

# Fortinet

## FCP\_FSM\_AN-7.2

### Fortinet FCP - FortiSIEM 7.2 Analyst

For More Information – Visit link below:

<https://www.examsempire.com/>

**Product Version**

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/fcp-fsm-an-7-2>

# Latest Version: 6.0

## Question: 1

Refer to the exhibit.

Adware process found - Edit Details

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
<input type="radio"/>	AdwareFound	<input type="radio"/>		<input type="radio"/>

Save Cancel

What does the Define Condition time field determine for this rule?

- A. The time of day the rule will trigger.
- B. How often the rule will evaluate the subpattern(s).
- C. How often the rule will perform remediation.
- D. The time period over which the rule evaluates events.

**Answer: D**

## Question: 2

What are the five categories of incidents on FortiSIEM?

- A. Performance, other, availability, security, and change
- B. Devices, users, high risk, other, and low risk
- C. Security, change, high risk, low risk, and other
- D. Performance, other, devices, high risk, and low risk

**Answer: A**

## Question: 3

What must you configure to apply ZTNA tags from FortiSIEM to devices in FortiClient EMS?

- A. Syslog connection to FortiSIEM from FortiGate firewalls
- B. Syslog connection to FortiGate firewalls from FortiSIEM
- C. API connection from FortiSIEM to FortiClient EMS
- D. API connection from FortiClient EMS to FortiSIEM

**Answer: C**

#### Question: 4

Where can an analyst configure rule notifications and automated remediation on FortiSIEM?

- A. Notification policy
- B. Response policies
- C. Notification engine
- D. Automation policy

**Answer: D**

#### Question: 5

Which two elements can you use to define how an automation policy activates?  
(Choose two.)

- A. Lookup table
- B. Rules
- C. Watchlist
- D. Time range

**Answer: B,D**

#### Question: 6

From which two sources can you import data to train FortiSIEM machine learning?  
(Choose two.)

- A. Syslog archives
- B. CSV files
- C. FortiSIEM reports
- D. SQL database

**Answer: B,C**

## Question: 7

Refer to the exhibit.

**Edit SubPattern**

Name: DomainAcctLockout

**Filters:**

	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Event Type	IN	EventTypes: Domain Account Lockout	-	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 settings that determine which attribute associations are used to trigger an incident?

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

**Answer: D**

## Question: 8

What feature defines when an incident is created by FortiSIEM?

- A. Rules
- B. Cases
- C. Analytics
- D. CMDB

**Answer: A**

## Question: 9

When using user and entity behavior analytics (UEBA) on FortiSIEM, what must you use to dynamically supply a list of IP addresses to a FortiGate device for blocking purposes?

- A. API Connection
- B. SCP
- C. Watchlists
- D. Lookup tables

**Answer: C**

### Question: 10

Which two attributes can you not select together in the Group By and Display Fields?  
(Choose two.)

- A. Source IP
- B. Raw Event Log
- C. Destination IP
- D. Event Reporting Time
- E. Reporting IP

**Answer: B,C**

**Thank You for Trying Our Product**

**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**