Pass2Certify.com
Prepare, Practice, & Pass.

Fortinet

NSE6_FSM_AN-7.4

ExamName: Fortinet NSE 6 - FortiSIEM 7.4 Analyst

Exam Version: 6.0

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

https://pass2certify.com/exam/nse6_fsm_an-7.4

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Multi Select)

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. (Single Select)

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. (Multi Select)

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 4. (Single Select)

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 5. (Multi Select)

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

Need more info? Check the link below:

https://pass2certify.com/exam/nse6_fsm_an-7.4

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com