Free PDF Fortinet - The Best Latest FCP_FSM_AN-7.2 Exam Testking

Fortinet FCP_FSM_AN-7.2 Exam

Fortinet NSE 6 - FortiSIEM 7.2 Analyst

https://www.passquestion.com/fcp_fsm_an-7-2.html

Save 35% OFF on ALL Exams

Coupon: 2025

35% OFF on All, Including FCP_FSM_AN-7.2 Questions and Answers

Pass FCP_FSM_AN-7.2 Exam with PassQuestion FCP_FSM_AN-7.2 questions and answers in the first attempt.

https://www.passquestion.com/

1 / 4

P.S. Free & New FCP_FSM_AN-7.2 dumps are available on Google Drive shared by DumpsKing: https://drive.google.com/open?id=1SGPilTe4MO-lUSVlCCY7_aUzjCKsWT1g

Everyone wants to stand out in such a competitive environment, but they don't know how to act. Maybe our FCP_FSM_AN-7.2 exam questions can help you. Having a certificate may be something you have always dreamed of, because it can prove that you have a certain capacity. Our FCP_FSM_AN-7.2 learning materials can provide you with meticulous help and help you get your certificate. Our FCP_FSM_AN-7.2 training prep is credible and their quality can stand the test. Therefore, our FCP_FSM_AN-7.2 practice materials can help you get a great financial return in the future and you will have a good quality of life.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	- 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	- 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.
Topic 3	- 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 4	- 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.

>> Latest FCP_FSM_AN-7.2 Exam Testking <<

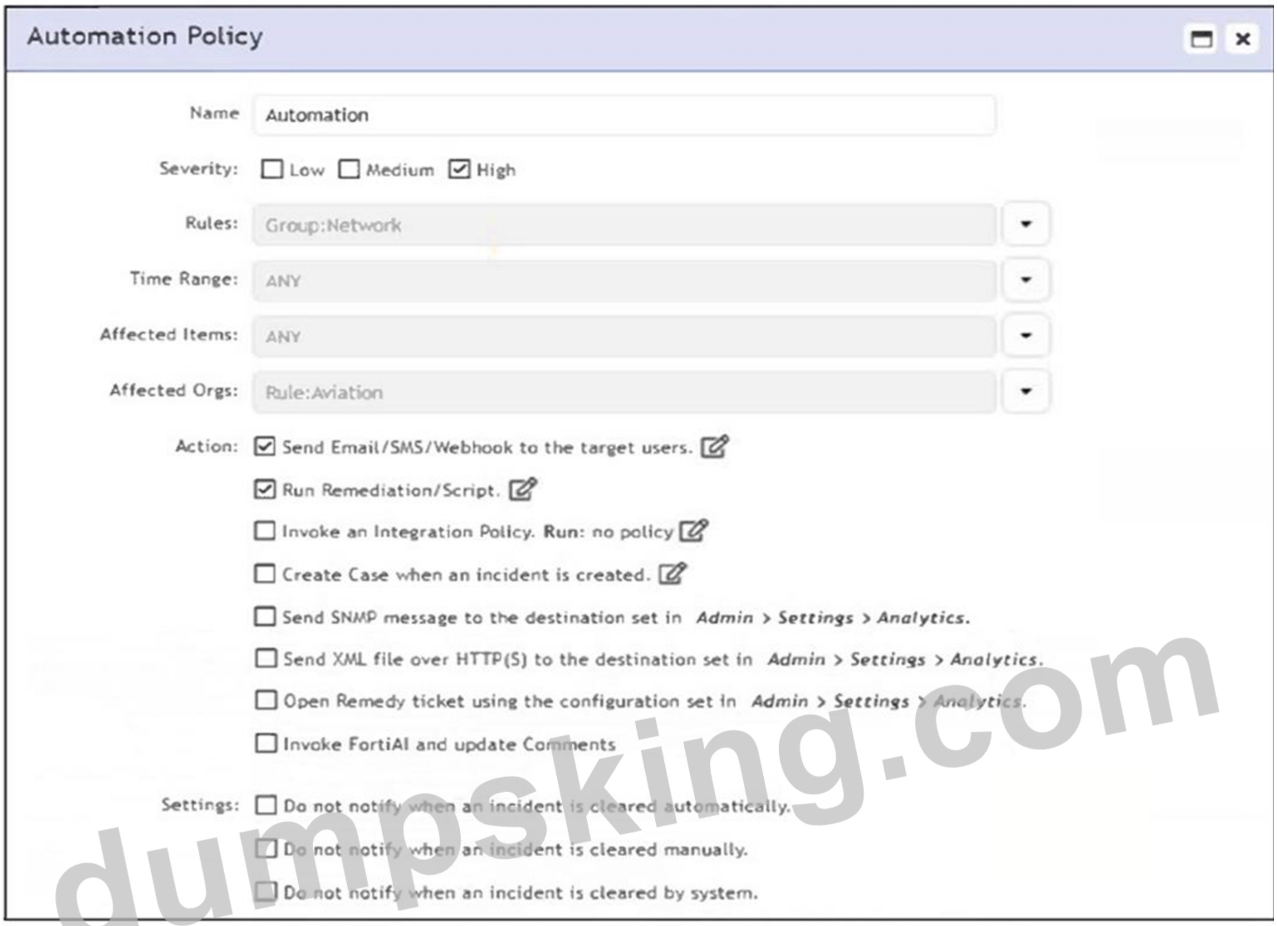
High-quality FCP_FSM_AN-7.2 - Latest FCP - FortiSIEM 7.2 Analyst Exam Testking

The FCP_FSM_AN-7.2 practice materials are a great beginning to prepare your exam. Actually, just think of our FCP_FSM_AN-7.2 practice materials as the best way to pass the exam is myopic. They can not only achieve this, but ingeniously help you remember more content at the same time. It is estimated conservatively that the passing rate of the exam is over 98 percent with our FCP_FSM_AN-7.2 Study Materials as well as considerate services. We not only provide all candidates with high pass rate study materials, but also provide them with good service.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q33-Q38):

NEW QUESTION # 33
Refer to the exhibit.

Automation Policy



Automation Policy

Name: Automation

Severity: □ Low □ Medium ☑ High

Rules: Group:Network

Time Range: ANY

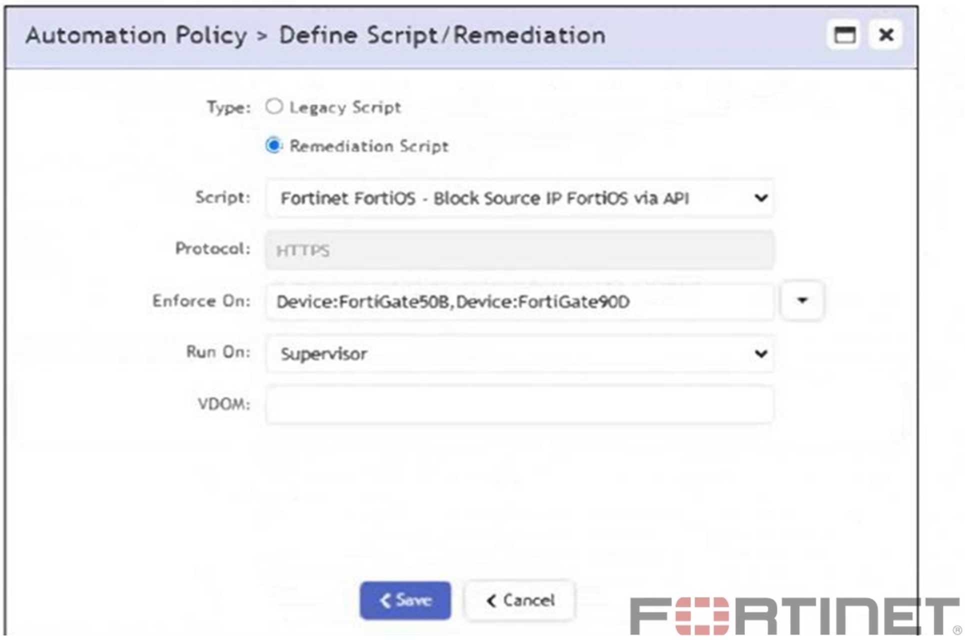
Affected Items: ANY

Affected Orgs: Rule:Aviation

Action:
- ☑ Send Email/SMS/Webhook to the target users.
- ☑ Run Remediation/Script.
- □ Invoke an Integration Policy. Run: no policy
- □ Create Case when an incident is created.
- □ Send SNMP message to the destination set in *Admin > Settings > Analytics.*
- □ Send XML file over HTTP(S) to the destination set in *Admin > Settings > Analytics.*
- □ Open Remedy ticket using the configuration set in *Admin > Settings > Analytics.*
- □ Invoke FortiAI and update Comments

Settings:
- □ Do not notify when an incident is cleared automatically.
- □ Do not notify when an incident is cleared manually.
- □ Do not notify when an incident is cleared by system.

Remediation/Script Options



Automation Policy > Define Script/Remediation

Type: ○ Legacy Script
● Remediation Script

Script: Fortinet FortiOS - Block Source IP FortiOS via API

Protocol: HTTPS

Enforce On: Device:FortiGate50B,Device:FortiGate90D

Run On: Supervisor

VDOM:

If a rule containing the automation policy shown in the exhibit triggers, what will happen?

- A. Associated source IP addresses will be blocked on all FortiGate firewalls.
- B. Associated source IP addresses will be blocked on two FortiGate firewalls.
- C. Associated source IP addresses will be blocked on devices in the Aviation organization.
- D. Associated source IP addresses will be blocked on devices in the Network CMDB group.

Answer: B

Explanation:
The automation policy is configured to run a remediation script named "Fortinet FortiOS - Block Source IP FortiOS via API". It specifies enforcement on two FortiGate devices: FortiGate508 and FortiGate90D. Therefore, associated source IP addresses will be blocked on those two FortiGate firewalls only.

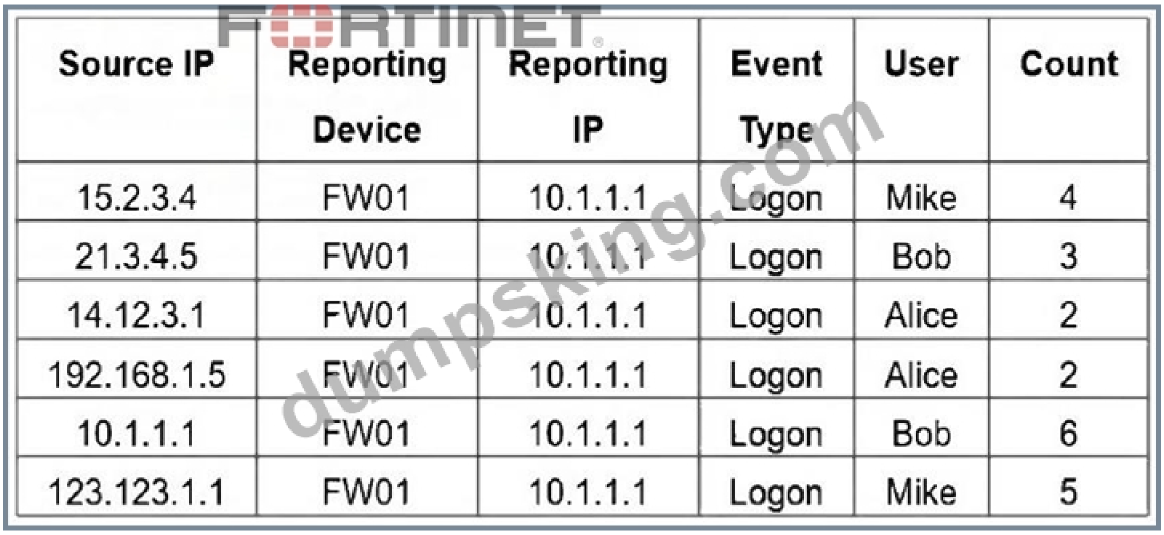
NEW QUESTION # 34
When configuring anomaly detection machine learning, in which step must you select the fields to analyze?

- A. Schedule
- B. Design
- C. Prepare Data
- D. Train

Answer: C

Explanation:
In the Prepare Data step of configuring anomaly detection in FortiSIEM, you must select the fields to analyze. This step defines the input features that the machine learning model will evaluate during training and detection.

NEW QUESTION # 35
Refer to the exhibit.



Source IP	Reporting Device	Reporting IP	Event Type	User	Count
15.2.3.4	FW01	10.1.1.1	Logon	Mike	4
21.3.4.5	FW01	10.1.1.1	Logon	Bob	3
14.12.3.1	FW01	10.1.1.1	Logon	Alice	2
192.168.1.5	FW01	10.1.1.1	Logon	Alice	2
10.1.1.1	FW01	10.1.1.1	Logon	Bob	6
123.123.1.1	FW01	10.1.1.1	Logon	Mike	5

If you group the events by User and Count attributes, how many results will FortiSIEM display?

- A. Five
- B. Three
- C. Two
- D. One
- E. Six

Answer: A

Explanation:
Grouping by User and Count yields five unique pairs: (Mike,4), (Bob,3), (Alice,2), (Bob,6), (Mike,5).

NEW QUESTION # 36
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

- A. Remediation script configured
- B. ZTNA tags defined on FortiSIEM
- C. FortiSIEM API credentials defined on FortiEMS\
- D. FortiEMS API credentials defined on FortiSIEM

Answer: C,D

Explanation:
To allow FortiSIEM to apply tags to devices in FortiClient EMS, FortiEMS API credentials must be defined on FortiSIEM to enable communication with EMS, and FortiSIEM API credentials must be defined on FortiEMS to allow EMS to accept tagging instructions from FortiSIEM. This bidirectional API trust is essential for tag application.

NEW QUESTION # 37
Which items are used to define a subpattern?

- A. Filters, Group By, Threshold definitions
- B. Filters, Aggregate, Group By definitions
- C. Filters, Threshold, Time Window definitions
- D. Filters, Aggregate, Time Window definitions

Answer: B

Explanation:
A subpattern in FortiSIEM is defined using Filters to match specific events, Aggregate conditions to apply statistical thresholds (e.g., COUNT), and Group By attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

NEW QUESTION # 38
......

Remember that this is a crucial part of your career, and you must keep pace with the changing time to achieve something substantial in terms of a certification or a degree. So do avail yourself of this chance to get help from our exceptional Fortinet FCP_FSM_AN-7.2 Dumps to grab the most competitive Fortinet FCP_FSM_AN-7.2 certificate. DumpsKing has formulated the FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) product in three versions. You will find their specifications below to understand them better.

New FCP_FSM_AN-7.2 Braindumps Questions: https://www.dumpsking.com/FCP_FSM_AN-7.2-testking-dumps.html

- {Online Realistic} Fortinet FCP_FSM_AN-7.2 Practice Test Questions □ Copy URL ➽ www.testkingpass.com □ open and search for ✔ FCP_FSM_AN-7.2 □✔□ to download for free □Reliable FCP_FSM_AN-7.2 Test Tips
- mindgrafts.com, tutor.mawgood-eg.com, devfolio.co, school.kpisafidon.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bd.enrollbusiness.com, a.callqy.cn, ycs.instructure.com, house.jiatc.com, justpaste.me, Disposable vapes

BONUS!!! Download part of DumpsKing FCP_FSM_AN-7.2 dumps for free: https://drive.google.com/open?id=1SGPilTe4MO-lUSVlCCY7_aUzjCKsWT1g