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

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

An analyst is encountering a large number of false positive results. Legitimate internal network traffic contains valid flows and events which are making it difficult to identify true security incidents.

What can the analyst do to reduce these false positive indicators?

A. Create X-Force rules to detect false positive events.

B. Create an anomaly rule to detect false positives and suppress the event.

C. Filter the network traffic to receive only security related events.

D. Modify rules and/or Building Block to suppress false positive activity.

Correct Answer: C

QUESTION 3

An analyst wants to view information about repeated offenders and IP addresses that generate many attacks or are subject to many attacks.

What should the analyst choose from the navigation options in the Offense tab?

A. By Event Category or By Event Source

B. By Source IP or By Destination IP

C. By Log Source IP or By Event Source

D. By Event or By Flows

Correct Answer: B

Explanation:

Use the navigation options on the left to view the offenses from different perspectives. For example, select

By Source IP or By Destination IP.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 4

What is displayed in the status bar of the Log Activity tab when streaming events?

A. Average number of results that are received per second.

B. Average number of results that are received per minute.

C. Accumulated number of results that are received per second.

D. Accumulated number of results that are received per minute.

Correct Answer: A

Explanation:

Status bar

When streaming events, the status bar displays the average number of results that are received per

second.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-log-activity-tab-overview

QUESTION 5

After working with an Offense, an analyst set the Offense as hidden. What does the analyst need to do to view the Offense at a later time?

A. In the all Offenses view, at the top of the view, select “Show hidden” from the “Select an option” drop-down.

B. Search for all Offenses owned by the analyst.

C. Click Clear Filter next to the “Exclude Hidden Offenses”.

D. In the all Offenses view, select Actions, then select show hidden Offenses.

Correct Answer: C

Explanation:

To clear the filter on the offense list, click Clear Filter next to the Exclude Hidden Offenses search parameter.

Reference: https://www.ibm.com/docs/fi/qradar-on-cloud?topic=actions-showing-hidden-offenses