

FCP_FSM_AN-7.2 Exam Quizzes | Latest

FCP_FSM_AN-7.2 Braindumps Pdf

FNP Final Exam Practice Test | Correct Questions And Verified Answers | Latest 2026

____ 1. What is the most influential factor that has shaped the nursing profession?

- 1)
Physicians need for handmaidens
- 2)
Societal need for healthcare outside the home
- 3)
Military demand for nurses in the field
- 4)
Germ theory influence on sanitation - ✓✓3

____ 2. Which of the following is an example of an illness prevention activity? Select all that apply.

- 1)
Encouraging the use of a food diary
 - 2)
Joining a cancer support group
 - 3)
Administering immunization for HPV
 - 4)
Teaching a diabetic patient about his diet - ✓✓3
- food diary- health promotion activity

____ 3. Which of the following contributions of Florence Nightingale had an immediate impact on improving patients health?

- 1)

DOWNLOAD the newest PassTestking FCP_FSM_AN-7.2 PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1rvEmOZyu-m5xi5XjEBhiwcl5iEi3LXqP>

One of the key factors for passing the exam is practice. Candidates must use FCP_FSM_AN-7.2 practice test material to be able to perform at their best on the real exam. This is why PassTestking has developed three formats to assist candidates in their Fortinet FCP_FSM_AN-7.2 Preparation. These formats include desktop-based Fortinet FCP_FSM_AN-7.2 practice test software, web-based practice test, and a PDF format.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.
Topic 2	<ul style="list-style-type: none">Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.

Topic 3	<ul style="list-style-type: none"> Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.
Topic 4	<ul style="list-style-type: none"> Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.

>> FCP_FSM_AN-7.2 Exam Quizzes <<

Latest FCP_FSM_AN-7.2 Braindumps Pdf, FCP_FSM_AN-7.2 Exam Test

To pass the Fortinet FCP_FSM_AN-7.2 Exam is a dream who are engaged in IT industry. If you want to change the dream into reality, you only need to choose the professional training. PassTestking is a professional website that providing IT certification training materials. Select PassTestking, it will ensure your success. No matter how high your pursuit of the goal, PassTestking will make your dreams become a reality.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q20-Q25):

NEW QUESTION # 20

What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

- A. SNMP
- B. FortiSIEM worker
- C. FortiSIEM agent
- D. SSH

Answer: C

Explanation:

The FortiSIEM agent can be used to send detailed endpoint data such as user activity and process behavior to FortiSIEM, which is essential for performing User and Entity Behavior Analytics (UEBA).

NEW QUESTION # 21

Refer to the exhibit.

Rule Subpattern

Edit SubPattern

Name: DomainAcctLockout

Filters:

	Paren	Attribute	Operator	Value	Paren	Next	Row
	-	+ Event Type	IN	EventTypes: Domain Account Lockout	-	+ AND OR	+ -

Aggregate:

	Paren	Attribute	Operator	Value	Paren	Next	Row
	-	+ COUNT(Matched Events)	>=	1	-	+ AND OR	+ -

Group By: Attribute

	Row	Move
Reporting Device	+ -	↑ ↓
Reporting IP	+ -	↑ ↓
User	+ -	↑ ↓

Run as Query Save as Report Save Cancel

Which section contains the subpattern configuration that determines how many matching events are needed to trigger the rule?

- A. Actions
- B. Aggregate
- C. Filters
- D. Group By

Answer: B

Explanation:

The Aggregate section contains the condition COUNT(Matched Events) >= 1, which defines how many events must match the filter criteria for the rule to trigger. This is the subpattern configuration that determines the event threshold.

NEW QUESTION # 22

Refer to the exhibit.

Incident Details

The screenshot displays the incident details for ID 3984. The incident title is 'Server Disk Latency C:\ Critical on THREATSOCDC'. The rule name is 'Server Disk Latency Critical' and the event type is 'PH_RULE_SERVER_DISK_LATENCY_CRIT'. The severity category is 'High'. The incident occurred 33 minutes ago on Jan 15, 2025, at 08:07:15 AM. The category is 'Performance', subcategory is 'Impact', and tactics are 'Impact'. The technique is 'Endpoint Denial of Service: OS Exhaustion Flood' and the organization is 'Super'. The reporting device is 'WIN-RAQBSNW8OVY' with IP '10.1.1.33'. The reporting device status is 'Pending'. The target is '10.1.1.33' and 'THREATSOCDC'. The detail shows 'Disk Name: C:\', 'Disk Read Latency ms: 100.03ms', and 'Disk Write Latency ms: 1ms'. The count is 1. The incident status is 'Auto Cleared' with the reason 'Rule has not been triggered for 20 minutes' and cleared time '13 Minutes ago (Jan 15 2025, 08:27:17 AM)'.

Incident ID : 3984

Incident Title : Server Disk Latency C:\ Critical on THREATSOCDC

Rule Name : Server Disk Latency Critical

Event Type : PH_RULE_SERVER_DISK_LATENCY_CRIT

Severity Category : High

First Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Last Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Category : Performance

Subcategory : Impact

Tactics : Impact

Technique : Endpoint Denial of Service: OS Exhaustion Flood

Organization : Super

Reporting : 30 WIN-RAQBSNW8OVY

Reporting IP : 30 10.1.1.33

Reporting Device Status : Pending

Target : 30 10.1.1.33
THREATSOCDC

Detail : Disk Name: C:\
Disk Read Latency ms: 100.03ms
Disk Write Latency ms: 1ms

Count : 1

Incident Status : Auto Cleared

Cleared Reason : Rule has not been triggered for 20 minutes

Cleared Time : 13 Minutes ago (Jan 15 2025, 08:27:17 AM)

How was this incident cleared?

- A. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.
- B. FortiSIEM cleared the incident automatically after 24 hours.
- C. The analyst manually cleared the incident from the incident table.
- D. The incident was cleared automatically by the rule.

Answer: D

Explanation:

The Incident Status shows "Auto Cleared", and the Cleared Reason states: "Rule has not been triggered for 20 minutes." This indicates that the incident was automatically cleared by the rule logic after a defined period of inactivity.

NEW QUESTION # 23

Refer to the exhibit.

Rule Properties

Create Rule

Step 1: General > **Step 2: Define Condition** > Step 3: Define Action

Condition: If this Pattern occurs within any second time window

Paren	Subpattern	Paren	Next	Row
<input type="button" value="+"/>	<input type="button" value="-"/> Failed_Logon <input type="button" value="v"/>	<input type="button" value="v"/>	<input type="button" value="+"/>	<input type="button" value="-"/>

OK Cancel

SubPattern Properties

Edit SubPattern

Name: Failed_Logon

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
<input type="button" value="-"/>	<input type="button" value="+"/>	Event Type	IN	Group: Logon Failure	<input type="button" value="-"/>	<input type="button" value="+"/> AND OR	<input type="button" value="+"/> <input type="button" value="v"/>

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
<input type="button" value="-"/>	<input type="button" value="+"/>	COUNT(Matched Events)	>	value...	<input type="button" value="-"/>	<input type="button" value="+"/> AND OR	<input type="button" value="+"/> <input type="button" value="v"/>

Group By: Attribute

	Row	Move
User	<input type="button" value="+"/> <input type="button" value="-"/>	<input type="button" value="v"/>
Destination IP	<input type="button" value="+"/> <input type="button" value="-"/>	<input type="button" value="v"/>
Source IP	<input type="button" value="+"/> <input type="button" value="-"/>	<input type="button" value="v"/>

Run as Query Save as Report Save Cancel

An analyst wants the rule shown in the exhibit to trigger when three failed login attempts occur within three minutes. What should the values be for the condition time window and aggregate count?

- A. Time window 180 seconds, aggregate count 2
- B. Time window 90 seconds, aggregate count 3
- C. Time window 180 seconds, aggregate count 3
- D. Time window 90 seconds, aggregate count 2

Answer: C

Explanation:

To detect three failed login attempts within three minutes, you must set the aggregate count to 3 in the subpattern and the time window to 180 seconds in the rule condition. This ensures the rule triggers only if three or more failed logins occur in that timeframe.

NEW QUESTION # 24

How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

- A. FortiSIEM changes the incident status to Repeated, and updates the Last Seen timestamp.
- B. FortiSIEM updates the Incident Count value and Last Seen timestamp.

- Answer: B**

When a performance rule triggers repeatedly, FortiSIEM updates the existing incident by incrementing the Incident Count and refreshing the Last Seen timestamp. This avoids flooding the incident table with duplicates while still tracking repeated occurrences.

• • • • •

Latest FCP_FSM_AN-7.2 Braindumps Pdf: https://www.passtestking.com/Fortinet/FCP_FSM_AN-7.2-practice-exam-dumps.html

- [illegible]

What's more, part of that PassTesting FCP_FSM_AN-7.2 dumps now are free: <https://drive.google.com/open?id=1rvEmOZyu-m5xi5XjEBhiwcI5iEBLXqP>