Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

NEW 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

Answer: AD

NEW QUESTION 2
What is the role of a collector in the communication control policy?

A. A collector blocks unsafe applications from running
B. A collector is used to change the reputation score of any application that collector runs
C. A collector records applications that communicate externally
D. A collector can quarantine unsafe applications from communicating

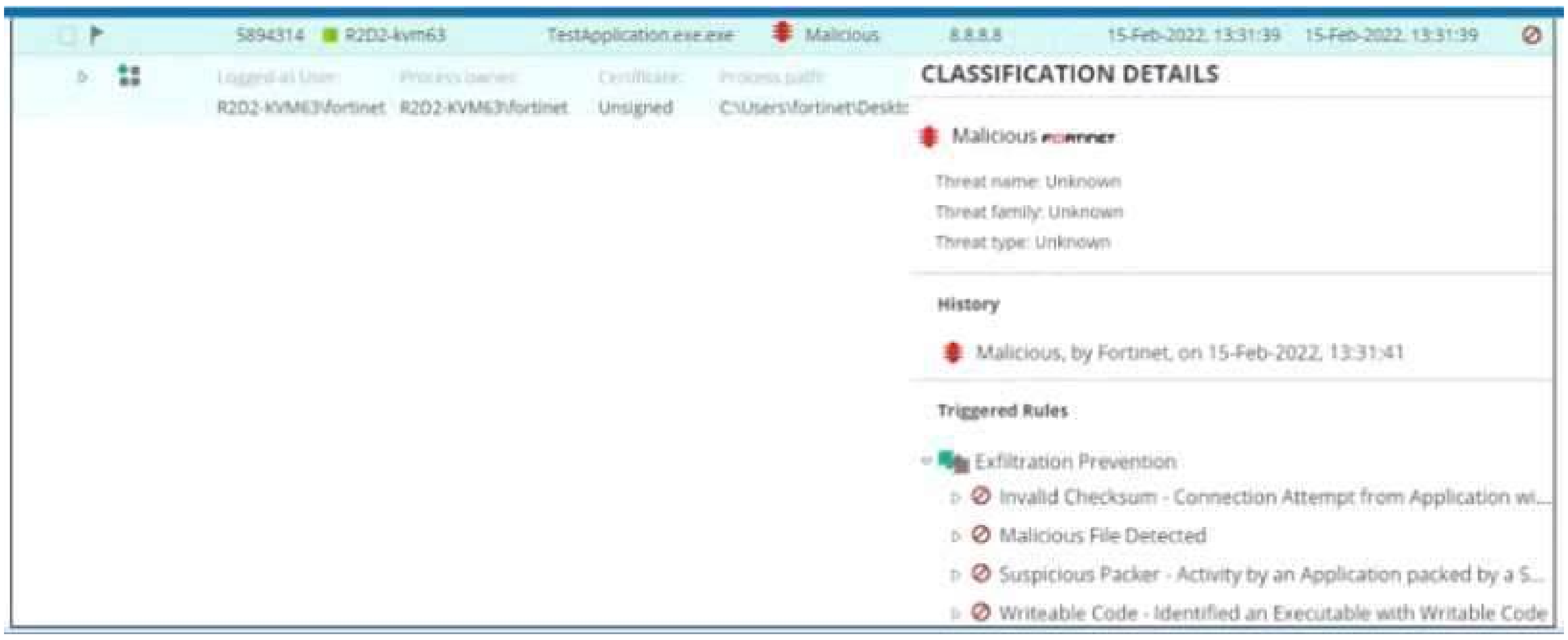
Answer: A

NEW QUESTION 3
An administrator needs to restrict access to the ADMINISTRATION tab inthe 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

Answer: C

NEW QUESTION 4
Refer to the exhibit.



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:	Process owner:	Certificate:	Process path:
R2D2-KVM63\fortinet	R2D2-KVM63\fortinet	Unsigned	C:\Users\fortinet\Deskt

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

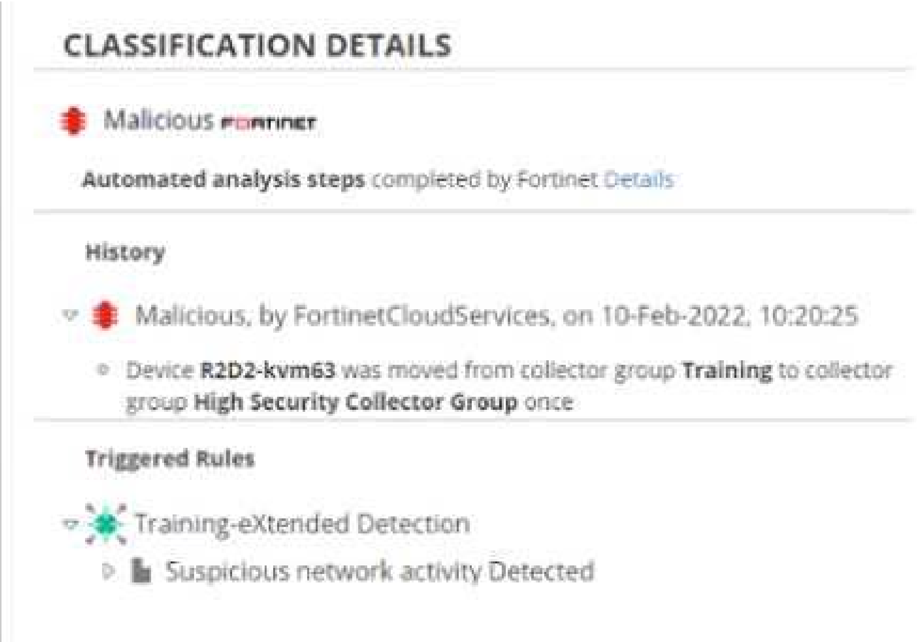
Exfiltration Prevention
- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code

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

Answer: AB

NEW QUESTION 5
Exhibit.



CLASSIFICATION DETAILS

Malicious FORTINET

Automated analysis steps completed by Fortinet Details

History

Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25

- Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

Training-eXtended Detection

Suspicious network activity Detected

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

A. The device is moved to isolation.
B. Playbooks is configured for this event.
C. The event has been blocked
D. The policy is in simulation mode

Answer: BD

NEW QUESTION 6
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

Answer: C

NEW QUESTION 7
Which security policy has all of its rules disabled by default?

A. Device Control
B. Ransomware Prevention
C. Execution Prevention
D. Exfiltration Prevention

Answer: B

NEW QUESTION 8
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

Answer: C

NEW QUESTION 10
......