



Vendor: Fortinet

Exam Code: NSE5_EDR-5.0

Exam Name: Fortinet NSE 5 - FortiEDR 5.0

Version: DEMO

QUESTION 1

What is the purpose of the Threat Hunting feature?

- A. Delete any file from any collector in the organization
- B. Find and delete all instances of a known malicious file or hash in the organization
- C. Identify all instances of a known malicious file or hash and notify affected users
- D. Execute playbooks to isolate affected collectors in the organization

Answer: B

Explanation:

Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it's a search and destroy operation.

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

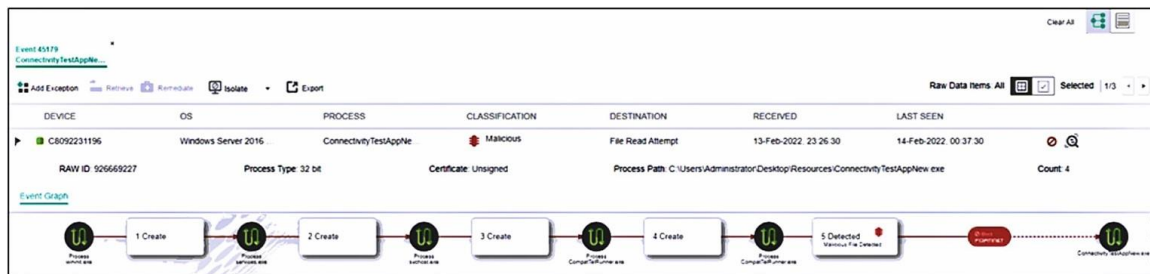
Answer: B

Explanation:

User: can view and edit all information in all tabs except ADMINISTRATION.

QUESTION 3

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



- A. The device cannot be remediated.
- B. The execution prevention policy has blocked this event.
- C. The event was blocked because the certificate is unsigned.
- D. Device C8092231196 has been isolated.

Answer: AB

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 a new communication control policy and shares it with other organizations.
- C. An administrator creates a new communication control policy for each organization.
- D. A local administrator creates a new communication control policy and assigns it globally to all organizations.

Answer: C



Explanation:

<https://docs.fortinet.com/document/fortiedr/5.2.1/administration-guide/967281/communication-control>

QUESTION 5



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

CLASSIFICATION DETAILS

 Malicious 



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

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

Answer: BD

QUESTION 6

Which threat hunting profile is the most resource intensive?

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

Answer: A

Explanation:

Comprehensive Profile collects almost all data from endpoints and is the most resource-intensive profile.

QUESTION 7

When installing a FortiEDR collector, why is a 'Registration Password' for collectors needed?

- A. To restrict installation and uninstallation of collectors
- B. To verify Fortinet support request
- C. To restrict access to the management console
- D. To verify new group assignment

Answer: A

Explanation:

Registration Password is used to restrict the installation and uninstallation of aggregators, cores, and collectors.

QUESTION 8

Which FortiEDR component must have JumpBox functionality to connect with FortiAnalyzer?

- A. Collector
- B. Core
- C. Central manager
- D. Aggregator

Answer: B

Explanation:

You need an on premise CORE , with jump box functionality and valid API access, to Gate, Analyzer, NAC and or Sandbox.

QUESTION 9

Which two types of traffic are allowed while the device is in isolation mode? (Choose two.)

- A. Outgoing SSH connections
- B. HTTP sessions
- C. ICMP sessions
- D. Incoming RDP connections

Answer: CD

Explanation:

By design, ICMP and incoming RDP connection are allowed on an isolated unit to assist IT.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14