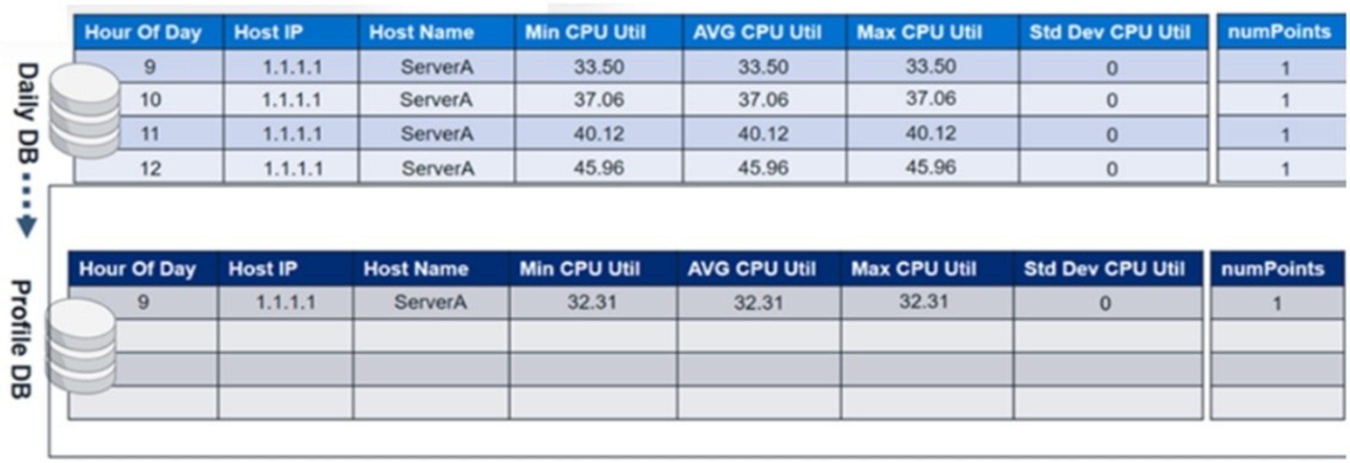
NSE7_ADA-6.3$^{Q\&As}$

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit. Click on the calculator button.


Daily DB
Profile DB

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	33.50	33.50	33.50	0	1
10	1.1.1.1	ServerA	37.06	37.06	37.06	0	1
11	1.1.1.1	ServerA	40.12	40.12	40.12	0	1
12	1.1.1.1	ServerA	45.96	45.96	45.96	0	1

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	32.31	32.31	32.31	0	1

The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database.

In the profile database, in the Hour of Day column where 9 is the value, what will be the updated minimum, maximum, and average CPU utilization values?

A. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=33.50

B. Min CPU Util=32.31, Max CPU Ucil=33.50 and AVG CPU Util=32.67

C. Min CPU Util=32.31, Max CPU Ucil=32.31 and AVG CPU Util=32.31

D. Min CPU Util=33.50, Max CPU Ucil=33.50 and AVG CPU Util=33.50

Correct Answer: B

Explanation: The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database using a weighted average formula:

New value = (Old value x Old weight) + (New value x New weight) / (Old weight + New weight)

The weight is determined by the number of days in each database. In this case, the profile database has one day of data and the daily database has one day of data, so the weight is equal for both databases. Therefore, the formula simplifies

to:

New value = (Old value + New value) / 2

In the profile database, in the Hour of Day column where 9 is the value, the updated minimum, maximum, and average CPU utilization values are:

Min CPU Util = (32.31 + 32.31) / 2 = 32.31 Max CPU Util = (33.50 + 33.50) / 2 = 33.50 AVG CPU Util = (32.67 + 32.67) /

2 = 32.67

QUESTION 2

What are the modes of Data Ingestion on FortiSOAR? (Choose three.)

A. Rule based

B. Notification based

C. App Push

D. Policy based

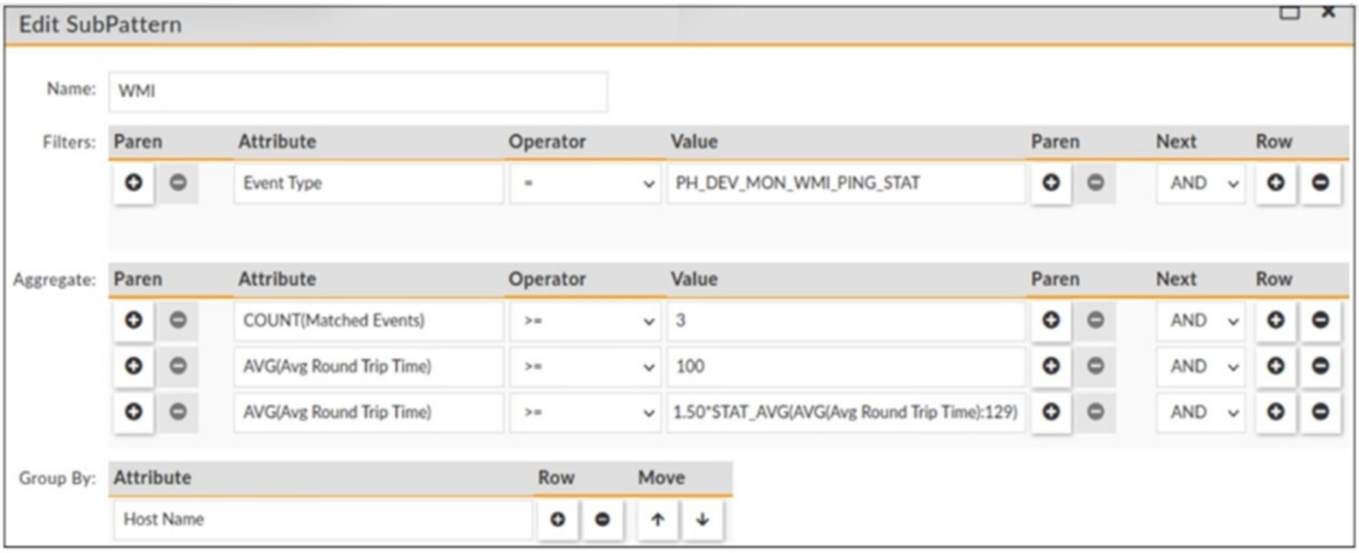
E. Schedule based

Correct Answer: BCE

Explanation: The modes of Data Ingestion on FortiSOAR are notification based, app push, and schedule based. Notification based mode allows FortiSOAR to receive data from external sources via webhooks or email notifications. App push mode allows FortiSOAR to receive data from external sources via API calls or scripts. Schedule based mode allows FortiSOAR to pull data from external sources at regular intervals using connectors. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 17

QUESTION 3

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

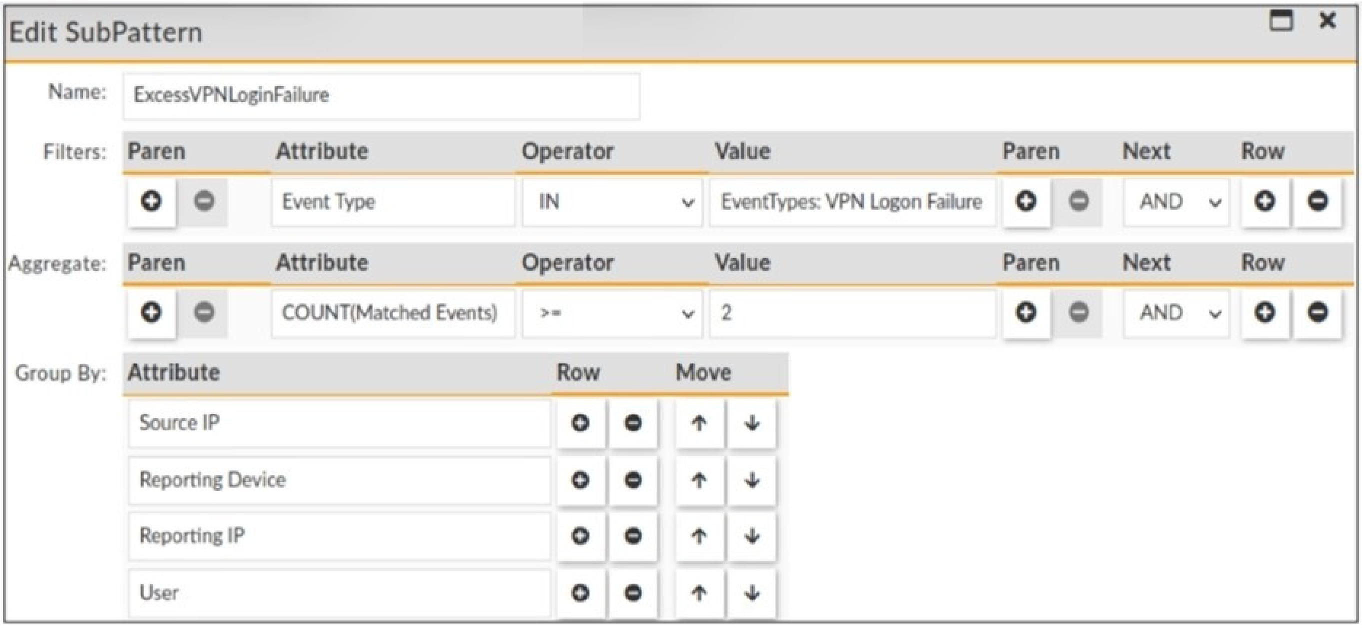
D. A sudden 150% increase in WMI response times over a 30-minute time window

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 4

Refer to the exhibit.



Edit SubPattern

Name: ExcessVPNLoginFailure

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	IN	EventTypes: VPN Logon Failure	⊕ ⊖	AND	⊕ ⊖

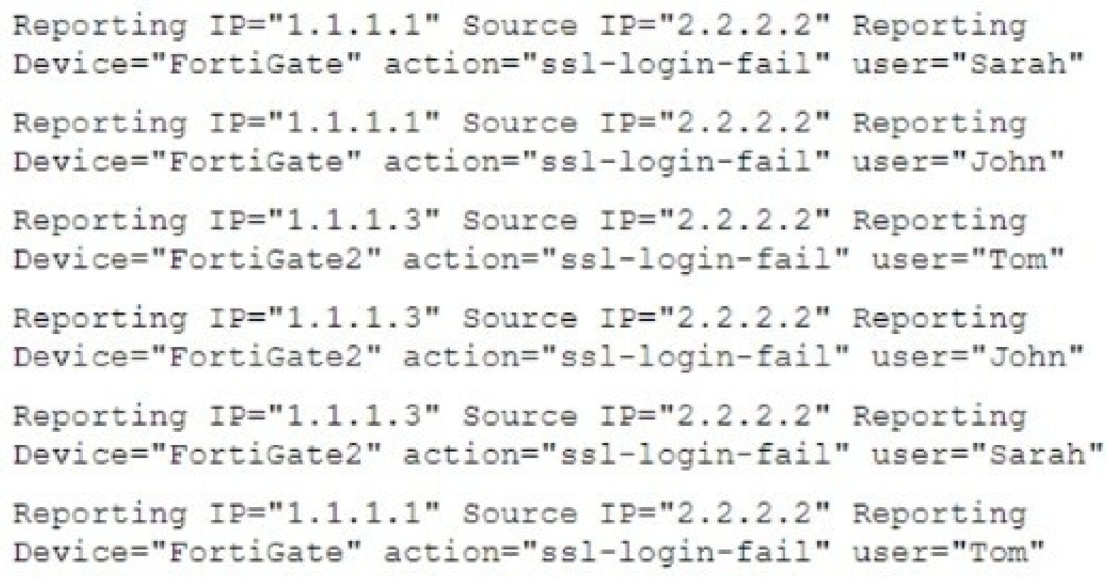
Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	2	⊕ ⊖	AND	⊕ ⊖

Group By:

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

The rule evaluates multiple VPN logon failures within a ten-minute window. Consider the following VPN failure events received within a ten-minute window:



```
Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="Sarah"

Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="John"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="Tom"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="John"

Reporting IP="1.1.1.3" Source IP="2.2.2.2" Reporting
Device="FortiGate2" action="ssl-login-fail" user="Sarah"

Reporting IP="1.1.1.1" Source IP="2.2.2.2" Reporting
Device="FortiGate" action="ssl-login-fail" user="Tom"
```

How many incidents are generated?

A. 1

B. 2

C. 0

D. 3

Correct Answer: B

Explanation: The rule evaluates multiple VPN logon failures within a ten-minute window. The rule will generate an incident if there are more than three VPN logon failures from the same source IP address within a ten-minute window. Based

on the VPN failure events received within a ten-minute window, there are two incidents generated:

One incident for source IP address 10.10.10.10, which has four VPN logon failures at 09:01, 09:02, 09:03, and 09:04.

One incident for source IP address 10.10.10.11, which has four VPN logon failures at 09:06, 09:07, 09:08, and 09:09.

QUESTION 5

Which three statements about phRuleMaster are true? (Choose three.)

A. phRuleMaster queues up the data being received from the phRuleWorkers into buckets.

B. phRuleMaster is present on the supervisor and workers.

C. phRuleMaster is present on the supervisor only

D. phRuleMaster wakes up to evaluate all the rule data in series, every 30 seconds.

E. phRuleMaster wakes up to evaluate all the rule data in parallel, even/ 30 seconds

Correct Answer: ABE

Explanation: phRuleMaster is a process that performs rule evaluation and incident generation on FortiSIEM. phRuleMaster queues up the data being received from the phRuleWorkers into buckets based on time intervals, such as one minute, five minutes, or ten minutes. phRuleMaster is present on both the supervisor and workers nodes of a FortiSIEM cluster. phRuleMaster wakes up every 30 seconds to evaluate all the rule data in parallel using multiple threads.

Latest NSE7_ADA-6.3 Dumps NSE7_ADA-6.3 PDF Dumps NSE7_ADA-6.3 Braindumps