Fortinet

NSE6_FSM_AN-7.4

Fortinet NSE 6 - FortiSIEM 7.4 Analyst

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.**

Latest Version: 6.0

Question: 1

Which two approaches best support severity-based notification routing?
(Choose two.)

A. Page on-call for every incident to ensure coverage
B. Disable email alerts to reduce noise without tuning
C. Create separate notification policies for critical vs medium/low severity
D. Add policy conditions based on incident severity/state

Answer: C,D

Question: 2

An analyst wants to find systems running a specific software version and then pivot to related events.
Which analytics capability supports that pivot best?

A. CMDB query combined with event search filtering
B. HA heartbeat election
C. Remediation playbook execution
D. Notification policy escalation only

Answer: A

Question: 3

In the Agentless ZTNA with FortiSIEM UEBA and FortiGate use case, which two statements are accurate?
(Choose two.)

A. FortiSIEM replaces FortiGate as the ZTNA enforcement device
B. The integration guide includes a deployment overview and prerequisite concepts
C. FortiSIEM provides FortiGate with IP addresses tied to suspicious or malicious activity
D. The integration requires disabling UEBA to function

Answer: B,C

Question: 4

How are FortiEDR security policies applied to endpoints in most deployments?

A. By assigning the policy to a Collector Group
B. By applying the policy per dashboard widget
C. By embedding the policy in a FortiSIEM query
D. By linking the policy to a FortiWeb server policy

Answer: A

Question: 5

Which two statements are true about creating a Communication Control policy?
(Choose two.)

A. A new policy can be created by cloning an existing policy
B. New policies are typically created to assign different behavior to specific Collector Groups
C. Communication Control policies are created only to generate FortiSIEM dashboards
D. Communication Control policies automatically upgrade endpoint agents

Answer: A,B

Question: 6

In FortiEDR playbooks, which category best represents actions that contain or fix an issue (for example, kill process, isolate host, cleanup)?

A. Routing actions
B. UI customization actions
C. License actions
D. Remediation actions

Answer: D

Question: 7

Which two outcomes are typical reasons to use aggregation in a rule?
(Choose two.)

A. Require a threshold (N events) before triggering an incident
B. Encrypt search results automatically
C. Reduce noise by correlating repeated activity within a time window

D. Disable CMDB enrichment for matched events

Answer: A,C

Question: 8

When building multi-step investigations, what is the primary advantage of using nested lookups over manual copy/paste of values?

A. It guarantees the query will never return false positives
B. It makes correlation repeatable and less error-prone across searches
C. It automatically blocks matched entities
D. It converts the investigation into a playbook without configuration

Answer: B

Question: 9

Which two tasks align directly with the FortiEDR security settings and policies objectives listed for this exam?
(Choose two.)

A. Configure FortiSIEM CMDB database replication
B. Configure communication control policy
C. Configure FortiWeb reverse proxy certificates
D. Configure playbooks

Answer: B,D

Question: 10

If FCS reclassifies a security event after initial classification, where is that reclassification context typically reflected?

A. Only in FortiSIEM CMDB records
B. Only in FortiWeb traffic logs
C. In the event details/overview information associated with the security event
D. Only in the Central Manager server OS syslog

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

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

Visit our website.

https://examsempire.com/