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

What event information within an offense would provide the analyst with a deep insight as to how it was created?

A. Event Category

B. Event QID

C. Event Payload

D. Event Magnitude

Correct Answer: D

QUESTION 2

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

QUESTION 3

An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.

How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Navigate, and then Destination Summary

B. Right-click on the destination address, More Options, then IP Owner

C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup

D. Right-click on the destination address, More Options, then Information, and then DNS Lookup

Correct Answer: A

Explanation:

Navigate > View Destination Summary Displays the offenses that are associated with the selected

destination IP address.

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

QUESTION 4

What is a valid offense naming mechanism? This information should:

A. set the naming of the associated offense(s).

B. set or replace the naming of the associated offense(s).

C. replace the naming of the associated offense(s).

D. be included in the naming of the associated offense(s).

Correct Answer: A

Explanation:

Under "Offense Naming", check "This information should

contribute to the name of the associated offense(s)".

Reference: https://www.ibm.com/support/pages/apar/IJ27086

QUESTION 5

An analyst has observed that for a particular user, authentication to an organization\\'s critical server is different than the normal access pattern.

How can the analyst verify that all the authentications initiated from the user are valid?

A. Perform a search with filter Destination IP group by Username, then validate the Username

B. Perform a search with filter Source IP group by Username, then validate the Username

C. Perform a search with filter Username group by Source IP, then validate the Destination IP

D. Perform a search with filter Username group by Source IP, then validate the Source IP

Correct Answer: B

C1000-018 VCE Dumps C1000-018 Exam Questions C1000-018 Braindumps