



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

Exhibit.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt	01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

Process Path: C:\Users\fortinet\Desktop\bot.exe

Count: 135

Stack: ESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, FILE READ ATTEMPT, PRE EXECUTE

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt

Process Type: 32 bit

Certificate: Unsigned

Stack: ESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION

Stack: PARENT PROCESS CREATION, FILE READ ATTEMPT, PRE EXECUTE

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 in the stacks view
- C. The device has been isolated



D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

QUESTION 2

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 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

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

QUESTION 5

Refer to the exhibit.

Save Query

Query Name: Query profile

Description: [Empty]

Tags: +

Full Query

Category: All Categories | Device: C8092231196

RemotePort3389

Community Query

Scheduled Query

Classification: Suspicious

Repeat every: 15 Minutes

Save Cancel

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



[Latest NSE5_EDR-5.0
Dumps](#)

[NSE5_EDR-5.0 PDF
Dumps](#)

[NSE5_EDR-5.0 Study
Guide](#)