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.pass4itsure.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

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

Correct Answer: D

QUESTION 2

An analyst is encountering a large number of false positive results. Legitimate internal network traffic contains valid flows and events which are making it difficult to identify true security incidents.

What can the analyst do to reduce these false positive indicators?

A. Create X-Force rules to detect false positive events.

B. Create an anomaly rule to detect false positives and suppress the event.

C. Filter the network traffic to receive only security related events.

D. Modify rules and/or Building Block to suppress false positive activity.

Correct Answer: C

QUESTION 3

An analyst needs to perform Offense management.

In QRadar SIEM, what is the significance of “Protecting” an offense?

A. Escalate the Offense to the QRadar administrator for investigation.

B. Hide the Offense in the Offense tab to prevent other analysts to see it.

C. Prevent the Offense from being automatically removed from QRadar.

D. Create an Action Incident response plan for a specific type of cyber attack.

Correct Answer: C

Explanation:

Protecting offenses:

You might have offenses that you want to retain regardless of the retention period. You can protect offenses to prevent them from being removed from QRadar after the retention period has elapsed.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 4

What is the intent of the magnitude of an offense?

A. It measures the age of the event attached to the offense.

B. It measures the age of the offense.

C. It measures the importance of the offense.

D. It measures the importance of the event attached to the offense.

Correct Answer: B

Explanation:

The age of the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization

QUESTION 5

An analyst needs to create a new custom dashboard to view dashboard items that meet a particular requirement.

What are the main steps in the process?

A. Select New Dashboard and enter unique name, description, add items and save.

B. Select New Dashboard and copy name, add description, items and save.

C. Request the administrator to create the custom dashboard with required items.

D. Locate existing dashboard and modify to include indexed items required and save.

Correct Answer: C

Explanation:

To create or edit your dashboards, log in as an administrator, click the Dashboards tab, and then click the gear icon. In edit mode, you can create new dashboards, add and remove widgets, edit display values in existing widgets, and reorder tabs.

Reference: https://documentation.solarwinds.com/en/success_center/tm/content/threatmonitor/tmeditdashboards.htm