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.pass2lead.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 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 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

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 5

What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

A. The core is responsible for all classifications if FCS playbooks are disabled

B. The core only assigns a classification if FCS is not available

C. FCS revises the classification of the core based on its database

D. FCS is responsible for all classifications

Correct Answer: C

QUESTION 6

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

How can the administrator achieve this?

A. An administrator creates a new communication control policy and shares it with other organizations

B. A local administrator creates new a communication control policy and shares it with other organizations

C. A local administrator creates a new communication control policy and assigns it globally to all organizations

D. An administrator creates a new communication control policy for each organization

Correct Answer: C

QUESTION 7

Which two types of traffic are allowed while the device is in isolation mode? (Choose two.)

A. Outgoing SSH connections

B. HTTP sessions

C. ICMP sessions D. Incoming RDP connections

Correct Answer: CD

QUESTION 8

An administrator needs to restrict access to the ADMINISTRATION tab in the central manager for a specific account. What role should the administrator assign to this account?

A. Admin

B. User

C. Local Admin

D. REST API

Correct Answer: B

QUESTION 9

Which threat hunting profile is the most resource intensive?

A. Comprehensive

B. Inventory

C. Default

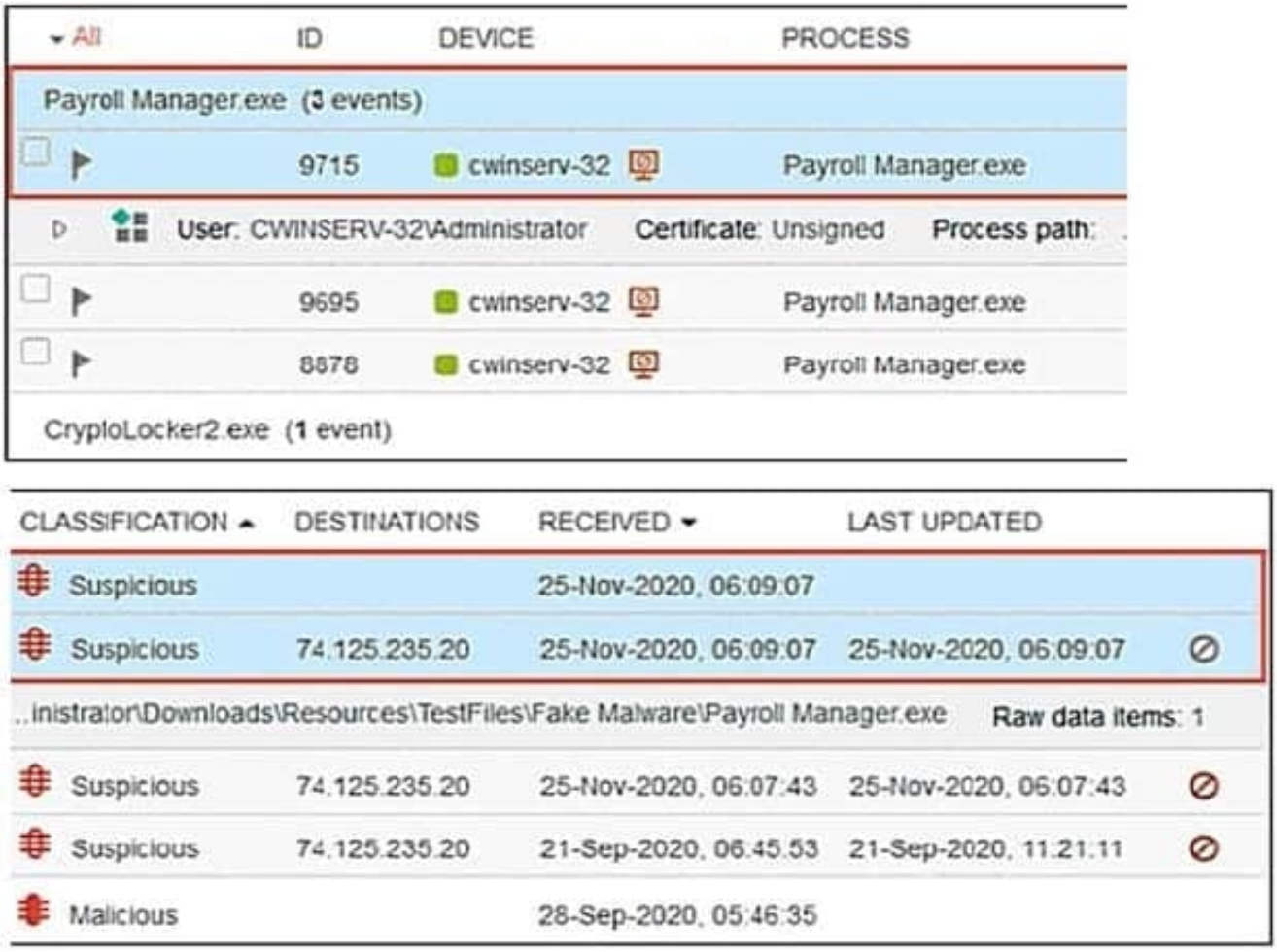
D. Standard Collection

Correct Answer: A

QUESTION 10

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