



Vendor: Fortinet

Exam Code: NSE6_FSM_AN-7.4

Exam Name: Fortinet NSE 6 - FortiSIEM 7.4 Analyst

Version: DEMO

QUESTION 1

Refer to the exhibit. When the subpattern is matched, what does the time condition of 60 seconds mean?

The screenshot shows the 'Add New Rule' configuration window. The 'Step 2: Define Condition' tab is selected. The condition is set to 'If this Pattern occurs within any 60 second time window'. The subpattern is 'VPNLogon'. The 'Next' field is empty. The 'Save' and 'Cancel' buttons are at the bottom.

- A. The subpattern must be matched at least twice within 60 seconds to trigger this rule.
- B. The rule will trigger remediation actions every 60 seconds when the subpattern is triggered.
- C. The rule engine will evaluate events every 60 seconds looking for the subpattern.
- D. It is the time period over which the rule will aggregate and evaluate events.

Answer: D

Explanation:

The 60-second time window defines the aggregation and evaluation period for the rule. FortiSIEM evaluates whether the specified subpattern conditions occur within that 60-second interval before triggering the rule.

QUESTION 2

What is one difference between a lookup table and a watchlist?

- A. Watch list entries do not expire, lookup table entries have a defined lifetime.
- B. A lookup table requires a parser to be able to query and interpret the data, a watchlist does not require a parser.
- C. A watchlist can be updated through an API, and a lookup table cannot.
- D. A lookup table can have multiple columns, and a watchlist only has one.

Answer: D

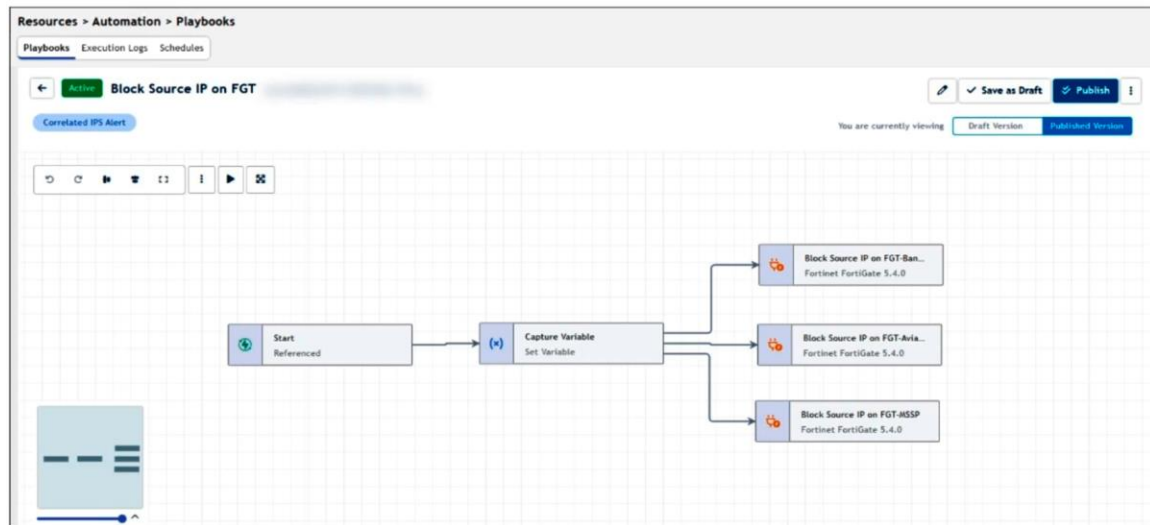
Explanation:

A lookup table supports multiple columns and structured datasets, allowing more complex mappings and queries. A watchlist contains only a single column of values used for direct matching operations.

QUESTION 3

Refer to the exhibit. If the Capture Variable step ingests the source IP address from an incident and the Block Source IP on FGT step blocks that source IP address on the configured firewall, what will happen when this playbook is executed?

Playbook configuration



- A. Three different source IP addresses, depending on the network configuration of the firewalls, will be blocked.
- B. A different source IP address, depending on the organization, will be blocked on all three firewalls.
- C. The same source IP address will be blocked on all three firewalls.
- D. A single source IP address from the incident will be blocked on the first playbook connector.

Answer: C

Explanation:

The Capture Variable step extracts a single source IP address from the incident and passes that same value to each downstream firewall connector. As a result, the same source IP address will be blocked on all three configured firewalls when the playbook executes.

QUESTION 4

Refer to the exhibit. What will happen when a device being analyzed by the machine learning (ML) configuration shown in the exhibit has a consistently high memory use?

The screenshot shows the configuration for an ML regression model in FortiSIEM. It is set to 'Local' run mode, 'Regression' task, and 'DecisionTreeRegressor' algorithm. Under 'Fields to use for Prediction', four fields are listed: 'AVG(CPU Util)' (unchecked), 'AVG(Memory Util)' (checked), 'AVG(Sent Bytes64)' (checked), and 'AVG(Received Bytes64)' (checked). Under 'Field to Predict', four fields are listed: 'AVG(CPU Util)' (selected with a radio button), 'AVG(Memory Util)' (unselected), 'AVG(Sent Bytes64)' (unselected), and 'AVG(Received Bytes64)' (unselected).

- A. FortiSIEM will lower the CPU use trigger requirement for CPU use.
- B. FortiSIEM will update the regression tables for memory use, and average sent and received bytes.
- C. FortiSIEM will trigger an incident for high memory use.
- D. FortiSIEM will update the model with a higher memory use average value.

Answer: D

Explanation:

The ML regression model uses memory utilization, sent bytes, and received bytes as prediction inputs for CPU utilization. If memory usage remains consistently high, FortiSIEM adapts the learned baseline and updates the model with a higher average memory utilization value over time.

QUESTION 5

Refer to the exhibits. Which information will this analytics search display?

Analytics Search

Filter By:
Event Keywords
Event Attribute
CMDB Attribute
Clear All
Load
Save

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

Time Range:
Real-time
Relative
Absolute

Last 10 Days

Inner Query Value

Select From Report

Report: Server Inventory

Attribute: Device IP

OK Cancel

- A. Failed machine login events with a source IP address of servers in the Device IP report
- B. All servers in the Logon Failure user group
- C. Failed login events from all servers in the Server Inventory configuration management database (CMDB) report
- D. Failed login events from all servers defined in the CMDB

Answer: C

Explanation:

The search filters for Event Type values in the Logon Failure group and matches Destination IP addresses against the Device IP values returned from the Server Inventory CMDB report. This displays failed login events involving servers contained in the Server Inventory CMDB report.

QUESTION 6

Refer to the exhibit. Which two things that happen when this automation policy triggers? (Choose two.)

Automation policy

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.
 ☐ Run Playbook on Incident Trigger
 ☐ 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

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

Answer: BD

Explanation:

The automation policy has Send Email/SMS/Webhook to the target users enabled, so an email notification is sent. It also has Run Remediation/Script enabled, so the configured remediation script is executed when the policy triggers.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14