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:

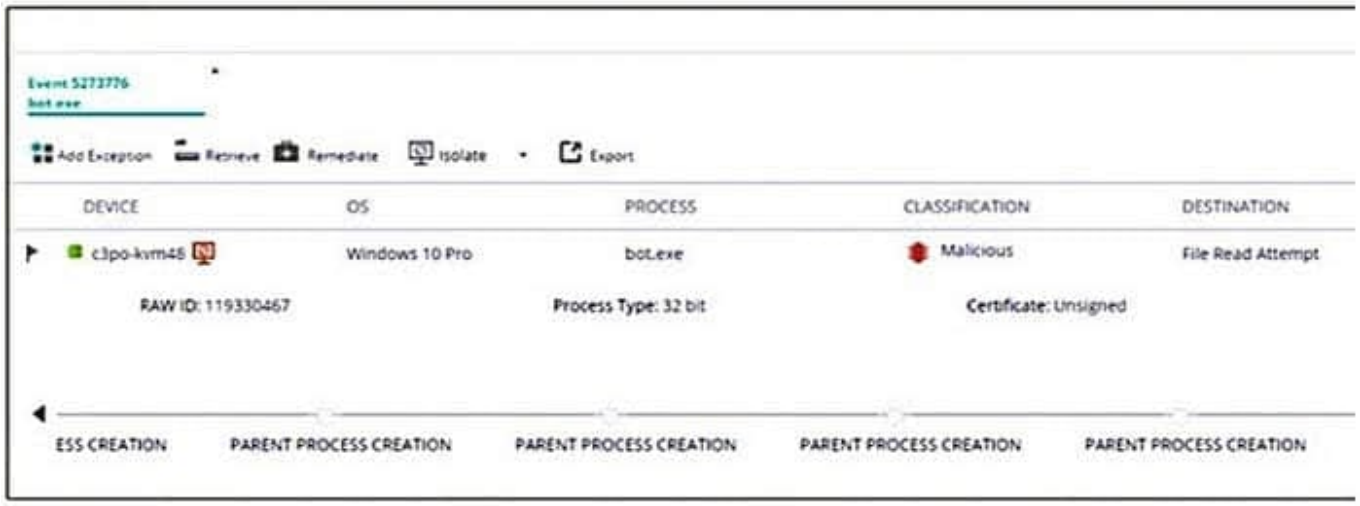
https://www.geekcert.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Exhibit.



Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

A. An exception has been created for this event

B. The forensics data is displayed m the stacks view

C. The device has been isolated

D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

QUESTION 2

Which scripting language is supported by the FortiEDR action managed?

A. TCL

B. Python

C. Perl

D. Bash

Correct Answer: B

QUESTION 3

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

How can the administrator achieve this?

A. The local administrator can create a new exception and share it with other organizations.

B. A user account can create a new exception and share it with other organizations.

C. The administrator can create a new exception and assign it globally to all organizations.

D. The administrator can create a new exception policy for each organization hosted on FortiEDR.

Correct Answer: C

Fortiedr AdminGuide "For a multi-organization FortiEDR system, an Administrator who is assigned to All organizations (see Users) can also specify whether the exception applies to all organizations. The All organizations option applies the exception to all organizations, regardless of whether or not the security event already occurred."

QUESTION 4

How does the FortiEDR approach compare to the traditional EDR? (Choose two.)

A. FortiEDR blocks threats in real time, eliminating the response gap

B. Traditional EDR is faster

C. There is no difference in response time

D. FortiEDR requires less staff

Correct Answer: AD

QUESTION 5

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