DUMPSBOSS.

Fortinet NSE 6 - FortiSIEM 7.4 Analyst

Fortinet NSE6_FSM_AN-7.4

Version Demo

Total Demo Questions: 6

Total Premium Questions: 63

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture	2
Topic 2, Discovery	1
Topic 3, Incidents	23
Topic 4, Analytics	37
Total	63

QUESTION NO: 1

When configuring machine learning (ML), in which step can you modify how the model fits the training data set?

A. Prepare Data

B. Train

C. Statistics

D. Design

ANSWER: B

Explanation:

Train is the correct step because it is where FortiSIEM creates and evaluates the machine-learning model using the prepared data set. In this stage, the analyst selects the ML task and algorithm, identifies the relevant target or prediction fields when applicable, and defines the Train factor. The Train factor controls the division of available records between model training and testing, directly affecting the data on which the model is fitted and validated.

The Train workflow also provides the controls needed to refine fitting behavior after an initial training run. Through *Tune & Train*, an analyst can adjust algorithm parameters, save those changes, and retrain the model. This iterative process is essential for improving predictive quality based on the resulting model metrics. For example, regression results can be assessed with measures such as mean absolute error and R-squared, which indicate how closely model predictions fit the observed values. Therefore, the Train step is the FortiSIEM ML workflow stage intended for configuring, tuning, and retraining the model against the training data. See the FortiSIEM 7.4 documentation and the FortiSIEM 7.4 User Guide.

QUESTION NO: 2

An analyst is creating an Analytics search for events reported by devices that belong to a CMDB device group. The analyst has selected **Reporting IP** as the event attribute and wants the search to use the current membership of the CMDB group.

Which two actions should the analyst perform to complete the condition? (Choose two.)

A. Select the IN operator

B. Click Value > Select from CMDB

C. Enter each current device IP address as a static value

D. Click Attribute > Select from CMDB

ANSWER: A B

Explanation:

The analyst must select the **IN** operator and use **Value > Select from CMDB** to choose the CMDB group. The IN operator evaluates whether the Reporting IP belongs to the selected group, while the CMDB value-selection workflow supplies the maintained group object. Entering a static IP address does not preserve dynamic group membership, and selecting a CMDB object from the Attribute control does not define the comparison value.

QUESTION NO: 3

In an automation policy, which two methods can you use to notify analysts when an incident is triggered? (Choose two.)

A. Email

B. FortiSIEM Case

C. Syslog

D. Pop-up window

ANSWER: A B

Explanation:

Email and **FortiSIEM Case** are the applicable automation-policy methods for getting analyst attention and initiating analyst handling after an incident is triggered. An automation policy can send an incident notification by email, using the notification settings and template configured in FortiSIEM. This provides a direct alerting path to the intended recipients, and notification frequency controls can be applied so that repeat incident activity does not create unnecessary mail volume.

An automation policy can also create a FortiSIEM case when the incident is created. A case turns the incident into a trackable analyst work item: it can be assigned and processed through the case-management workflow, with analyst teams participating in the handling sequence. This is an analyst-notification and response-routing mechanism because it places the incident into the operational queue where analysts investigate, document actions, and manage resolution. Together, email provides immediate outbound notification, while case creation provides structured workflow ownership and tracking. Fortinet documents automation and incident-response capabilities in the FortiSIEM 7.4 documentation and describes FortiSIEM case-management functionality in the FortiSIEM User Guide.

QUESTION NO: 4

FortiSIEM is integrated with FortiClient EMS by using the FortiEMS API credentials. An analyst wants to use the integration in an endpoint-response workflow.

Which two operations can FortiSIEM perform through this integration? (Choose two.)

A. Retrieve ZTNA tags from managed endpoints

B. Apply or remove endpoint classification tags

C. Retrieve FortiSIEM license information

D. Retrieve host login credentials

E. Modify FortiSIEM rule definitions

ANSWER: A B

Explanation:

FortiSIEM can **retrieve ZTNA tags** from FortiClient EMS and can **apply or remove supported endpoint classification tags** through an automated remediation workflow. The retrieved tag context can be used during investigation and correlation, while a tag change can support downstream, tag-driven access-control enforcement.

The FortiClient EMS integration does not provide FortiSIEM license information or host login credentials. FortiSIEM also does not use the EMS API connection to modify FortiSIEM rule definitions.

QUESTION NO: 5

An automation policy must create an analyst work item for each qualifying incident so that it can be assigned, investigated, and tracked through resolution.

Which automation-policy action should the analyst configure?

A. Send an email notification

B. Create a FortiSIEM Case

C. Forward the incident by syslog

D. Display a pop-up window

ANSWER: B

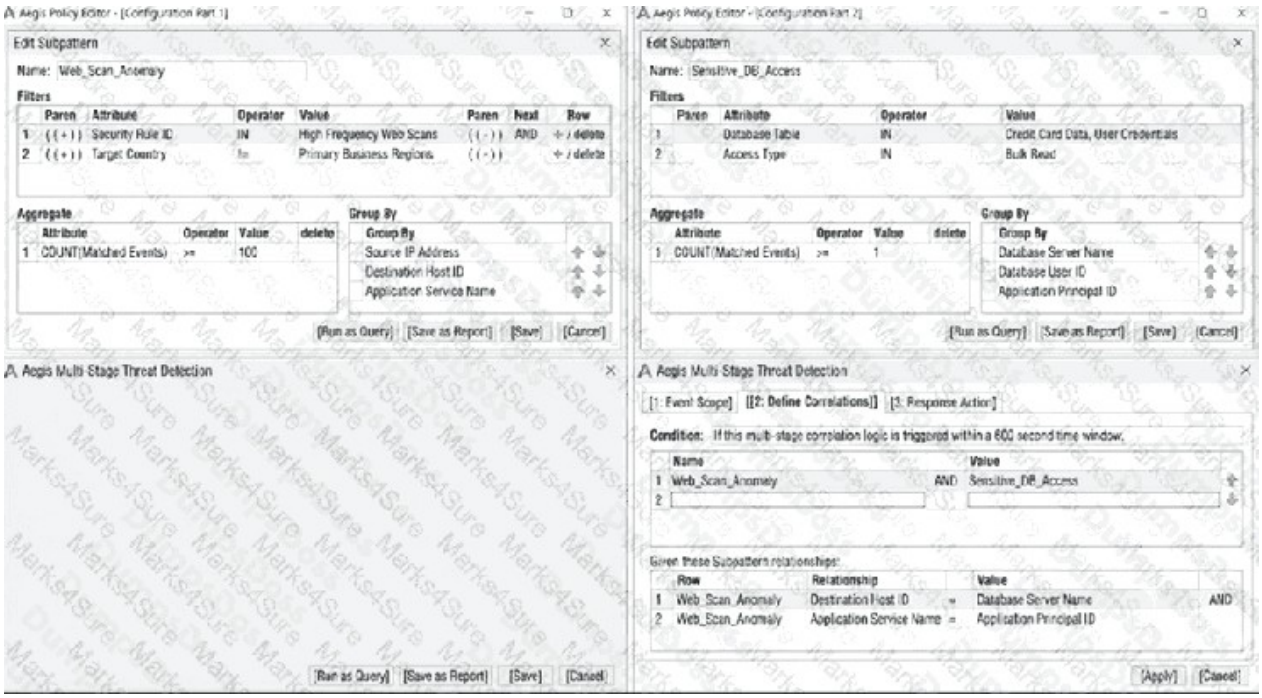
Explanation:

Create a FortiSIEM Case is correct because a case provides a structured analyst workflow for assignment, investigation, documentation, and resolution tracking. It turns the incident into a work item that can be managed by the analyst team.

Email can notify recipients that an incident occurred, but it does not create a trackable case-management record. Syslog forwarding and a pop-up window do not provide the FortiSIEM case workflow required by the scenario.

QUESTION NO: 6

Refer to the exhibits.



You are troubleshooting why the rule shown in the exhibit is generating incidents for successful Remote Desktop Protocol (RDP) connections with correct logins. It should only be triggering when a person fails to log in three or more times to the target device when connecting with RDP.

What is causing the rule to be triggered by correct login events? (Choose one answer)

A. The subpattern relationship RDP_Connection:User = Failed_Logon:User never matches.

B. The Boolean between the subpatterns is incorrect.

C. The attribute types in the subpatterns do not match.

D. The RDP login is different from the login used to access the target device.

ANSWER: B

Explanation:

The Boolean between the subpatterns is incorrect. The rule contains two separate conditions: one identifies the RDP connection activity, and the other identifies three or more failed logon events. When the next/subpattern operator is configured as **OR**, FortiSIEM treats either subpattern as sufficient to satisfy the rule's detection logic within its time window. Consequently, an ordinary successful RDP connection can match the RDP-connection subpattern and generate an incident without any corresponding failed-login activity.

For the stated detection goal, the correlation logic must require the RDP connection context together with the repeated failed-login condition, while applying the intended shared-attribute constraints such as user and target device. In practice,

this means the relationship between the subpatterns must use the Boolean logic that requires both relevant conditions rather than allowing either one independently. FortiSIEM correlation rules use subpatterns, temporal windows, and attribute relationships to identify multi-event conditions; choosing the correct Boolean operator is therefore essential to ensure that the incident represents the complete intended sequence rather than a single matching event. See Fortinet's FortiSIEM 7.4 documentation and the Fortinet Training Institute for FortiSIEM correlation-rule guidance.