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.leads4pass.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 needs to review additional information about the Offense top contributors, including notes and annotations that are collected about the Offense.

Where can the analyst review this information?

A. In the top portion of the Offense Summary window

B. In the bottom portion of the Offense main view

C. In the bottom portion of the Offense Summary window

D. In the top portion of the Offense main view

Correct Answer: C

Explanation:

In the bottom portion of the Offense Summary window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using summary-information

QUESTION 2

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

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

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 5

An analyst for a particular offense needs to investigate to understand the breakdown of the offense details.

How can the analyst do this?

A. Look at the magnitude information and its breakdown.

B. Look at all the event QIDs attached to the offense.

C. View the attack path of the offense.

D. Look at the list of categories, event low level categories and the events attached.

Correct Answer: A