



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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which threat hunting profile is the most resource intensive?

- A. Comprehensive
- B. Inventory
- C. Default
- D. Standard Collection

Correct Answer: A

QUESTION 2

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 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

Exhibit.



Event 5273776
bot.exe

Raw Data Items: All Selected | 1/1

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

RAW ID: 119330467
Process Type: 32 bit
Certificate: Unsigned
Process Path: C:\Users\fortinet\Desktop\bot.exe
Count: 135

ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE

Event 5273776
bot.exe

Raw Data Items: All Selected | 1/1

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

RAW ID: 119330467
Process Type: 32 bit
Certificate: Unsigned

ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION

Raw Data Items: All Selected | 1/1

RECEIVED	LAST SEEN
01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

Process Path: C:\Users\fortinet\Desktop\bot.exe
Count: 135

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



VCE & PDF

GeekCert.com

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

2024 Latest geekcert NSE5_EDR-5.0 PDF and VCE dumps Download

[Latest NSE5_EDR-5.0
Dumps](#)

[NSE5_EDR-5.0 Exam
Questions](#)

[NSE5_EDR-5.0 Braindumps](#)