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

A. FortiNAC

B. FortiGate

C. FortiSiem

D. FortiSandbox

Correct Answer: AB

QUESTION 2

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

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

Correct Answer: C

QUESTION 3

Which statement is true about the flow analyzer view in forensics?

A. It displays a graphic flow diagram.

B. Two events can be compared side-by-side.

C. It shows details about processes and sub processes.

D. The stack memory of a specific device can be retrieved

Correct Answer: A

QUESTION 4

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 5

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."