

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.

Incident generator window

Generate Incident for: Logon_Failure

Incident Attributes:

Event Attribute	Subpattern	Filter Attribute	Row
Source IP	= Logon_Fail	Source IP	
Destination IP	= Logon_Fail	Destination IP	
User	= Logon_Fail	User	

Insert Attribute:

Destination IP

+

Incident Title:

Suser from SsrcIpAddr failed to logon to SdestIpAddr

Triggered Attributes:

Available: Search...

1/33

WLAN Interface Intereference Index

Execute Thread Peak

Session Process Time ms

Tomcat manager Check Frequency

Printer Current Supply Level

Printer Supply Name

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

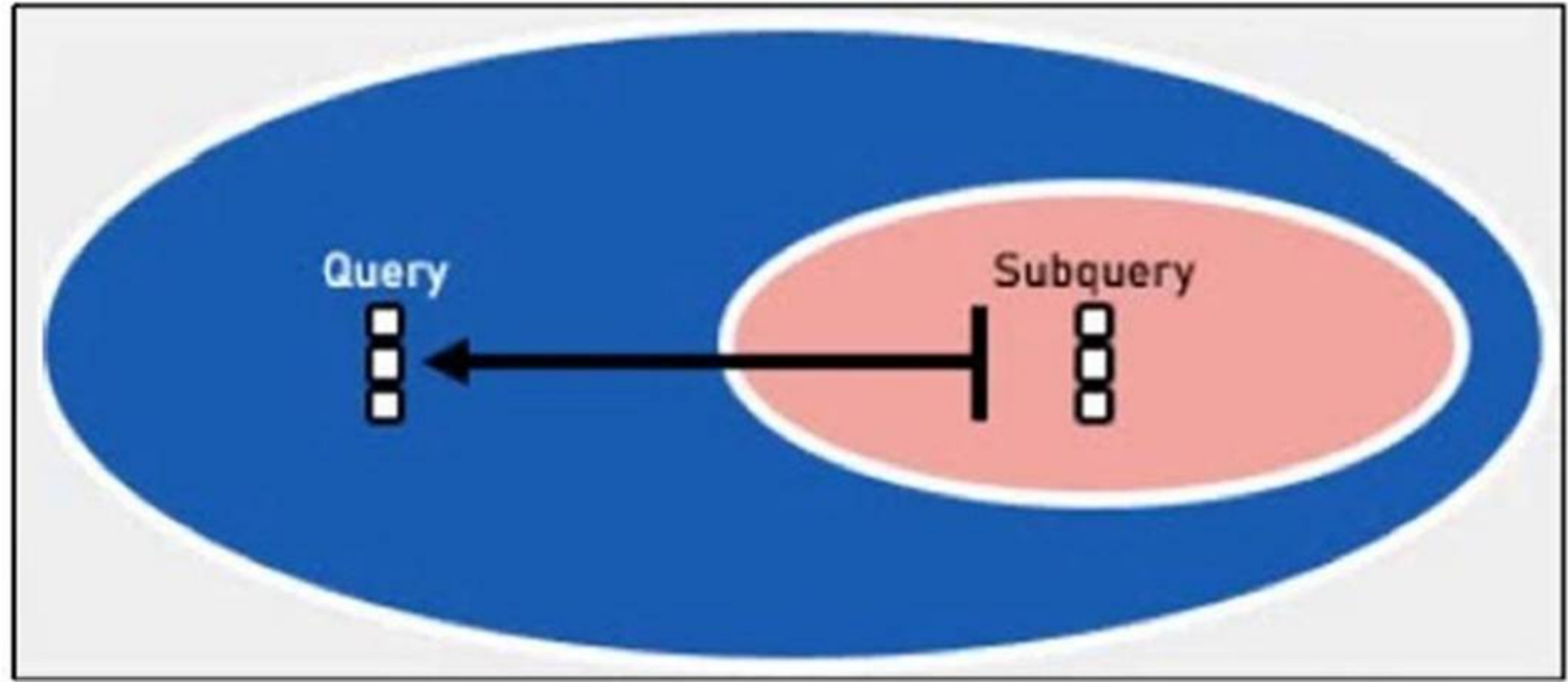
Which statement about thresholds is true?

- 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 4

Refer to the exhibit.



Which two lookup types can you reference as the subquery in a nested analytics query? (Choose two.)

- A. LDAP Query
- B. CMDB Query
- C. SNMP Query
- D. Event Query

Answer: BD

NEW QUESTION 5

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 6

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 7

Which analytics search can be used to apply a user and entity behavior analytics (UEBA) tag to an event for a failed login by the user JSmith?

- A. User = smith
- B. Username NOT END WITH jsmith
- C. User IS jsmith
- D. Username CONTAIN smit

Answer: D

NEW QUESTION 8

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 9

Refer to the exhibit.

Subpattern 1

Edit SubPattern

Name: RDP_Connection

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Destination TCP/UDP Port	=	3389	+	AND OR	+ -
+	Event Type	=	FortiGate-traffic-forward	+	AND OR	+ -

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT(Matched Events)	>=	1	+	AND OR	+ -

Group By:

Attribute	Row	Move
User	+	+
Source IP	+	+

Run as Query

Save as Report

Save

Cancel

Subpattern 2

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)	>=	3	+	AND OR	+ -

Group By:

Attribute	Row	Move
User	+	+
Source IP	+	+
Destination IP	+	+

Run as Query

Save as Report

Save

Cancel

Rule Conditions

Step 1: General >

Step 2: Define Condition >

Step 3: Define Action

Condition: If this Pattern occurs within any 300 second time window

Paren	Subpattern	Paren	Next	Row
+	RDP_Connection	+	FOLLOWED_BY	+
+	Failed_Logon	+		+

Given these Subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next	Row
RDP_Connection	User	=	Failed_Logon	User	AND	+
RDP_Connection	Source IP	=	Failed_Logon	Source IP		+

Save

Cancel

Which two conditions will match this rule and subpatterns? (Choose two.)

- A. A user using RDP over SSL VPN fails to log in to an application five times.
- B. A user runs a brute force password cracker against an RDP server.
- C. A user fails twice to log in when connecting through RDP.
- D. A user connects to the wrong IP address for an RDP session five times.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Answer: AB

Explanation:

The user initiates an RDP session (Subpattern 1) and then fails to log in multiple times (Subpattern 2 with COUNT(Matched Events) > = 3) - both from the same Source IP and User within 300 seconds.

The brute force attempts typically involve a successful RDP connection followed by multiple failed logins, satisfying the sequence and grouping conditions in the rule.

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 10

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

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.

NEW QUESTION 14

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 19

Refer to the exhibit.

Automation Policy

Name
SOC Notification

Severity:
☒ Low
☒ Medium
☒ High

Rules:
ANY

Time Range:
ANY

Affected Items:
ANY

Affected Orgs:
ANY

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:

Save
Cancel

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 24

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

Refer to the exhibit.



Expression: COUNT()/Matched Events

Builder: ☐ Vertical Add to ↑ ?

Select function...

"count()matched events" is invalid

Validate Clear

OK Cancel

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

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](#)