NSE7_ADA-6.3 Q&As

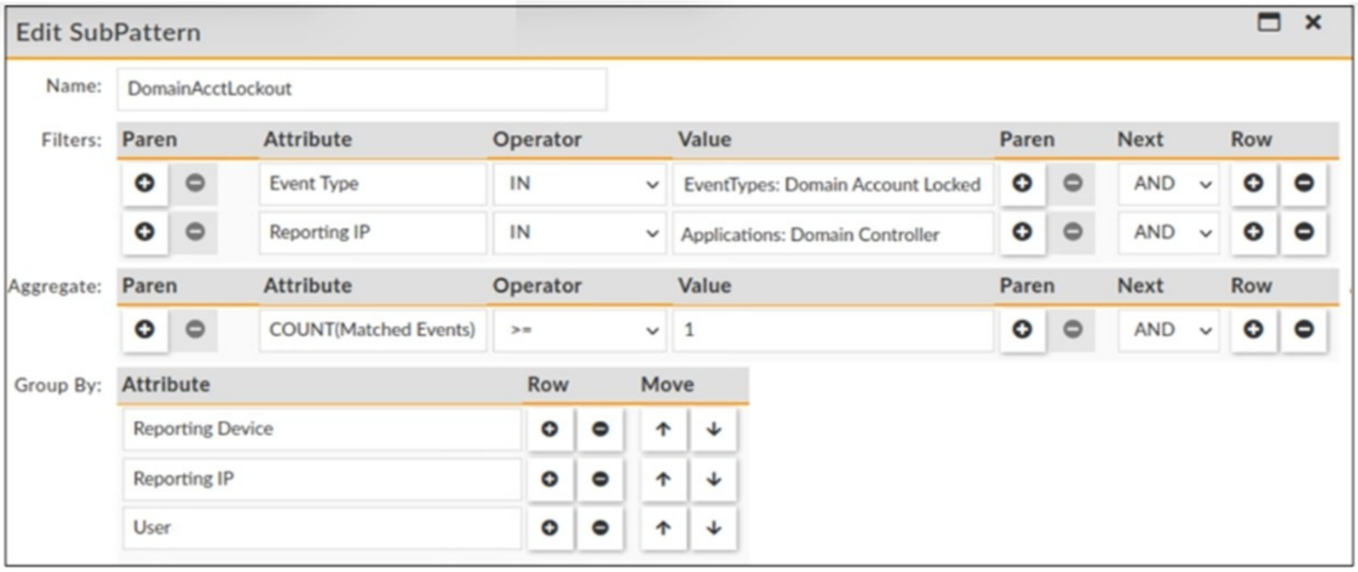
Fortinet NSE 7 - Advanced Analytics 6.3

Pass Fortinet NSE7_ADA-6.3 Exam with 100% Guarantee

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

QUESTION 1

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 2

Which three processes are collector processes? (Choose three.)

A. phAgentManaqer

B. phParser

C. phRuleMaster

D. phReportM aster

E. phMonitorAgent

Correct Answer: BCE

Explanation: The collector processes are responsible for receiving, parsing, normalizing, correlating, and monitoring events from various sources. The collector processes are phParser, phRuleMaster, and phMonitorAgent.

QUESTION 3

From where does the rule engine load the baseline data values?

A. The profile report

B. The daily database

C. The profile database

D. The memory

Correct Answer: C

Explanation: The rule engine loads the baseline data values from the profile database. The profile database contains historical data that is used for baselining calculations, such as minimum, maximum, average, standard deviation, and percentile values for various metrics.

QUESTION 4

In the event of a WAN link failure between the collector and the supervisor, by default, what is the maximum number of event files stored on the collector?

A. 30.000

B. 10.000

C. 40.000

D. 20.000

Correct Answer: B

Explanation: By default, the maximum number of event files stored on the collector in the event of a WAN link failure between the collector and the supervisor is 10.000. This value can be changed in the collector.properties file by modifying the parameter max_event_files_to_store. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 13

QUESTION 5

What happens to UEBA events when a user is off-net?

A. The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector

B. The agent will cache events locally if it cannot upload them to a FortiSIEM collector

C. The agent will upload the events to the Supervisor if it cannot upload them to a FortiSIEM collector

D. The agent will drop the events if it cannot upload them to a FortiSIEM collector

Correct Answer: B

Explanation: When a user is off-net, meaning they are not connected to a network where a FortiSIEM collector is reachable, then UEBA events will be cached locally by the agent if it cannot upload them to a FortiSIEM collector. The agent will store up to 100 MB of events in a local database file and try to upload them when it detects a network change or every five minutes.