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.leads4pass.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

Refer to the exhibit.

Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	User	Raw Event Log
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.46	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02…
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sarah	<189>date=2018-02-02…
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02…

An administrator runs an analytic search for all FortiGate SSL VPN logon failures. The results are grouped by source IP, reporting IP, and user. The administrator wants to restrict the results to only those rows where the COUNT >= 3. Which user would meet that condition?

A. Sarah

B. Jan

C. Tom

D. Admin

Correct Answer: C

Explanation: The user who would meet that condition is Tom. Tom has four rows in the results where the COUNT is greater than or equal to three, meaning he had at least three SSL VPN logon failures from the same source IP and reporting IP. The other users have either less than three rows or less than three COUNT in each row.

QUESTION 2

Which three statements about collector communication with the FortiSIEM cluster are true? (Choose three.)

A. The only communication between the collector and the supervisor is during the registration process.

B. Collectors communicate periodically with the supervisor node.

C. The supervisor periodically checks the health of the collector.

D. The supervisor does not initiate any connections to the collector node.

E. Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node.

Correct Answer: BCE

Explanation: The statements about collector communication with the FortiSIEM cluster that are true are:

Collectors communicate periodically with the supervisor node. Collectors send heartbeat messages to the supervisor every 30 seconds to report their status and configuration.

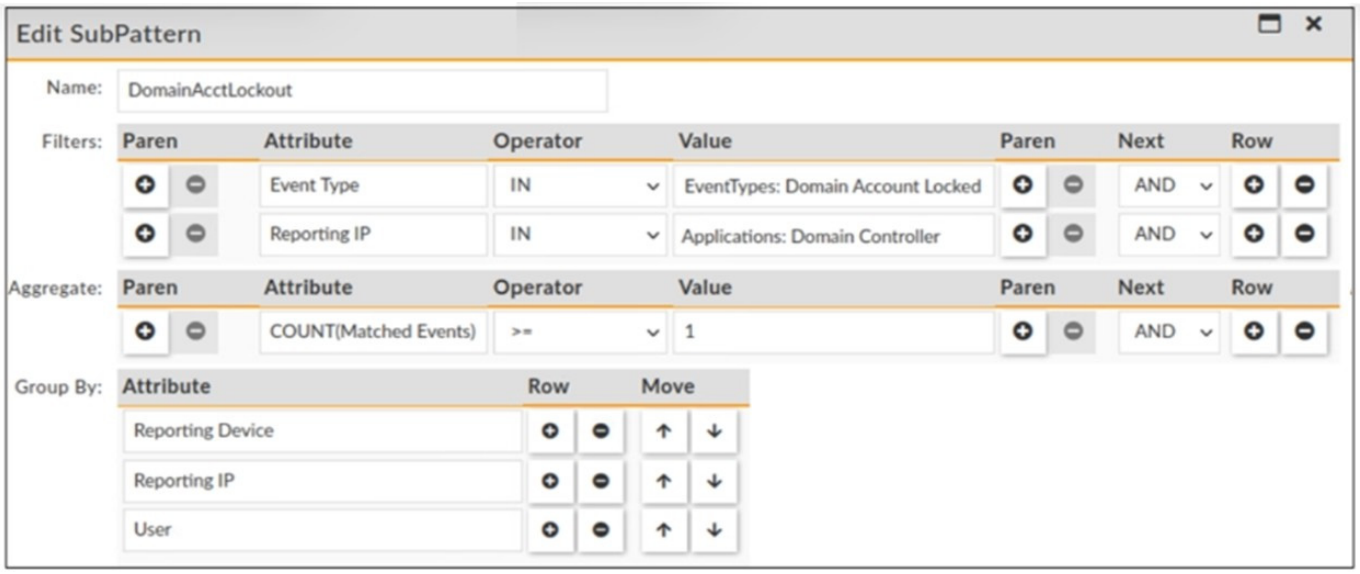
The supervisor periodically checks the health of the collector. The supervisor monitors the heartbeat messages from collectors and alerts if there is any issue with their connectivity or performance.

Collectors upload event data to any node in the worker upload list, but report their health directly to the supervisor node. Collectors use a round-robin algorithm to distribute event data among worker nodes in the worker upload list, which is

provided by the supervisor during registration. However, collectors only report their health and status to the supervisor node.

QUESTION 3

Refer to the exhibit.



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 4

What is the disadvantage of automatic remediation?

A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network.

B. It is equivalent to running an IPS in monitor-only mode -- watches but does not block.

C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.

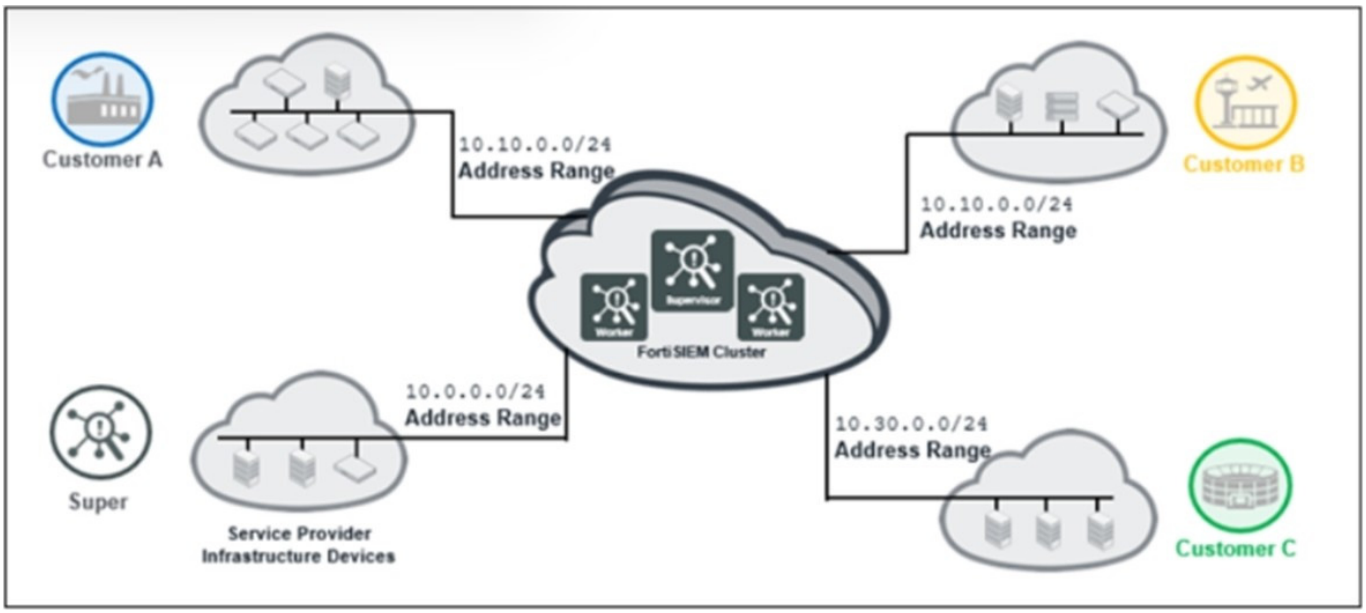
D. Threat behaviors occurring during the night could take hours to respond to.

Correct Answer: A

Explanation: The disadvantage of automatic remediation is that it can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. Automatic remediation can have unintended consequences if not carefully planned and tested. Therefore, it is recommended to use manual or semi-automatic remediation for sensitive or critical systems. References: Fortinet NSE 7 - Advanced Analytics 6.3 escription, page 15

QUESTION 5

Refer to the exhibit.



The service provider deployed FortiSIEM without a collector and added three customers on the supervisor. What mistake did the administrator make?

A. Customer A and customer B have overlapping IP addresses.

B. Collectors must be deployed on all customer premises before they are added to organizations on the supervisor.

C. The number of workers on the FortiSIEM cluster must match the number of customers added.

D. At least one collector must be deployed to collect logs from service provider infrastructure devices.

Correct Answer: A

Explanation: The mistake that the administrator made is that customer A and customer B have overlapping IP addresses. This will cause confusion and errors in event collection and correlation, as well as CMDB discovery and classification. To avoid this problem, each customer should have a unique IP address range or use NAT to translate their IP addresses.