C1000-018 Q&As

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

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

https://www.geekcert.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active

B. Custom rule equals device stopped sending events

C. Log source type does not equal active

D. Log source status does not equal error

Correct Answer: A

QUESTION 2

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

Correct Answer: D

QUESTION 3

Which consideration should be given to the position of rule tests that evaluate regular expressions (Regex tests)?

A. They can only be used in Building Blocks to ensure they are evaluated as infrequently as possible.

B. They are usually the most specific. As such, they should appear first in the order.

C. They are usually the most expensive. As such, they should appear last in the order.

D. They are stateful tests. As such QRadar automatically evaluates them last.

Correct Answer: A

Reference: https://towardsdatascience.com/everything-you-need-to-know-about-regular-expressions8f622fe10b03

QUESTION 4

An analyst needs to find all events that are creating offenses that are triggered by rules that contain the word suspicious in the rule name.

Which query can the analyst use as a working sample?

A. SELECT LOGSOURCETYPE(logsourceid), “from log_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

B. SELECT LOGSOURCERULES(logsourceid), “from rule_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

C. SELECT LOGGEDOFFENSE(logsourceid), *from offense_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

D. SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-advanced-search-options

QUESTION 5

What information is included in flow details but is not in event details?

A. Log source information

B. Number of bytes and packets transferred

C. Network summary information

D. Magnitude information

Correct Answer: C

Explanation:

Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other

data, into flow records, which effectively are records of network sessions between two hosts.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=overview-qradar-events-flows