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.passapply.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 exhibits.

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilia application?

A. Deny application in Finance policy

B. Assign Finance policy to DBA group

C. Assign Finance policy to Default Collector Group

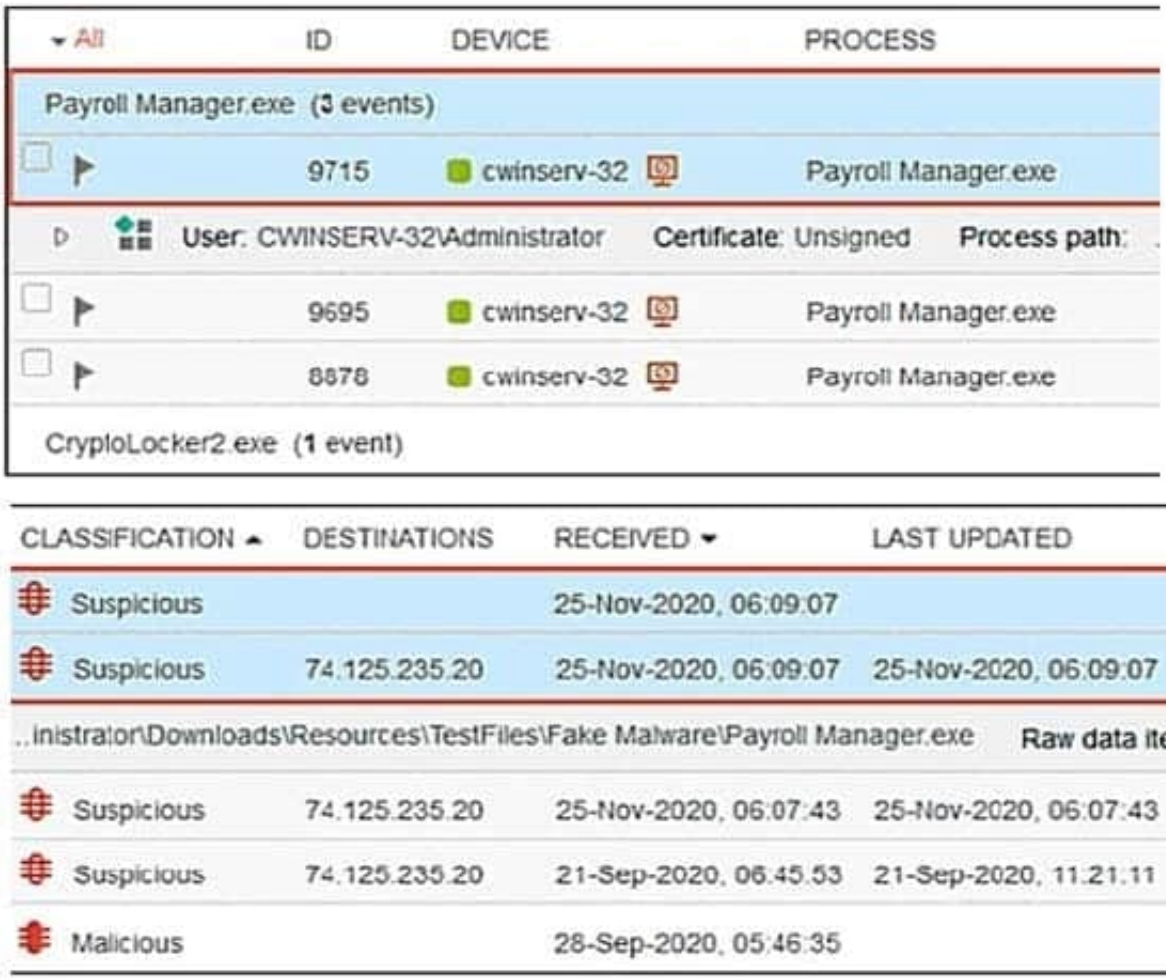
D. Assign Simulation Communication Control Policy to DBA group

Correct Answer: B

QUESTION 2

Refer to the exhibit.

The exhibit shows an event viewer.



What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C

QUESTION 3

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 4

What is the purpose of the Threat Hunting feature?

A. Delete any file from any collector in the organization

B. Find and delete all instances of a known malicious file or hash in the organization

C. Identify all instances of a known malicious file or hash and notify affected users

D. Execute playbooks to isolate affected collectors in the organization

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it\\'s a search and destroy operation."

QUESTION 5

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.

NSE5_EDR-5.0 PDF Dumps | NSE5_EDR-5.0 VCE Dumps | NSE5_EDR-5.0 Study Guide