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 investigate why an Offense was created. How can the analyst investigate?

A. Review the Offense summary to investigate the flow and event details.

B. Review the X-Force rules to investigate the Offense flow and event details.

C. Review pages of the Asset tab to investigate Offense details.

D. Review the Vulnerability Assessment tab to investigate Offense details.

Correct Answer: A

QUESTION 2

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

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 aims to improve the detection capabilities on all the Offense rules. QRadar SIEM has a tool that allows the analyst to update all the Building Blocks related to Host and Port Definition in a single page.

How is this accomplished?

A. Admin –andgt; Reference Set management

B. Assets –andgt; Asset Profiles

C. Assets –andgt; Server Discovery

D. Admin –andgt; Asset Profile Configuration

Correct Answer: C

QUESTION 5

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