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

QUESTION 1

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 2

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 3

Which two statements about the FortiEDR solution are true? (Choose two.)

A. It provides pre-infection and post-infection protection

B. It is Windows OS only

C. It provides central management

D. It provides pant-to-point protection

Correct Answer: AC

QUESTION 4

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 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