NSE7_ADA-6.3 Q&As

Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse7_ada-6-3.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. Rule based

B. Notification based

C. App Push

D. Policy based

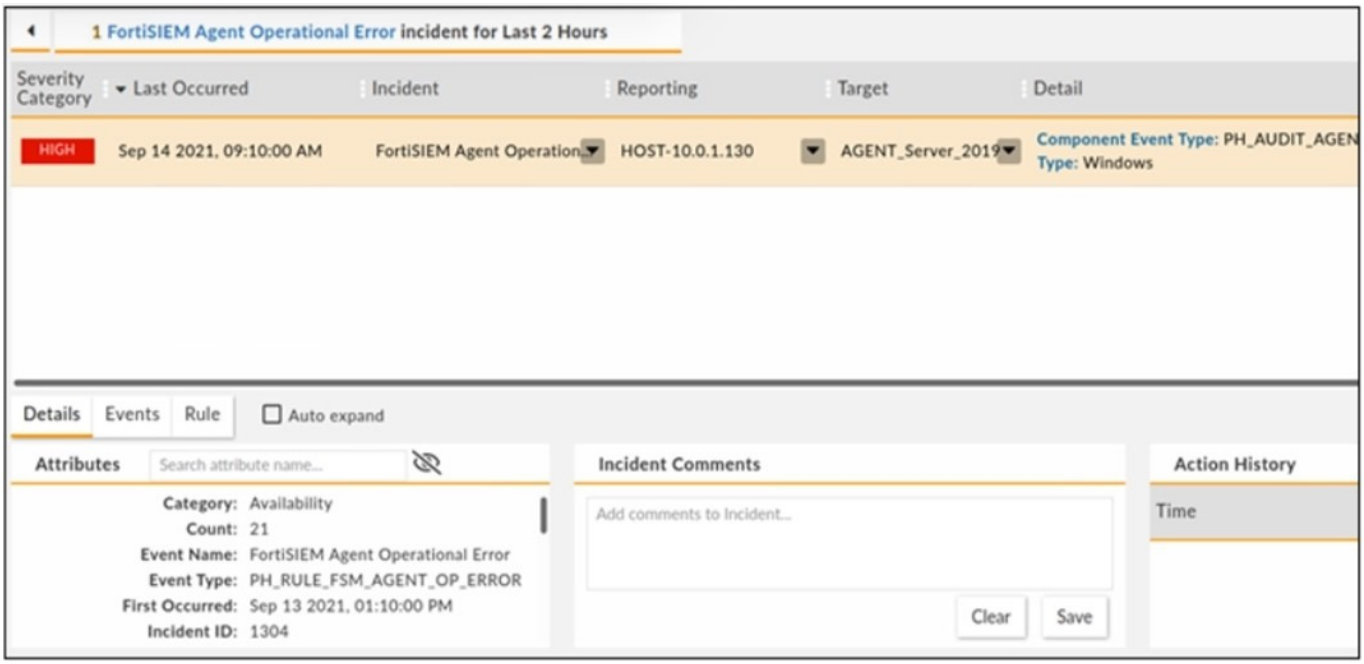
E. Schedule based

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 2

Refer to the exhibit.



How long has the UEBA agent been operationally down?

A. 21 Hours

B. 9 Hours

C. 20 Hours

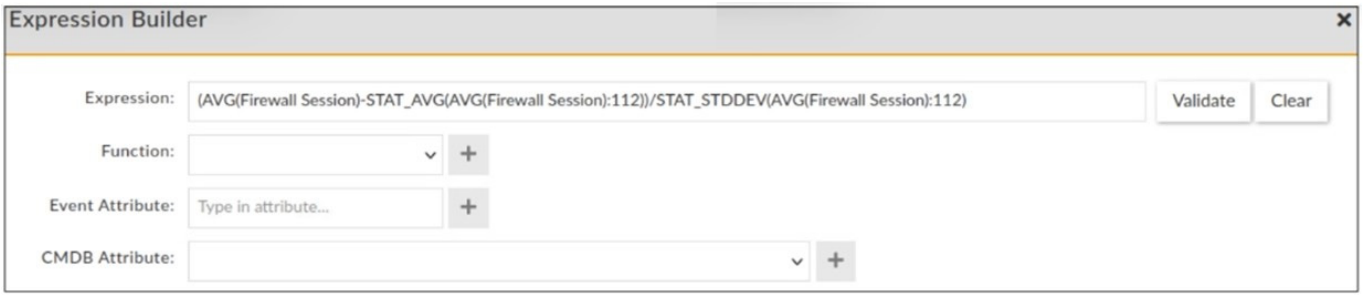
D. 2 Hours

Correct Answer: A

Explanation: The UEBA agent status shows that it has been operationally down for one day and three hours ago (1d3h). This means that it has been down for 24 hours plus three hours, which is equal to 21 hours.

QUESTION 3

Refer to the exhibit.



If the Z-score for this rule is greater than or equal to three, what does this mean?

A. The rate of firewall connection is optimum.

B. The rate of firewall connection is above the historical average value.

C. The rate of firewall connection is above the current average value.

D. The rate of firewall connection is below historical average value.

Correct Answer: B

Explanation: If the Z-score for this rule is greater than or equal to three, it means that the rate of firewall connection is above the historical average value. The Z-score is a measure of how many standard deviations a value is away from the mean of a distribution. A Z-score of three or more indicates that the value is significantly higher than the mean, which implies an anomaly or deviation from normal behavior.

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

What is Tactic in the MITRE ATTandCK framework?

A. Tactic is how an attacker plans to execute the attack

B. Tactic is what an attacker hopes to achieve

C. Tactic is the tool that the attacker uses to compromise a system

D. Tactic is a specific implementation of the technique

Correct Answer: B

Explanation: Tactic is what an attacker hopes to achieve in the MITRE ATTandCK framework. Tactic is a high-level category of adversary behavior that describes their objective or goal. For example, some tactics are Initial Access, Persistence, Lateral Movement, Exfiltration, etc. Each tactic consists of one or more techniques that describe how an attacker can accomplish that tactic.

QUESTION 6

On which disk are the SQLite databases that are used for the baselining stored?

A. Disk1

B. Disk4

C. Disk2

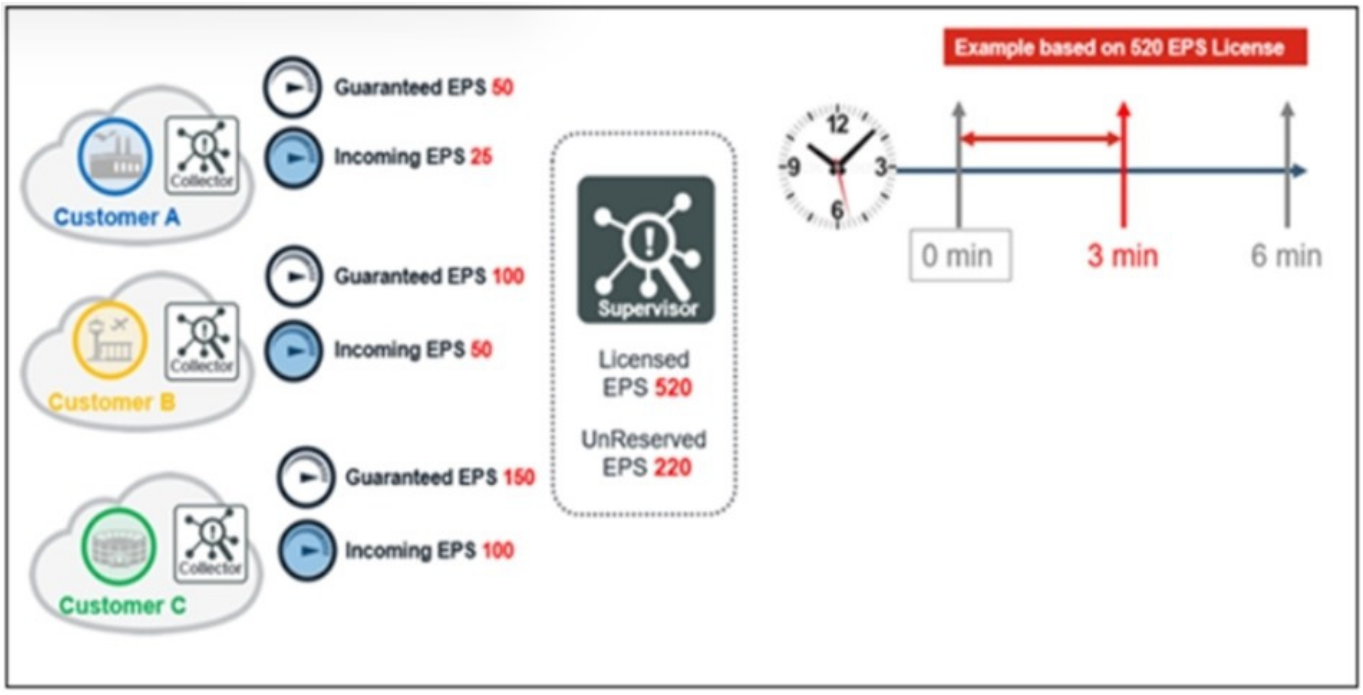
D. Disk3

Correct Answer: D

Explanation: The SQLite databases that are used for the baselining are stored on Disk3 of the FortiSIEM server. Disk3 is also used for storing raw event data and CMDB data.

QUESTION 7

Refer to the exhibit. Click on the calculator button.



Based on the information provided in the exhibit, calculate the unused events for the next three minutes for a 520 EPS license.

A. 72460

B. 73460

C. 74460

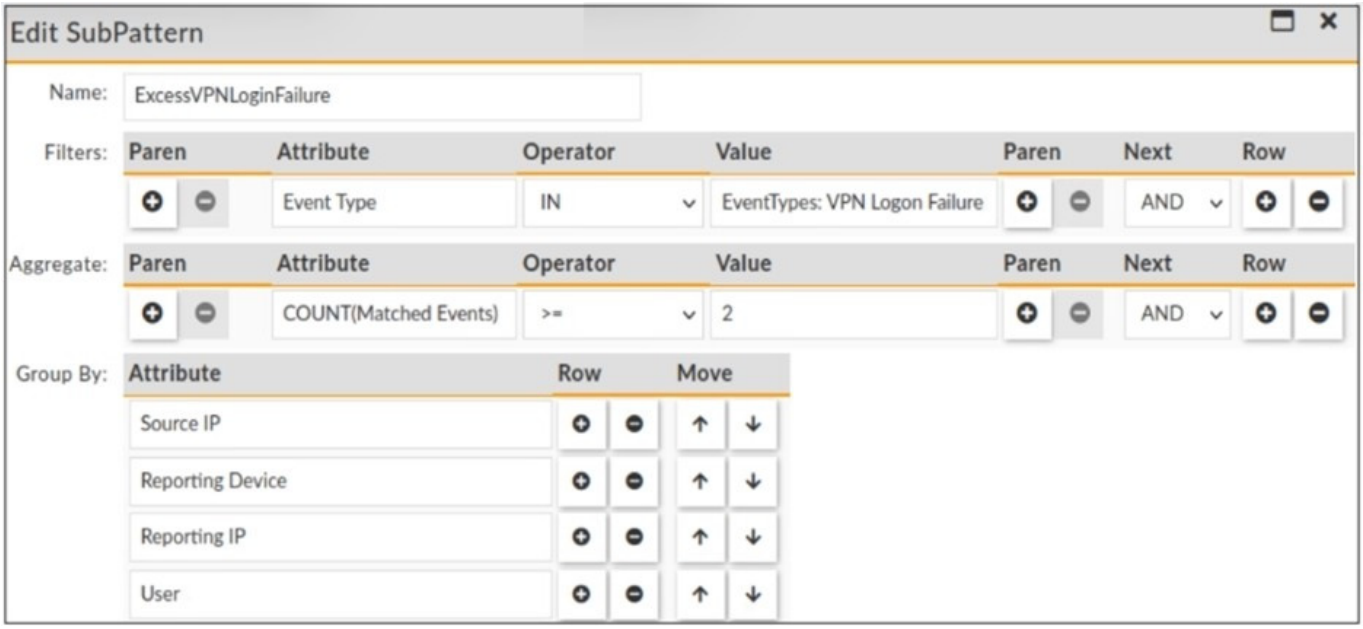
D. 71460

Correct Answer: B

Explanation: The unused events for the next three minutes for a 520 EPS license can be calculated by multiplying the licensed EPS by the time interval and subtracting the total number of events received in that interval. In this case, the calculation is: 520 x 180 - 27000 = 73460

QUESTION 8

Refer to the exhibit.



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 9

How can you invoke an integration policy on FortiSIEM rules?

A. Through Notification Policy settings

B. Through Incident Notification settings

C. Through remediation scripts

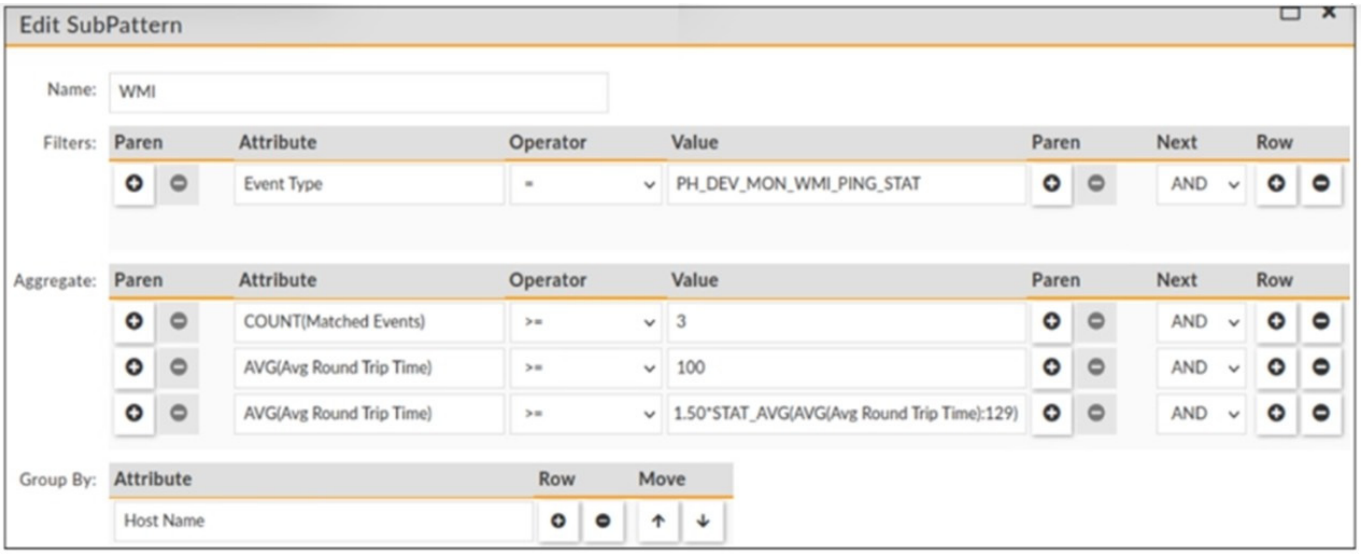
D. Through External Authentication settings

Correct Answer: A

Explanation: You can invoke an integration policy on FortiSIEM rules by configuring the Notification Policy settings. You can select an integration policy from the drop-down list and specify the conditions for triggering it. For example, you can invoke an integration policy when an incident is created, updated, or closed. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 9

QUESTION 10

Refer to the exhibit.



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.