Fortinet.FCP_FSM_AN-7.2.v2026-01-22.q14

Exam Code:	FCP_FSM_AN-7.2
Exam Name:	FCP - FortiSIEM 7.2 Analyst
Certification Provider:	Fortinet
Free Question Number:	14
Version:	v2026-01-22
# of views:	120
# of Questions views:	140
https://www.freepdfdumps.com/Fortinet.FCP_FSM_AN-7.2.v2026-01-22.q14.html	

NEW QUESTION: 1
Which information can FortiSIEM retrieve from FortiClient EMS through an API connection?
A. Host software versions
B. FortiSIEM license
C. Host login credentials
D. ZTNA tags
Answer: D (LEAVE A REPLY)
FortiSIEM can retrieve ZTNA tags from FortiClient EMS through an API connection, enabling dynamic user and device classification for policy enforcement and incident response.

NEW QUESTION: 2
Refer to the exhibit.

How was this incident cleared?

A. The analyst manually cleared the incident from the incident table.

B. FortiSIEM cleared the incident automatically after 24 hours.

C. The incident was cleared automatically by the rule.

D. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.

Answer: (SHOW ANSWER)

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: 3
Refer to the exhibit.

A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown in the exhibit, why are there no search results?
A. The analyst selected AND in the Next column. This is the wrong Boolean operator.
B. The Time Range value should be set to Real-Time.
C. The keyword is case sensitive. Instead of typing udp in the Value field, the analyst should type UDP.
D. The analyst selected = in the Operator column. That is the wrong operator.
Answer: D (LEAVE A REPLY)
The operator is set to "=", which performs an exact match on the entire raw event log, not a substring search. To find logs that contain the keyword "udp", the analyst should use the CONTAIN operator instead. This will return all logs where "udp" appears anywhere in the raw log message.

NEW QUESTION: 4
What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?
A. FortiSIEM agent
B. SSH
C. SNMP
D. FortiSIEM worker
Answer: A (LEAVE A REPLY)

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: 5
What are two required components of a rule? (Choose two.)
A. Exception policy
B. Subpattern
C. Detection Technology
D. Clear policy
Answer: B,C (LEAVE A REPLY)
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.

NEW QUESTION: 6
Refer to the exhibit.

An analyst is trying to identify an issue using an expression based on the Expression Builder settings shown in the exhibit; however, the error message shown in the exhibit indicates that the expression is invalid.
What is the correct syntax to create an expression that generates a total count of matched events?
A. COUNT(Matched Events)
B. (COUNT) Matched Events
C. Matched Events (COUNT)
D. Matched Events COUNT()
Answer: A (LEAVE A REPLY)
The correct syntax is COUNT(Matched Events) - with proper capitalization and spacing - to generate a total count of matched events. The error in the exhibit likely stems from a formatting issue (e.g., lowercase count() or incorrect spacing), not the logical structure of the expression.

NEW QUESTION: 7
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, Source IP, and Count attributes, how many results will FortiSIEM display?

A. Two

B. Six

C. Three

D. Five

E. Four

Answer: B (LEAVE A REPLY)

Grouping by User, Source IP, and Count means that each unique combination of those three attributes will be treated as a separate result. In the table, all six rows have distinct combinations of User, Source IP, and Count - so FortiSIEM will display 6 results.

NEW QUESTION: 8

Refer to the exhibit.

Source IP	Reporting Device	Reporting IP	Event Type	User	Application Category
15.2.3.4	FW01	10.1.1.1	Logon	Mike	DB
21.3.4.5	FW02	10.1.1.2	Logon	Bob	WebApp
14.12.3.1	FW01	10.1.1.1	Logon	Alice	SSH
192.168.1.5	FW03	10.1.1.3	Logon	Alice	DB
10.1.1.1	FW01	10.1.1.1	Logon	Bob	DB
123.123.1.1	FW04	10.1.1.4	Logon	Mike	SSH

If you group the events by Reporting Device, Reporting IP, and Application Category, how many results will FortiSIEM display?

A. Four

B. Five

C. One

D. Six

E. Two

Answer: (SHOW ANSWER)

Grouping by Reporting Device, Reporting IP, and Application Category yields five unique tuples: (FW01, 10.1.1.1, DB), (FW02, 10.1.1.2, WebApp), (FW01, 10.1.1.1, SSH), (FW03, 10.1.1.3, DB), and (FW04, 10.1.1.4, SSH).

NEW QUESTION: 9

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

A. ZTNA tags defined on FortiSIEM

B. FortiSIEM API credentials defined on FortiEMS\

C. FortiEMS API credentials defined on FortiSIEM

D. Remediation script configured

Answer: (SHOW ANSWER)

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: 10

Refer to the exhibit.

Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

A. applist

B. Network.Service

C. SSL

D. wan1

Answer: C (LEAVE A REPLY)

The Application Name field in FortiSIEM is typically populated using the value of the app field in the raw log. In this event, app="SSL", so "SSL" is the expected application name parsed by FortiSIEM.

NEW QUESTION: 11

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?

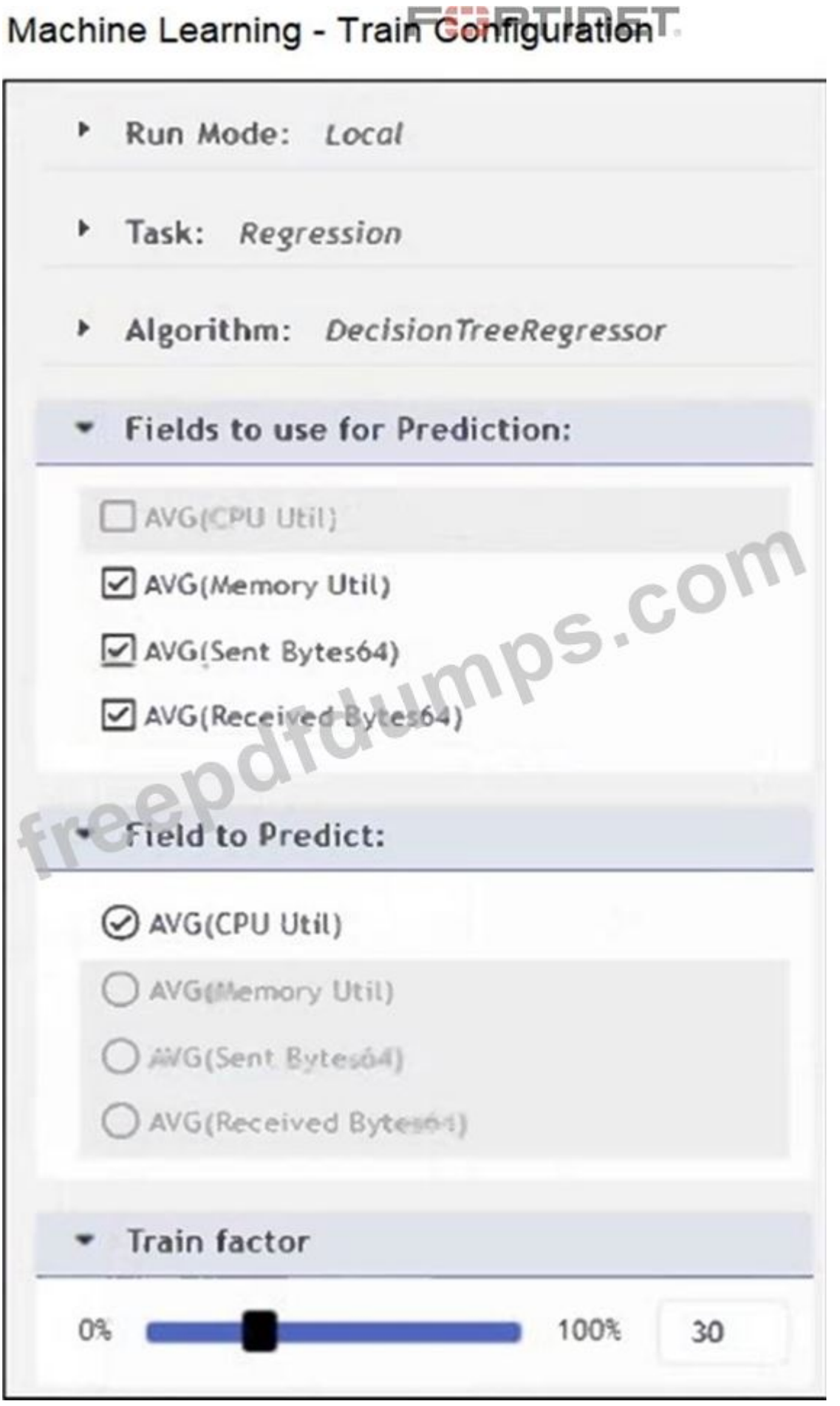
A. FortiSIEM will update the regression tables for memory utilization, and average sent and received bytes.

B. FortiSIEM will trigger an incident for high memory utilization.
C. FortiSIEM will lower the CPU utilization trigger requirement for CPU utilization.
D. FortiSIEM will update the model with a higher memory utilization average value.
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 12
Which statement about thresholds is true?
A. FortiSIEM uses fixed, hardcoded global and device thresholds for all performance metrics.
B. FortiSIEM uses only device thresholds for security metrics.
C. FortiSIEM uses global and per device thresholds for performance metrics.
D. FortiSIEM uses only global thresholds for performance metrics.
Answer: C (LEAVE A REPLY)
FortiSIEM evaluates performance metrics against both global thresholds, which apply system-wide, and per-device thresholds, which can be customized for individual devices. This dual approach allows flexibility in monitoring while ensuring consistent baseline alerting.

NEW QUESTION: 13
Which items are used to define a subpattern?
A. Filters, Aggregate, Group By definitions
B. Filters, Aggregate, Time Window definitions
C. Filters, Group By, Threshold definitions
D. Filters, Threshold, Time Window definitions
Answer: A (LEAVE A REPLY)
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: 14
Refer to the exhibit.



The configuration shown in the exhibit is incorrect.

What must you change to allow this configuration to be successfully applied to FortiSIEM?

A. The Train factor must be 70% or greater.

B. Run Mode must be set to ML.

C. Only one AVG type field must be selected under Fields to use for Prediction.

D. The selection in Fields to use for Prediction and Field to Predict must match.

Answer: B (LEAVE A REPLY)

The Run Mode is set to Local, which is not valid for training machine learning models in FortiSIEM. To apply this configuration correctly, the Run Mode must be set to ML, which enables proper model training and prediction using selected fields.