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

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 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 observed a port scan attack on an internal network asset from a remote network. Which filter would be useful to determine the compromised host?

A. Any IP

B. Destination IP [Indexed]

C. Source or Destination IP

D. Source IP [Indexed]

Correct Answer: A

QUESTION 4

An analyst needs to find events coming from unparsed log sources in the Log Activity tab. What is the log source type of unparsed events?

A. SIM Generic

B. SIM Unparsed

C. SIM Error

D. SIM Unknown

Correct Answer: A

Explanation:

SIM Generic log source or by using the Event is Unparsed filter.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

QUESTION 5

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