



Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

NEW QUESTION 1

Refer to the exhibit.

SubPattern edit window

Edit SubPattern

Name:Failed_Logon_Windows

Filters:

	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	Event Type	IN	Group: Logon Failure	-	+ANDOR	+🗑
-	+	Source IP	-	192.168.26.109	-	+ANDOR	+🗑
-	+	Destination IP	IN	Group: Windows	-	+ANDOR	+🗑
-	+	Destination Host Name	CONTAIN	training.org	-	+ANDOR	+🗑

Aggregate:

	Paren	Attribute	Operator	Value	Paren	Next	Row
-	+	COUNT(Source IP)	>=	2	-	+ANDOR	+🗑

Group By:

Attribute	Row	Move
Destination IP	🔄⊖	↑↓
User	🔄⊖	↑↓

Run as Query

Save as Report

Save

Cancel

An analyst is troubleshooting the rule shown in the exhibit. It is not generating any incidents, but the filter parameters are generating events on the Analytics tab. What is wrong with the rule conditions?

- A. The Event Type refers to a CMDB lookup and should be an Event lookup.
- B. The Destination Host Name value is not fully qualified.
- C. The Group By attributes restricts which events are counted.
- D. The Aggregate attribute is too restrictive.

Answer: C

NEW QUESTION 2

Refer to the exhibit.

Automation Policy

Name
Automation

Severity:
☒ Low
☒ Medium
☒ High

Rules:
GROUP:Security

Time Range:
ANY

Affected Items:
ANY

Affected Orgs:
Rule:Banking

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

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

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

Answer: B

NEW QUESTION 3

Refer to the exhibit.

Event Details

Raw Message

```
<190>Jan 14 08:32:45 date=
time=14:19:51 devname=FG240D3913800441 devid=FG240D3913800441 logid=1059028704 type=utm subtype=app-ctrl
eventtype=app-ctrl-all level=information vd=root appid=15895 user=" srcip=192.168.88.11 srcport=53866 srcintf="DMZ" dstip=121.111.236.179 dstport=443
dstintf="wan1" profiletype="applist" proto=6 service="HTTPS" policyid=2 sessionid=51943532 applist="default" appcat="Network.Service" app="SSL"
action=pass msg="Network.Service: SSL"
```

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

NEW QUESTION 4

Refer to the exhibit.

Rule Subpattern

Edit SubPattern

Name: DomainAcctLockout

Filters:

	Paren	Attribute	Operator	Value	Paren	Next	Row
	⊖	⊕ Event Type	IN	EventTypes: Domain Account Lox	⊖	⊕ AND OR	⊕ 🗑

Aggregate:

	Paren	Attribute	Operator	Value	Paren	Next	Row
	⊖	⊕ COUNT(Matched Events)	>=	1	⊖	⊕ AND OR	⊕ 🗑

Group By:

Attribute	Row	Move
Reporting Device	⊕ ⊖	⬆ ⬇
Reporting IP	⊕ ⊖	⬆ ⬇
User	⊕ ⊖	⬆ ⬇

Run as Query

Save as Report

Save

Cancel

Which section contains the subpattern configuration that determines how many matching events are needed to trigger the rule?

- A. Aggregate
- B. Group By
- C. Actions
- D. Filters

Answer: A

NEW QUESTION 5

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

NEW QUESTION 6

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?

- A. Unique values cannot be grouped
- 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.

Guaranteed success with Our exam guides

visit - https://www.certshared.com

Answer: A

NEW QUESTION 7

Refer to the exhibit.

Event Attribute

Filter By:

Event Keywords

Event Attribute

CMDB Attribute

Clear All

Load

Save

Paren	Attribute	Operator	Value	Paren	Next	Row
⊖	⊕ Raw Event Log	=	⌵ udp	⊖	⊕ AND OR	⊕ 🗑

Time Range:

Real-time

Relative

Absolute

Last

2

Hours

⌵

Trend Interval:

Auto

⌵

Result Limit:

100

K rows

Apply & Run

Apply

Cancel

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 colum

B. This is the wrong Boolean operator.

C. The Time Range value should be set to Real-Time.

D. The keyword is case sensitiv

E. Instead of typing udp in the Value field, the analyst should type UDP.

F. The analyst selected = in the Operator colum

G. That is the wrong operator.

Answer: D

NEW QUESTION 8

How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

- A. FortiSIEM changes the incident status to Repeated, and updates the Last Seen timestamp.

B. FortiSIEM updates the Incident Count value and Last Seen timestamp.

C. FortiSIEM generates a new incident based on the Rule Frequency value, and updates the First Seen and Last Seen timestamps.

D. FortiSIEM generates a new incident each time the rule triggers, and updates the First Seen and Last Seen timestamps.

Answer: B

NEW QUESTION 9

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

NEW QUESTION 10

Refer to the exhibit.

Analytics Search

Filter By:

Event Keywords

Event Attribute

CMDB Attribute

Clear All

Load

Save

	Paren	Attribute	Operator	Value	Paren	Next	Row
	⊖	⊕ User	IN	▼ Device IP: Server Inventory	⊖	⊕ AND OR	+ 🗑
	⊖	⊕ Event Type	IN	▼ Group: Logon Failure	⊖	⊕ AND OR	+ 🗑

Time Range:

Real-time

Relative

Absolute

Last

10

Days

▼

The analyst is troubleshooting the analytics query shown in the exhibit. Why is this search not producing any results?

- A. The Time Range is set incorrectly.
- B. The inner and outer nested query attribute types do not match.
- C. You cannot reference User and Event Type attributes in the same search.
- D. The Boolean operator is wrong between the attributes.

Answer: B

NEW QUESTION 10

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

Explanation:

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 13

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: B

NEW QUESTION 16

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	/ + -		+ -

SubPattern Properties

Edit SubPattern

Name: Failed_Logon

Filters:

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

Aggregate:

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

Group By: Attribute

User	+ -	↑ ↓
Destination IP	+ -	↑ ↓
Source IP	+ -	↑ ↓

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?

- 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

NEW QUESTION 18

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

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

Answer: AC

NEW QUESTION 22

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

NEW QUESTION 27

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

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

Answer: A

NEW QUESTION 30

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FSM_AN-7.2 Practice Exam Features:

- * FCP_FSM_AN-7.2 Questions and Answers Updated Frequently
- * FCP_FSM_AN-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FSM_AN-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FSM_AN-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FSM_AN-7.2 Practice Test Here](#)