FCP_FSM_AN-7.2證照考試 & FCP_FSM_AN-7.2考試題庫

順便提一下，可以從雲存儲中下載KaoGuTi FCP_FSM_AN-7.2考試題庫的完整版：https://drive.google.com/open?id=1-fwoEm-DKguSCKjqfT1iwu5m9WTkH1kp

KaoGuTi是一個專門提供IT認證考試資料的網站，它的考試資料通過率達到100%，這也是大多數考生願意相信KaoGuTi網站的原因之一，KaoGuTi網站一直很關注廣大考生的需求，以最大的能力在滿足考生們的需要，KaoGuTi Fortinet的FCP_FSM_AN-7.2考試培訓資料是一個空前絕後的IT認證培訓資料，有了它，你將來的的職業生涯將風雨無阻。

Fortinet FCP_FSM_AN-7.2 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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.
主題 3	• 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.

主題 4	• 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.

Fortinet FCP_FSM_AN-7.2考試題庫 - FCP_FSM_AN-7.2考題寶典

為了每位IT認證考試的考生切身利益，我們網站提供KaoGuTi Fortinet的FCP_FSM_AN-7.2考試培訓資料是根據考生的需要而定做的，由我們KaoGuTi資質深厚的IT專家專門研究出來的，他們的奮鬥結果不僅僅是為了幫助你們通過考試，而且是為了讓你們有一個更好的明天。

最新的 Fortinet Certified Professional Security Operations FCP_FSM_AN-7.2 免費考試真題 (Q32-Q37):

問題 #32
What are two required components of a rule? (Choose two.)

- A. Clear policy
- B. Exception policy
- C. Subpattern
- D. Detection Technology

答案：C,D

解題說明：
A Subpattern defines the specific conditions or event patterns the rule is designed to detect, and the Detection Technology specifies the type of detection logic (e.g., real-time, historical). Both are essential for a rule to function in FortiSIEM.

問題 #33
Refer to the exhibit.

What will happen when a device being analyzed by the machine learning configuration shown in the exhibit has a consistently high memory utilization?

- A. FortiSIEM will trigger an incident for high memory utilization.
- B. FortiSIEM will update the model with a higher memory utilization average value.
- C. FortiSIEM will lower the CPU utilization trigger requirement for CPU utilization.

- D. FortiSIEM will update the regression tables for memory utilization, and average sent and received bytes.

答案： B

解題說明：
In the configuration shown, FortiSIEM uses Memory Util, Sent Bytes, and Received Bytes as input features to predict CPU Utilization via a regression model. If a device shows consistently high memory utilization, the model will incorporate that into its training data and update itself with a higher average value for memory utilization, influencing future CPU utilization predictions.

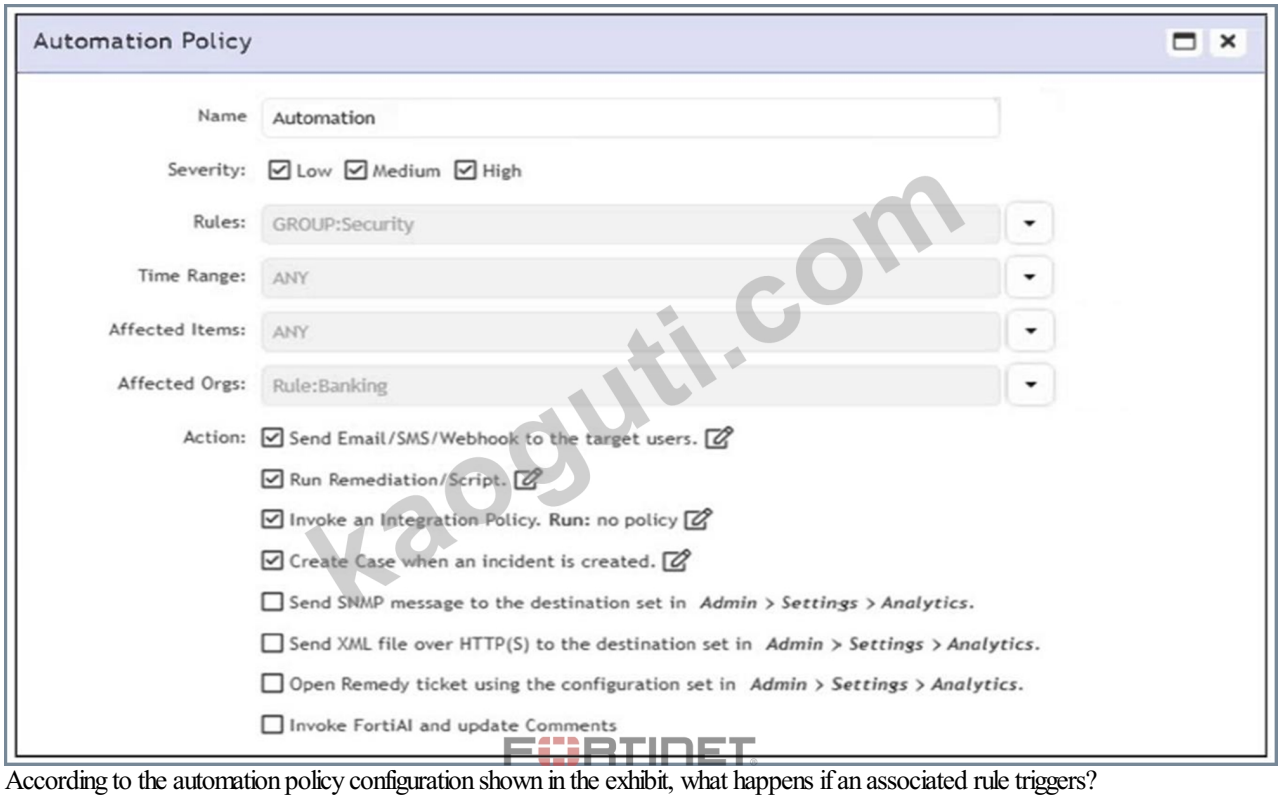
問題 #34
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

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

答案： A,C

解題說明：
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.

問題 #35
Refer to the exhibit.



According to the automation policy configuration shown in the exhibit, what happens if an associated rule triggers?

- A. FortiSIEM fails to the integration policy, because no policy is defined.
- B. FortiSIEM sends an email, because that is first on the list.
- C. FortiSIEM performs all selected actions.
- D. FortiSIEM runs the remediation script, because that takes precedence over all other options.

答案： C

解題說明：
When an associated rule triggers, FortiSIEM performs all selected actions in the automation policy. In this case, it will send an email/SMS/webhook, run the remediation script, invoke the integration policy (even if none is currently defined), and create a case. All checked actions are executed.

問題 #36
Which running mode takes the most time to perform machine learning tasks?

- A. Local auto
- B. Regression
- C. Local
- D. Forecasting

答案：C

解題說明：
In Local mode, FortiSIEM performs machine learning tasks using the full dataset without optimization shortcuts, making it the most time-consuming mode compared to Local Auto, Forecasting, or Regression.

問題 #37
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, wanderlog.com, Disposable vapes

此外，這些KaoGuTi FCP_FSM_AN-7.2考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1-fwoEm-DKguSCKjqfT1iwu5m9WTkH1kp