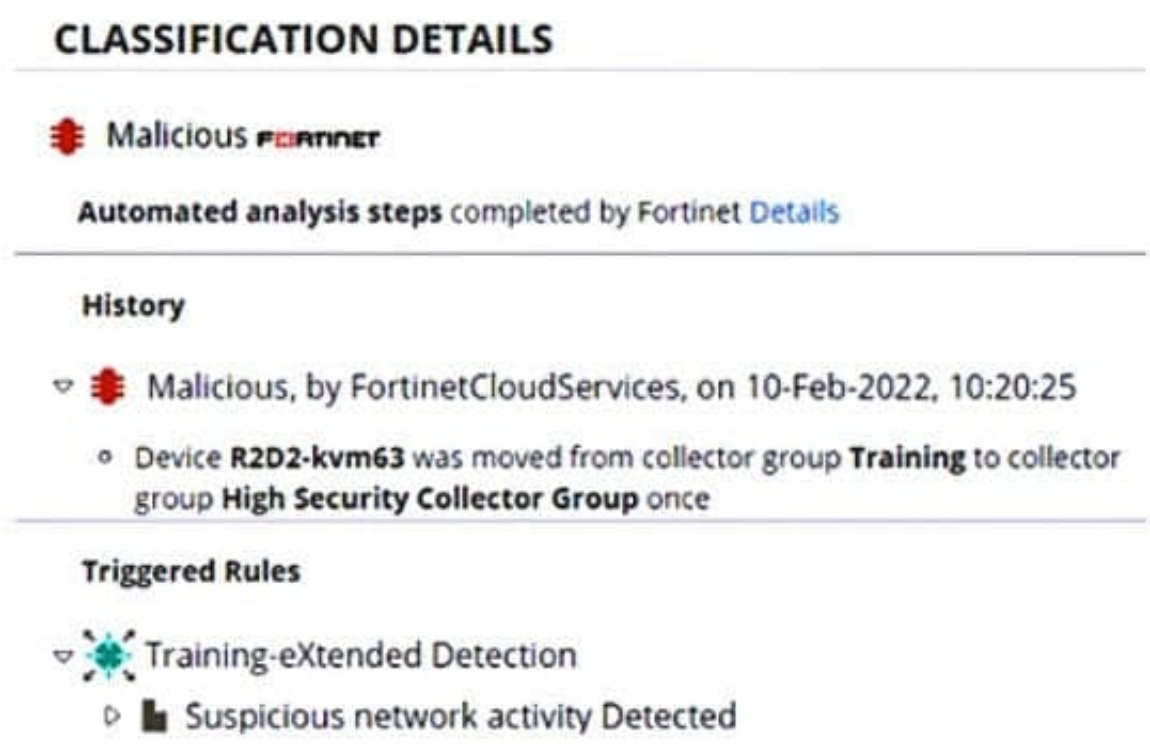
D. By real-time filtering to prevent malware from executing

Correct Answer: A

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf

QUESTION 9

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.

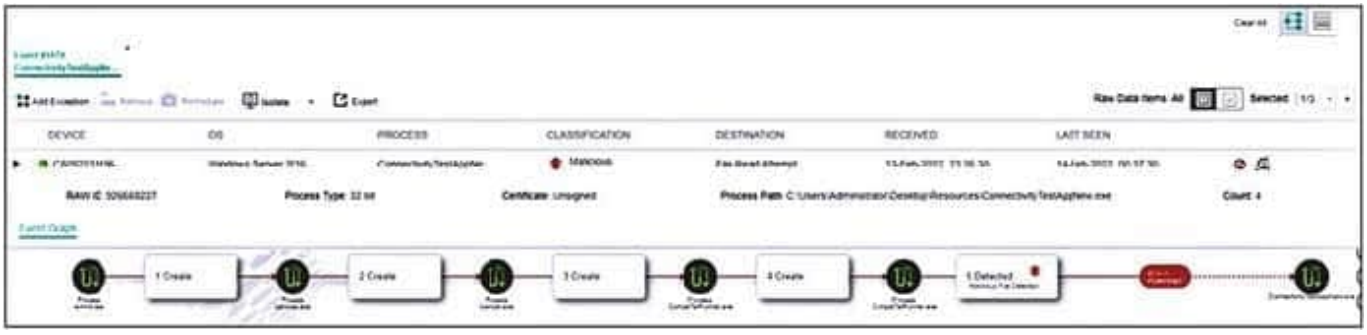
C. The event has been blocked

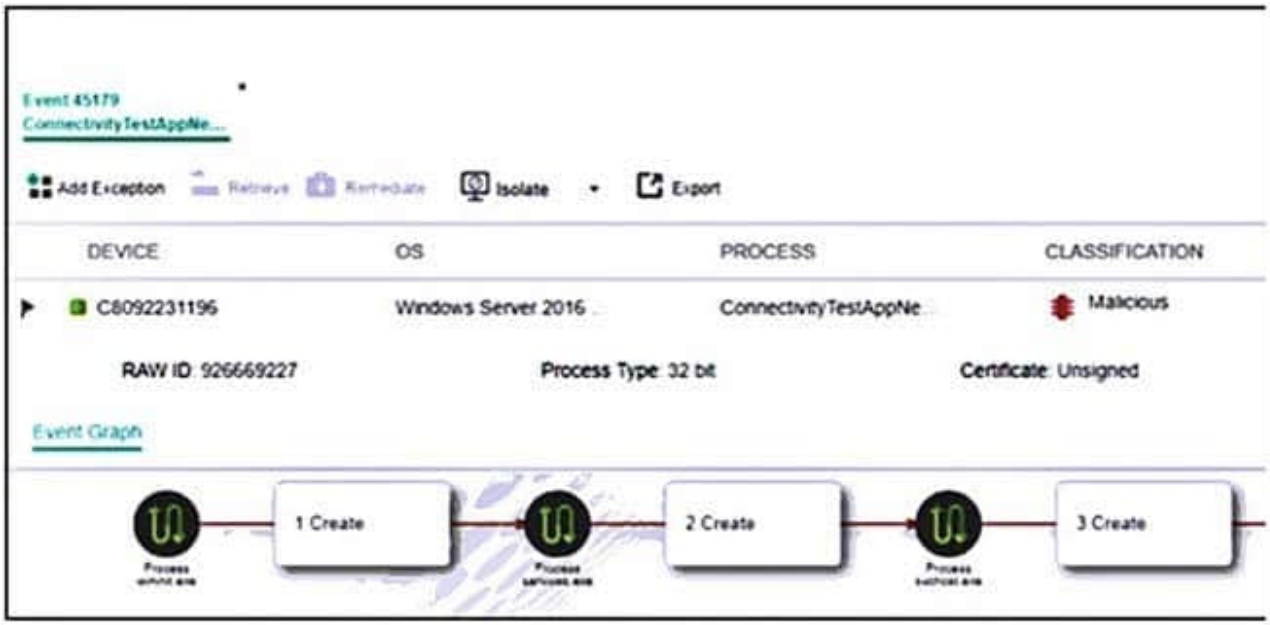
D. The policy is in simulation mode

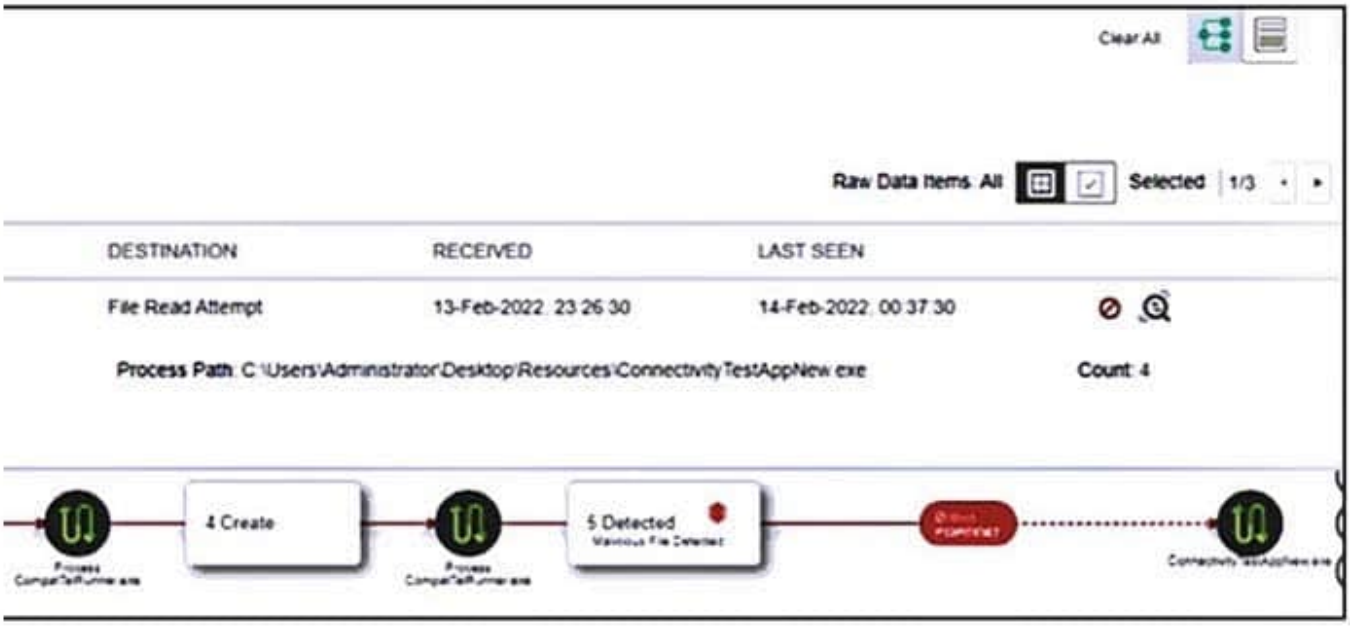
Correct Answer: BD

QUESTION 10

Exhibit.







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

A. The device cannot be remediated

B. The event was blocked because the certificate is unsigned

C. Device C8092231196 has been isolated

D. The execution prevention policy has blocked this event.

Correct Answer: AD