ExamEnroll
EXAM SUCCESS SIMPLIFIED

Fortinet

NSE6_EDR_AD-7.0

Fortinet NSE 6 - FortiEDR 7.0 Administrator

Exam Version: 6.0

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Thank you for Downloading NSE6_EDR_AD-7.0 exam PDF Demo

You can also try our NSE6_EDR_AD-7.0 practice exam software

Visit link below:

https://examsenroll.com/exam/nse6_edr_ad-7.0

Question 1. (Single Select)

After integrating FortiEDR with external SIEM tools, an administrator notices that some events are missing from the SIEM dashboard. What is the most likely cause?

A: Core component is prioritizing forensic analysis over event forwarding
B: Endpoint agents are not generating sufficient telemetry for event processing
C: Communication control policies are blocking outbound network connections
D: Event forwarding configuration is incomplete or filtering out specific event types

Answer: D

Question 2. (Multi Select)

Which two types of data are essential for reconstructing an attack timeline in FortiEDR?

(Choose two.)

A: Process execution logs showing parent-child relationships and timestamps
B: NAT session logs showing address translation activity
C: VLAN segmentation configuration across switching infrastructure devices
D: Routing table updates reflecting network path changes
E: File modification records indicating creation and alteration events

Answer: A, E

Question 3. (Single Select)

During investigation, an administrator identifies unusual privilege escalation attempts. What is the most likely goal of the attacker?

A: Gaining higher-level access to execute restricted actions on the system
B: Reducing system performance to cause denial-of-service conditions

C: Encrypting files to initiate ransomware attack across endpoints

D: Establishing outbound communication with command-and-control servers

Answer: A

Question 4. (Multi Select)

Which two conditions can cause FortiEDR to miss detecting malicious activity?

(Choose two.)

A: Static routing entries are misconfigured across network devices

B: Endpoint agents are outdated or not properly functioning on systems

C: VLAN segmentation is incorrectly configured across switching infrastructure

D: Security policies are not configured to detect specific threat behaviors

E: NAT translation rules are incorrectly applied on firewall interfaces

Answer: B, D

Question 5. (Single Select)

An administrator configures a FortiEDR deployment where endpoints connect through a centralized Collector. During peak hours, event processing becomes delayed. Which architectural adjustment would most effectively improve performance?

A: Reduce endpoint monitoring sensitivity to minimize generated events

B: Disable forensic data collection to reduce system processing overhead

C: Deploy additional Collectors to distribute endpoint communication load

D: Modify communication control policies to limit endpoint network activity

Answer: C

For More Information - Visit link below:

https://examsenroll.com/exam/nse6_edr_ad-7.0

Thanks for using our Product!

Pass Your Certification With ExamsEnroll Guarantee

For $20 discount, use coupon code:

MINUS20

Sales: sales@examsenroll.com

Support: support@examsenroll.com

