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

QUESTION 1

An administrator finds a third party free software on a user\\'s computer mat does not appear in me application list in the communication control console

Which two statements are true about this situation? (Choose two)

A. The application is allowed in all communication control policies

B. The application is ignored as the reputation score is acceptable by the security policy

C. The application has not made any connection attempts

D. The application is blocked by the security policies

Correct Answer: CD

QUESTION 2

Which threat hunting profile is the most resource intensive?

A. Comprehensive

B. Inventory

C. Default

D. Standard Collection

Correct Answer: A

QUESTION 3

Which scripting language is supported by the FortiEDR action managed?

A. TCL

B. Python

C. Perl

D. Bash

Correct Answer: B

QUESTION 4

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 5

What is the benefit of using file hash along with the file name in a threat hunting repository search?

A. It helps to make sure the hash is really a malware

B. It helps to check the malware even if the malware variant uses a different file name

C. It helps to find if some instances of the hash are actually associated with a different file

D. It helps locate a file as threat hunting only allows hash search

Correct Answer: B