Free Questions for C1000-162 by go4braindumps

Shared by Hodge on 28-02-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the effect of toggling the Global/Local option to Global in a Custom Rule?

Options:

A- It allows a rule to compare events & flows in real time.

B- It allows a rule to analyze the geographic location of the event source.

C- It allows rules to be tracked by the central processor for detection by any Event Processor.

D- It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Answer:

D

Question 2

Question Type: MultipleChoice

A Security Analyst has noticed that an offense has been marked inactive.

How long had the offense been open since it had last been updated with new events or flows?

Options:

A- 1 day + 30 minutes

B- 5 days + 30 minutes

C- 10 days + 30 minutes

D- 30 days + 30 minutes

Answer:

B

Question 3

Question Type: MultipleChoice

Which two high level Event Categories are used by QRadar? (Choose two.)

Options:

A- Policy

B- Direction

C- Localization

D- Justification

E- Authentication

Answer:

A, E

Question 4

Question Type: **MultipleChoice**

What can be considered a log source type?

Options:

A- ICMP

B- SNMP

C- Juniper IOP

D- Microsoft SMBtail

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which type of rule requires a saved search that must be grouped around a common parameter

Options:

A- Flow Rule

B- Event Rule

C- Common Rule

D- Anomaly Rule

Answer:

B

Question 6

Question Type: MultipleChoice

What is an effective method to fix an event that is parsed an determined to be unknown or in the wrong QReader category/

Options:

A- Create a DSM extension to extract the category from the payload

B- Create a Custom Property to extract the proper Category from the payload

C- Open the event details, select map event, and assign it to the correct category

D- Write a Custom Rule, and use Rule Response to send a new event in the proper category

Answer:

B

Question 7

Question Type: MultipleChoice

A Security Analyst was asked to search for an offense on a specific day. The requester was not sore of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.

Which fitters can the Security Analyst use to search for the information requested?

Options:

A- Offense ID, Source IP, Username

B- Magnitude, Source IP, Destination IP

C- Description, Destination IP. Host Name

D- Specific Interval, Username, Destination IP

Answer:

D