

# Fortinet

## NSE6\_EDR\_AD-7.0

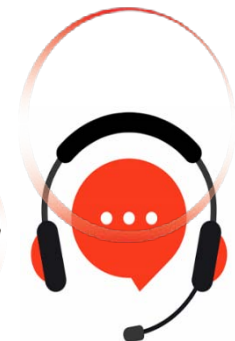
### Fortinet NSE 6 - FortiEDR 7.0 Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

**Product Version**

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/nse6-edr-ad-7-0>

# Latest Version: 6.0

## Question: 1

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

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

During a FortiEDR investigation, an administrator reviews a timeline showing the following sequence:

- A user downloads a file from an external website
- The file spawns a hidden process
- The process modifies system files and initiates outbound connections

Which conclusion best describes this activity?

- A. Legitimate application performing routine update and configuration tasks
- B. Multi-stage attack involving execution, persistence, and command-and-control communication
- C. System maintenance process modifying files and validating external connections
- D. Endpoint agent generating false positives due to aggressive detection settings

**Answer: B**

### Question: 4

Which two actions help reduce false positives in FortiEDR?  
(Choose two.)

- A. Remove endpoint monitoring to reduce event generation
- B. Ignore low-severity alerts when configuring policies
- C. Disable all detection rules to eliminate unnecessary alerts
- D. Use Simulation mode to validate policy impact before enforcement
- E. Fine-tune detection policies based on observed legitimate behavior patterns

**Answer: D,E**

### Question: 5

A FortiEDR deployment shows a high number of false positives after enabling a new security policy in Prevention mode. What is the most effective first step?

- A. Switch the policy to Simulation mode to evaluate and refine behavior
- B. Disable all security policies to immediately eliminate false positives
- C. Increase Core processing capacity to handle additional event volume
- D. Remove endpoint agents from affected systems to stop event generation

**Answer: A**

### Question: 6

Which two characteristics distinguish an incident from a single event in FortiEDR?  
(Choose two.)

- A. Event automatically triggers full forensic investigation workflow
- B. Incident provides contextual information linking events across endpoints
- C. Incident aggregates multiple related events into a single correlated case
- D. Event includes complete attack chain reconstruction by default
- E. Event represents only isolated activity without correlation

**Answer: B,C**

### Question: 7

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: 8

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: 9

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**

### Question: 10

Which two benefits result from integrating FortiEDR with the broader Fortinet ecosystem?  
(Choose two.)

- A. Improved threat detection through correlation across multiple security layers
- B. Faster incident response using coordinated actions across integrated systems
- C. Automatic configuration of network routing across infrastructure devices
- D. Replacement of endpoint agents with network-based detection systems
- E. Elimination of need for security policies across endpoints

**Answer: A,B**

**Thank You for Trying Our Product**  
**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**