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

QUESTION 1

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

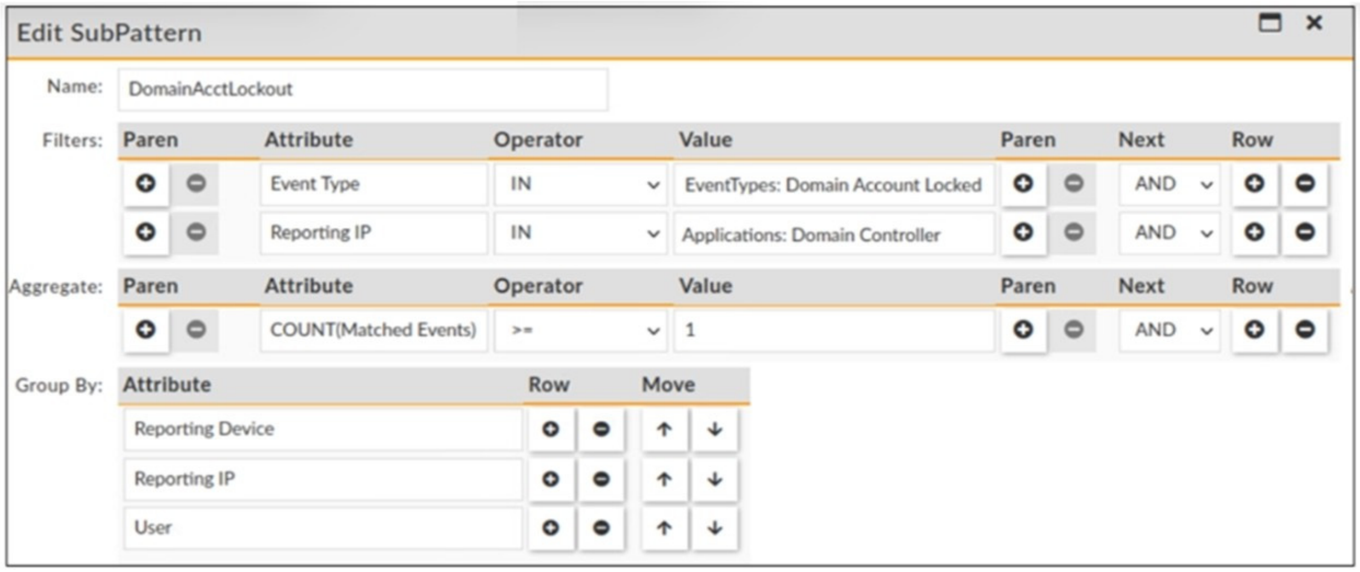
D. Tactic is a specific implementation of the technique

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 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

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

A. Rule based

B. Notification based

C. App Push

D. Policy based

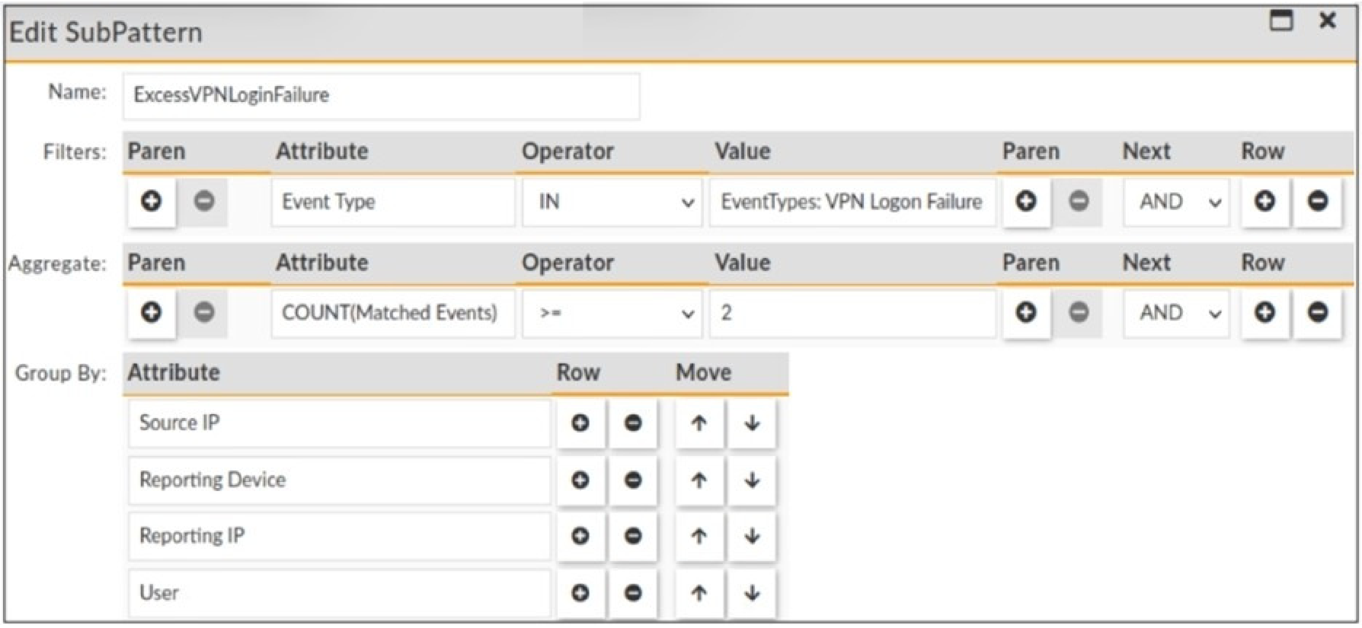
E. Schedule based

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 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	⊕ ⊖

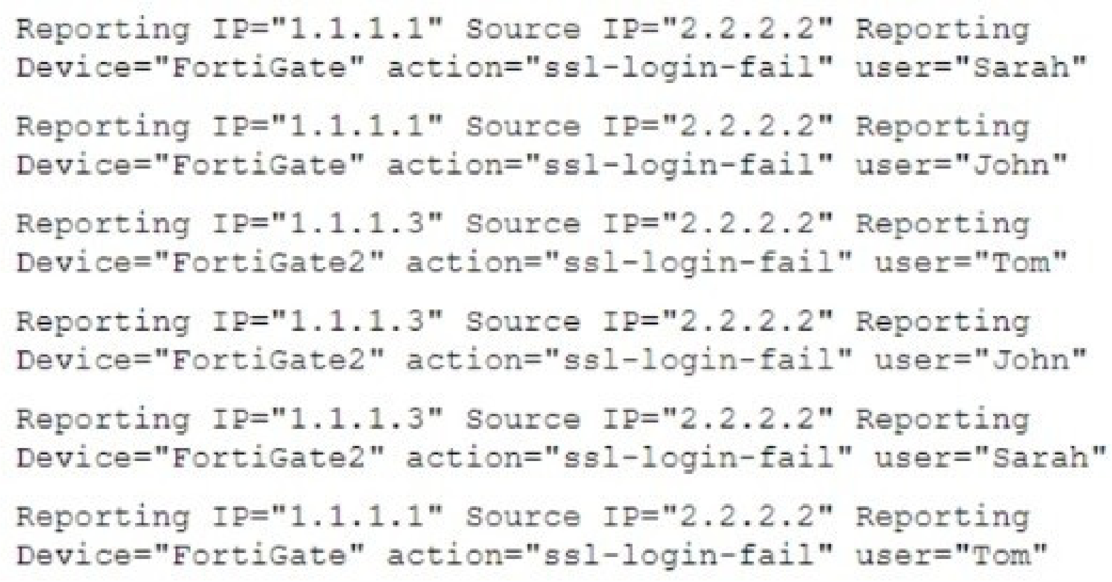
Aggregate:

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 two statements about the maximum device limit on FortiSIEM are true? (Choose two.)

A. The device limit is defined per customer and every customer is assigned a fixed number of device limit by the service provider.

B. The device limit is only applicable to enterprise edition.

C. The device limit is based on the license type that was purchased from Fortinet.

D. The device limit is defined for the whole system and is shared by every customer on a service provider edition.

Correct Answer: BC

Explanation: The device limit is a feature of the enterprise edition of FortiSIEM that restricts the number of devices that can be added to the system based on the license type. The device limit does not apply to the service provider edition, which allows unlimited devices per customer. The device limit is determined by the license type that was purchased from Fortinet, such as 100 devices, 500 devices, or unlimited devices.

Latest NSE7_ADA-6.3 Dumps   NSE7_ADA-6.3 VCE Dumps   NSE7_ADA-6.3 Braindumps