



Download Fortinet FCP_FSM_AN-7.2 Exam Dumps Free

Shared by Mosley on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

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

Options:

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



Answer:

B, C

Explanation:

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.

Question 2

Question Type: MultipleChoice

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	Nex	Row
+ -	Failed_Logon	✎ + -		↓ + -

OK Cancel

SubPattern Properties

Edit SubPattern

Name: Failed_Logon

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
- +	+ -	Event Type	IN	Group: Logon Failure	- +	AND OR	+ -

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
- +	+ -	COUNT(Matched Events)	>	value...	- +	AND OR	+ -

Group By: Attribute

Attribute	Row	Move
User	+ -	↑ ↓
Destination IP	+ -	↑ ↓
Source IP	+ -	↑ ↓

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?

Options:

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

Answer:

A

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.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Group By and Display Fields					Clear All	Load	Save
Attribute	Order	Display As	Row	Move			
Event Receive Time	DESC ▼		+ - ↺ ↓				
Reporting IP	▼		+ - ↑ ↓				
Event Type	▼		+ - ↑ ↓				
Raw Event Log	▼		+ - ↑ ↓				
COUNT(Matched Events)	▼		+ - ↑ ↺				

As shown in the exhibit, why are some of the fields highlighted in red?

Options:

- A- Unique values cannot be grouped B.
- B- The attribute COUNT(Matched Events) is an invalid expression.
- C- No RAW Event Log attribute information is available.
- D- The Event Receive Time attribute is not available for logs.

Answer:

A

Explanation:

The fields are highlighted in red because unique values such as Event Receive Time and Raw Event Log cannot be used in group-by operations. Grouping requires aggregatable or consistent values across events, while these fields are unique to each event, making them incompatible for grouping.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



▶ Run Mode: *Local*

▶ Task: *Regression*

▶ Algorithm: *DecisionTreeRegressor*

▼ Fields to use for Prediction:

- AVG(CPU Util)
- AVG(Memory Util)
- AVG(Sent Bytes64)
- AVG(Received Bytes64)

▼ Field to Predict:

- AVG(CPU Util)
- AVG(Memory Util)
- AVG(Sent Bytes64)
- AVG(Received Bytes64)

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

Options:

- 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

Explanation:

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.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

Incident generator window

The screenshot shows the 'Generate Incident for: Logon_Failure' window. It contains the following sections:

- Incident Attributes:** A table with columns: Event Attribute, Subpattern, Filter Attribute, and Row.

Event Attribute	Subpattern	Filter Attribute	Row
Source IP	Logon_Fail	Source IP	⊕ ⊖
Destination IP	Logon_Fail	Destination IP	⊕ ⊖
User	Logon_Fail	User	⊕ ⊖
- Insert Attribute:** A dropdown menu showing 'Destination IP' with a '+' button.
- Incident Title:** A text field containing 'Suser from SsrcIpAddr failed to logon to SdestIpAddr'.
- Triggered Attributes:** A list of attributes with a search bar and a '1/33' indicator.
 - Available: Search...
 - WLAN Interface Intereference Index
 - Execute Thread Peak
 - Session Process Time ms
 - Tomcat manager Check Frequency
 - Printer Current Supply Level
 - Printer Supply Name
- Selected:** A list of selected attributes.
 - Event Receive Time
 - Event Type
 - Reporting IP
 - Raw Event Log

At the bottom, there are 'Save' and 'Cancel' buttons.

An analyst is trying to generate an incident with a title that includes the Source IP, Destination IP,

User, and Destination Host Name. They are unable to add a Destination Host Name as an incident attribute.

What must be changed to allow the analyst to select Destination Host Name as an attribute?

Options:

- A- The Destination Host Name must be selected as a Triggered Attribute.
- B- The Destination Host Name must be set as an aggregate item in a subpattern.
- C- The Destination Host Name must be added as an Event type in the FortiSIEM.
- D- The Destination IP Event Attribute must be removed.

Answer:

A

Explanation:

For an attribute like Destination Host Name to be used in the incident title, it must first be included in the Triggered Attributes list. Only attributes listed there are available for substitution in the title template (e.g., \$destIpAddr, \$srcIpAddr).

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

Analytics

The screenshot shows the Analytics filter configuration interface. The 'Filter By' section is set to 'Event Attribute'. Two filters are applied:

Paren	Attribute	Operator	Value	Paren	Next	Row
-	Source IP	IN	Group: Windows	-	AND OR	+ 🗑️
-	User	IN	Group: FortiSIEM Analysts	-	AND OR	+ 🗑️

The 'Time Range' section is set to 'Relative' for the last 10 minutes. The 'Trend Interval' is set to 'Auto' and the 'Result Limit' is 100 K rows.

What is the Group: FortiSIEM Analysts value referring to?

Options:

- A- FortiSIEM organization group
- B- LDAP user group
- C- CMDB user group
- D- Windows Active Directory user group

Answer:

C



Explanation:

In FortiSIEM, the value Group: FortiSIEM Analysts under the User attribute refers to a CMDB user group. These groups are defined within FortiSIEM's CMDB and used to logically organize users for analytics, correlation rules, and reporting.

Question 7

Question Type: MultipleChoice

When configuring anomaly detection machine learning, in which step must you Choose the fields to analyze?

Options:

- A- Design
- B- Schedule
- 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.

Question 8

Question Type: MultipleChoice

Which statement about thresholds is true?



Options:

- 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

Explanation:

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.



Question 9

Question Type: MultipleChoice

Which items are used to define a subpattern?

Options:

- A- Filters, Aggregate, Group By definitions
- B- Filters, Aggregate, Time Window definitions

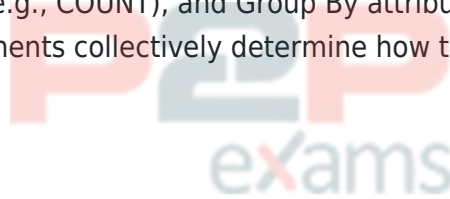
- C- Filters, Group By, Threshold definitions
- D- Filters, Threshold, Time Window definitions

Answer:

A

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.



Question 10

Question Type: MultipleChoice

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

Options:

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

Answer:

A



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).

To Get Premium Files for FCP_FSM_AN-7.2
Visit

https://www.p2pexams.com/products/fcp_fsm_an-7.2

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-fsm-an-7.2>

