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 two events can trigger FortiEDR NGAV policy violations? (Choose two.)

A. When a malicious file attempts to communicate externally

B. When a malicious file is executed

C. When a malicious file is read

D. When a malicious file attempts to access data

Correct Answer: BC

NGAV reacts when a file is Saved, Read, or Executed Page 79 of the guide

QUESTION 2

Refer to the exhibit.

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

A. The PING EXE process was blocked

B. The user fortinet has executed a ping command

C. The activity event is associated with the file action

D. There are no MITRE details available for this event

Correct Answer: BD

QUESTION 3

FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks

B. Security Policies

C. Forensic

D. Communication Control

Correct Answer: A

QUESTION 4

A FortiEDR security event is causing a performance issue with a third-parry application. What must you do first about the event?

A. Contact Fortinet support

B. Terminate the process and uninstall the third-party application

C. Immediately create an exception

D. Investigate the event to verify whether or not the application is safe

Correct Answer: D

QUESTION 5

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