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 use case type is appropriate for VPN log sources? (Choose two.)

A. Advanced Persistent Threat (APT)

B. Insider Threat

C. Critical Data Protection

D. Securing the Cloud

Correct Answer: AB

Reference: https://www.ibm.com/docs/en/dsm?topic=management-threat-use-cases-by-log-source-type

QUESTION 2

What does the Assets tab provide?

A unified view of the information that is known about:

A. network devices.

B. triggered Offenses.

C. log sources.

D. events and flows.

Correct Answer: D

Reference: https://www.ibm.com/support/pages/identity-and-how-log-source-events-update-assets-qradarsiem

QUESTION 3

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 4

When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?

A. When the source is [local or remote]

B. When the destination is [local or remote]

C. When the event(s) were detected by one or more of [these log sources]

D. When an event matches all of the following [Rules or Building Blocks]

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