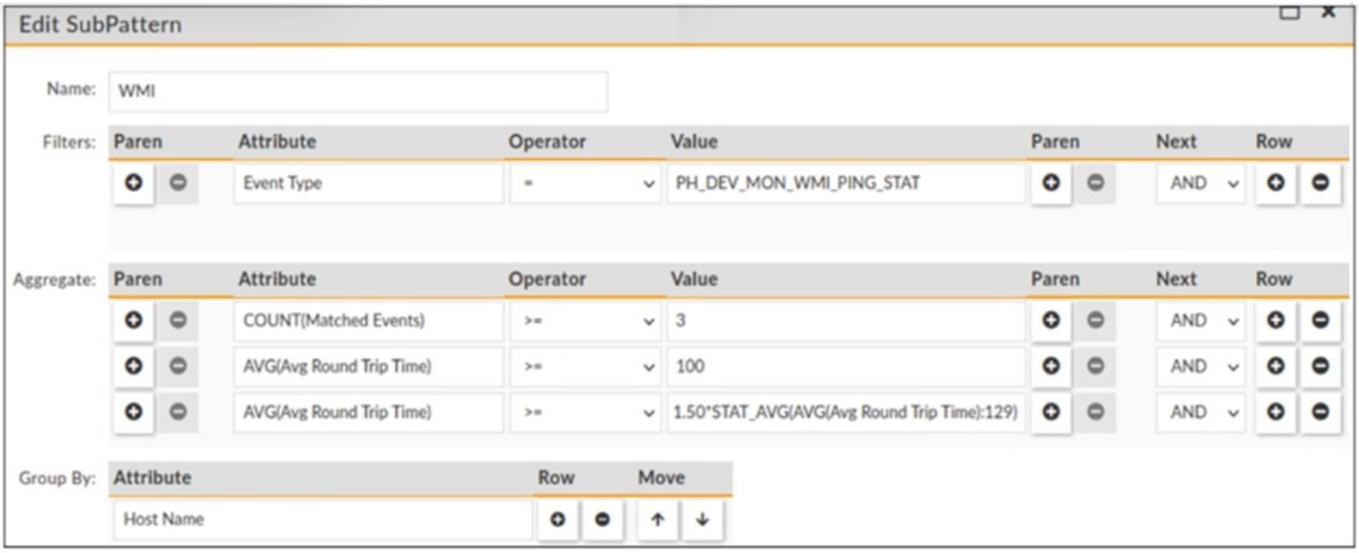
NSE7_ADA-6.3$^{Q\&As}$

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit.



Edit SubPattern

Name: WMI

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	=	PH_DEV_MON_WMI_PING_STAT	⊕ ⊖	AND	⊕ ⊖

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	3	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	AVG(Avg Round Trip Time)	>=	100	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	AVG(Avg Round Trip Time)	>=	1.50*STAT_AVG(AVG(Avg Round Trip Time):129)	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
Host Name	⊕ ⊖	↑ ↓

The window for this rule is 30 minutes. What is this rule tracking?

A. A sudden 50% increase in WMI response times over a 30-minute time window

B. A sudden 1.50 times increase in WMI response times over a 30-minute time window

C. A sudden 75% increase in WMI response times over a 30-minute time window

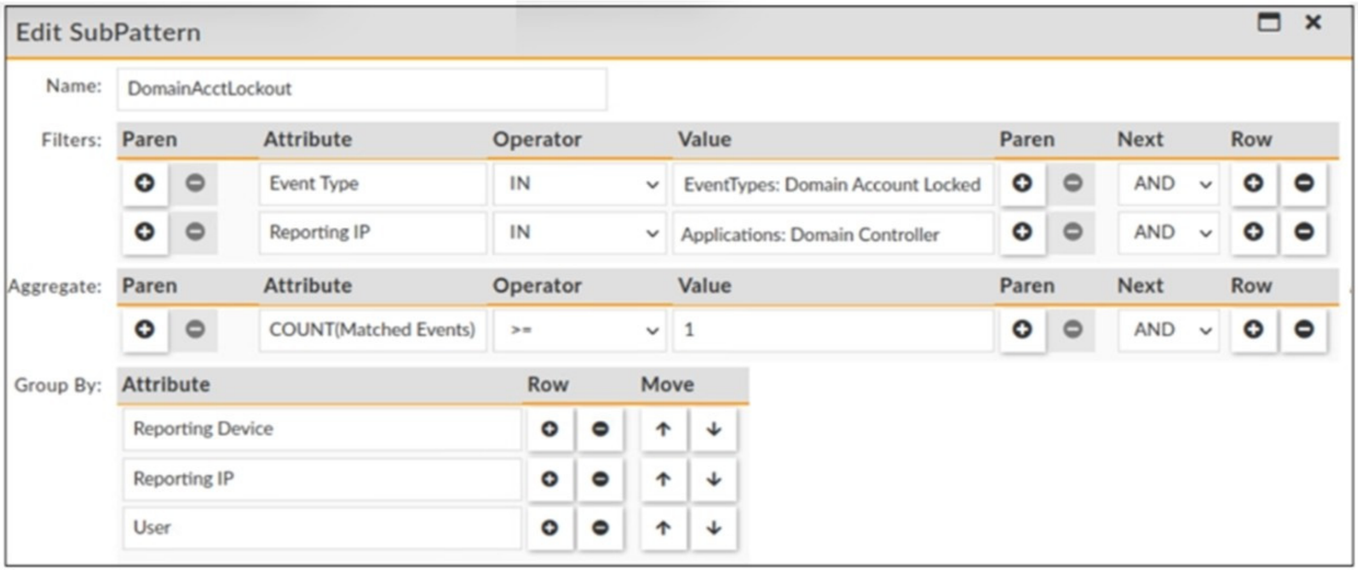
D. A sudden 150% increase in WMI response times over a 30-minute time window

Correct Answer: B

Explanation: The rule is tracking the WMI response times from Windows devices using a baseline calculation. The rule will trigger an incident if the current WMI response time is greater than or equal to 1.50 times the average WMI response time in the last 30 minutes.

QUESTION 2

Refer to the exhibit.



Edit SubPattern

Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	IN	EventTypes: Domain Account Locked	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	Reporting IP	IN	Applications: Domain Controller	⊕ ⊖	AND	⊕ ⊖

Aggregate:

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

Group By:

Attribute	Row	Move
Reporting Device	⊕ ⊖	↑ ↓
Reporting IP	⊕ ⊖	↑ ↓
User	⊕ ⊖	↑ ↓

Which statement about the rule filters events shown in the exhibit is true?

A. The rule filters events with an event type that belong to the Domain Account Locked CMDB group or a reporting IP that belong to the Domain Controller applications group.

B. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting |P that belong to the Domain Controller applications group.

C. The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a user that belongs to the Domain Controller applications group.

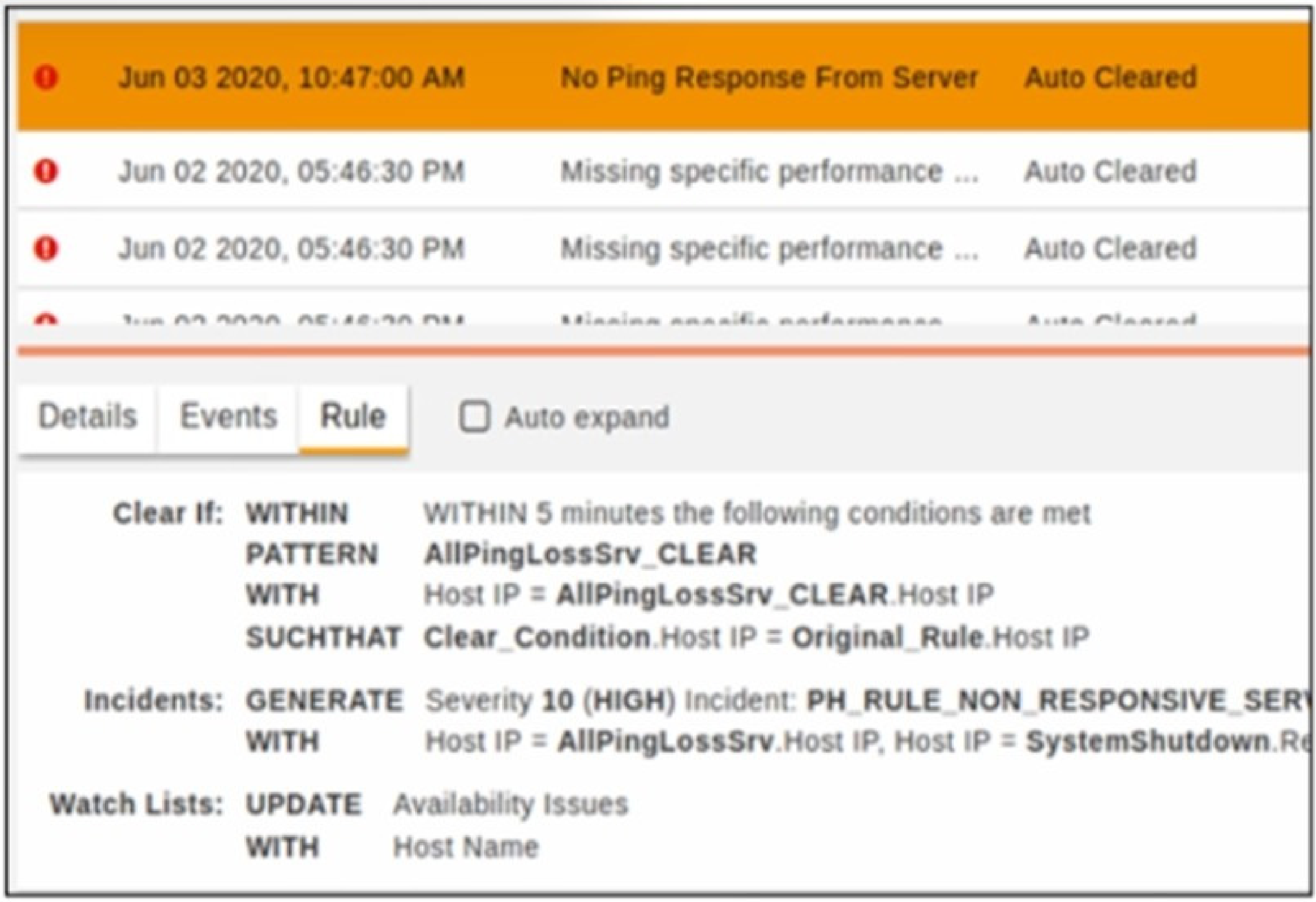
D. The rule filters events with an event type that equals Domain Account Locked and a reporting IP that equals Domain Controller applications.

Correct Answer: B

Explanation: The rule filters events with an event type that belong to the Domain Account Locked CMDB group and a reporting IP that belong to the Domain Controller applications group. This means that only events that have both criteria met will be processed by this rule. The event type and reporting IP are joined by an AND operator, which requires both conditions to be true.

QUESTION 3

Refer to the exhibit.



●	Jun 03 2020, 10:47:00 AM	No Ping Response From Server	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared
●	Jun 02 2020, 05:46:30 PM	Missing specific performance ...	Auto Cleared

```
      Clear If: WITHIN     WITHIN 5 minutes the following conditions are met
                PATTERN    AllPingLossSrv_CLEAR
                WITH       Host IP = AllPingLossSrv_CLEAR.Host IP
                SUCHTHAT   Clear_Condition.Host IP = Original_Rule.Host IP

    Incidents:  GENERATE   Severity 10 (HIGH) Incident: PH_RULE_NON_RESPONSIVE_SER
                WITH       Host IP = AllPingLossSrv.Host IP, Host IP = SystemShutdown.Re

  Watch Lists:  UPDATE   Availability Issues
                WITH     Host Name
```

Why was this incident auto cleared?

A. Within five minutes the packet loss percentage dropped to a level where the reporting IP is the same as the host IP

B. The original rule did not trigger within five minutes

C. Within five minutes, the packet loss percentage dropped to a level where the reporting IP is same as the source IP

D. Within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern

Correct Answer: D

Explanation: The incident was auto cleared because within five minutes, the packet loss percentage dropped to a level where the host IP of the original rule matches the host IP of the clear condition pattern. The clear condition pattern specifies that if there is an event with a packet loss percentage less than or equal to 10% and a host IP that matches any host IP in this incident, then clear this incident.

QUESTION 4

Identify the processes associated with Machine Learning/AI on FortiSIEM. (Choose two.)

A. phFortiInsightAI

B. phReportMaster

C. phRuleMaster

D. phAnomaly

E. phRuleWorker

Correct Answer: AD

Explanation: The processes associated with Machine Learning/AI on FortiSIEM are phFortiInsightAI and phAnomaly. phFortiInsightAI is responsible for detecting anomalous user behavior using UEBA (User and Entity Behavior Analytics) techniques. phAnomaly is responsible for detecting anomalous network behavior using NTA (Network Traffic Analysis) techniques.

QUESTION 5

Which syntax will register a collector to the supervisor?

A. phProvisionCollector --add

B. phProvisionCollector --add

C. phProvisionCollector --add

D. phProvisionCollector --add

Correct Answer: B

Explanation: The syntax that will register a collector to the supervisor is phProvisionCollector --add . This command will initiate the registration process between the collector and the supervisor, and exchange certificates and configuration information. The parameter is the IP address of the supervisor node.

Latest NSE7_ADA-6.3 Dumps   NSE7_ADA-6.3 Study Guide   NSE7_ADA-6.3 Exam Questions