

Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst



NEW QUESTION 1

Refer to the exhibit.

Event Details X

Raw Message i o

```
<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 2

Refer to the exhibit.

Incident generator window

Generate Incident for: Logon_Failure X

Incident Attributes:	Event Attribute	Subpattern	Filter Attribute	Filter Attribute	Row
	Source IP	= Logon_Fail	Source IP	Source IP	+ -
	Destination IP	= Logon_Fail	Destination IP	Destination IP	+ -
	User	= Logon_Fail	User	User	+ -

Insert Attribute: Destination IP +

Incident Title: Suser from SsrcIpAddr failed to logon to SdestIpAddr

Triggered Attributes: Available: Search...

- WLAN Interface Interefence Index
- Execute Thread Peak
- Session Process Time ms
- Tomcat manager Check Frequency
- Printer Current Supply Level
- Printer Supply Name

1/33

> < ^ v

Selected:

- Event Receive Time
- Event Type
- Reporting IP
- Raw Event Log

Save
Cancel

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?

- 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

NEW QUESTION 3

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.

Answer: A

NEW QUESTION 4

How can you query the configuration management database (CMDB) in an analytics search?

- A. Click Value > Select from CMDB.
- B. On the CMDB tab, select an entry, and then click Create Search.
- C. On the Admin tab, click CMDB Search.
- D. Click Attribute > Select from CMDB.

Answer: A

NEW QUESTION 5

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 6

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 and Count attributes, how many results will FortiSIEM display?

- A. Two
- B. Six
- C. Three
- D. Five
- E. One

Answer: D

NEW QUESTION 7

Refer to the exhibit.

Automation Policy

Name:

Severity: Low Medium High





Rules: ▼

Time Range: ▼

Affected Items: ▼

Affected Orgs: ▼

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

Settings:

- Do not notify when an incident is cleared automatically.
- Do not notify when an incident is cleared manually.
- Do not notify when an incident is cleared by system.

Comments:

What happens when an analyst clears an incident generated by a rule containing the automation policy shown in the exhibit?

- A. No notification is sent.
- B. An email is sent to the SOC manager.
- C. The remediation script is run.
- D. A notification is sent to the SOC manager dashboard.

Answer: B

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)