C1000-018$^{\text{Q\&As}}$

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

An analyst investigates an Offense that will need more research to outline what has occurred. The analyst marks a ‘Follow up’ flag on the Offense.

What happens to the Offense after it is tagged with a ‘Follow up’ flag?

A. Only the analyst issuing the follow up flag can now close the Offense.

B. New events or flows will not be applied to the Offense.

C. A flag icon is displayed for the Offense in the Offense view.

D. Other analysts in QRadar get an email to look at the Offense.

Correct Answer: C

Explanation:

The offense now displays the follow-up icon in the Flag column.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=actions-marking-offense-follow-up

QUESTION 2

Which are the supported protocol configurations for Check Point integration with QRadar? (Choose two.)

A. CHECKPOINT REST API

B. SYSLOG

C. JDBC

D. SFTP

E. OPSEC/LEA

Correct Answer: BE

QUESTION 3

An analyst needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter

B. List of test conditions

C. Rule actions

D. Rule responses

Correct Answer: A

QUESTION 4

An analyst needs to perform Offense management.

In QRadar SIEM, what is the significance of “Protecting” an offense?

A. Escalate the Offense to the QRadar administrator for investigation.

B. Hide the Offense in the Offense tab to prevent other analysts to see it.

C. Prevent the Offense from being automatically removed from QRadar.

D. Create an Action Incident response plan for a specific type of cyber attack.

Correct Answer: C

Explanation:

Protecting offenses:

You might have offenses that you want to retain regardless of the retention period. You can protect

offenses to prevent them from being removed from QRadar after the retention period has elapsed.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 5

An analyst is investigating a series of events that triggered an Offense. The analyst wants to get more detailed information about the IP address from the reference set.

How can the analyst accomplish this?

A. Click on Searches tab then perform an Advanced Search

B. Click on Log Activity tab then perform a Quick Search

C. Click on Searches tab then perform a Quick Search

D. Click on Log Activity tab then perform an Advanced Search

Correct Answer: A

C1000-018 PDF Dumps C1000-018 Practice Test C1000-018 Study Guide