NSE5_EDR-5.0$^{Q\&As}$

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

QUESTION 1

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.

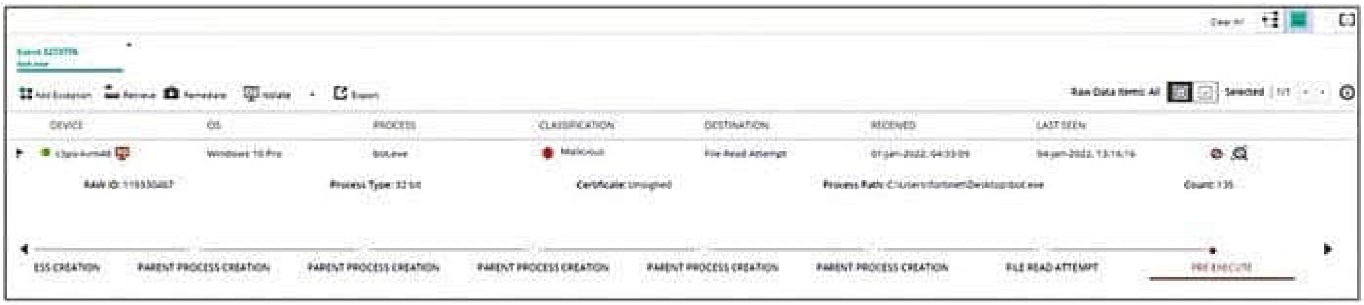
C. It shows details about processes and sub processes.

D. The stack memory of a specific device can be retrieved

Correct Answer: A

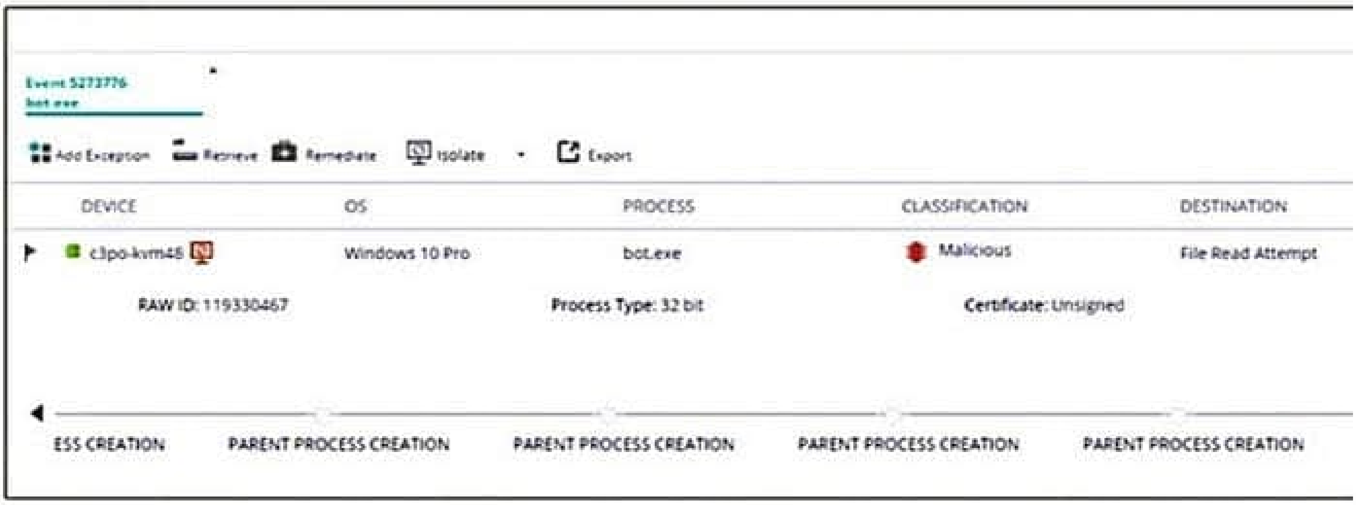
QUESTION 2

Exhibit.



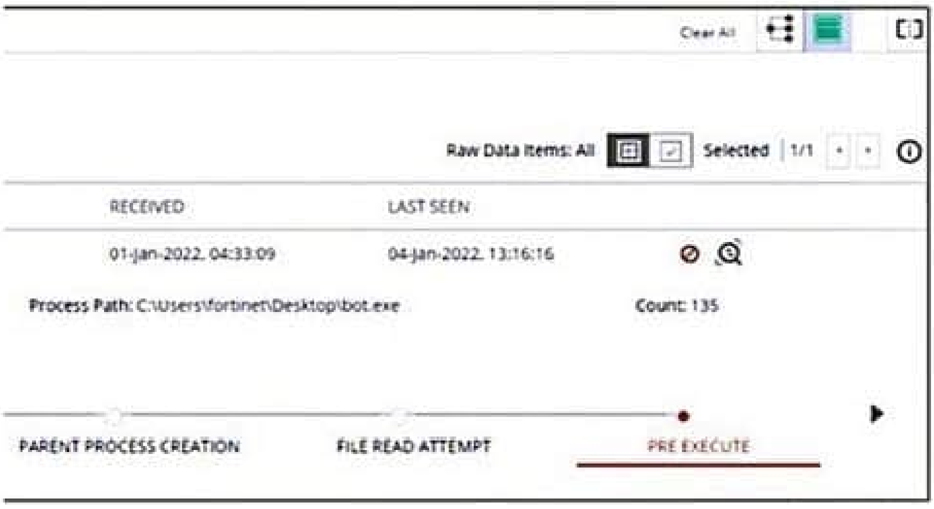
DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt	01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

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



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



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

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

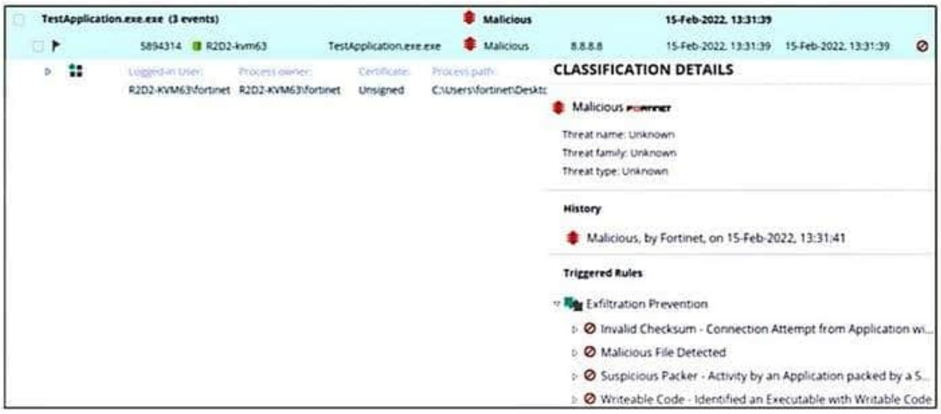
C. The device has been isolated

D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

QUESTION 3

Refer to the exhibit.



TestApplication.exe.exe (3 events) | Malicious | 15-Feb-2022, 13:31:39

5894314 | R2D2-kvm63 | TestApplication.exe.exe | Malicious | 8.8.8.8 | 15-Feb-2022, 13:31:39 | 15-Feb-2022, 13:31:39

Logged-in User: R2D2-KVM63\fortinet
Process owner: R2D2-KVM63\fortinet
Certificate: Unsigned
Process path: C:\Users\fortinet\Desktc

CLASSIFICATION DETAILS

Malicious FORTINET

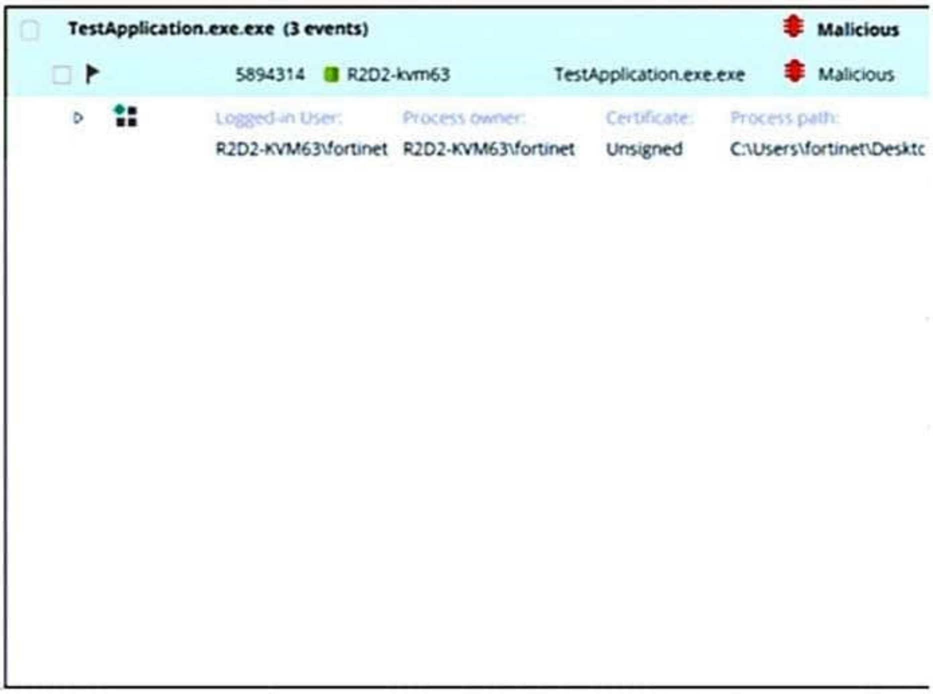
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

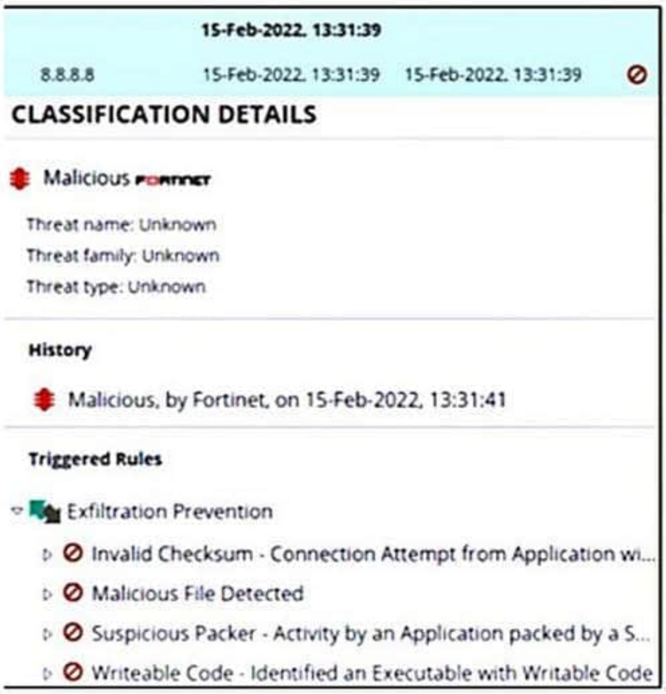
Exfiltration Prevention
- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code



TestApplication.exe.exe (3 events) | Malicious

5894314 | R2D2-kvm63 | TestApplication.exe.exe | Malicious

Logged-in User: R2D2-KVM63\fortinet
Process owner: R2D2-KVM63\fortinet
Certificate: Unsigned
Process path: C:\Users\fortinet\Desktc



15-Feb-2022, 13:31:39

8.8.8.8 | 15-Feb-2022, 13:31:39 | 15-Feb-2022, 13:31:39

CLASSIFICATION DETAILS

Malicious FORTINET

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

Exfiltration Prevention
- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code

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

A. The NGAV policy has blocked TestApplication exe

B. TestApplication exe is sophisticated malware

C. The user was able to launch TestApplication exe

D. FCS classified the event as malicious

Correct Answer: BC

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

The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious.

What playbook actions ate applied to the event?

A. Playbook actions applied to inconclusive events

B. Playbook actions applied to handled events

C. Playbook actions applied to suspicious events

D. Playbook actions applied to malicious events

Correct Answer: D