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

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 2

An analyst wants to view information about repeated offenders and IP addresses that generate many attacks or are subject to many attacks.

What should the analyst choose from the navigation options in the Offense tab?

A. By Event Category or By Event Source

B. By Source IP or By Destination IP

C. By Log Source IP or By Event Source

D. By Event or By Flows

Correct Answer: B

Explanation:

Use the navigation options on the left to view the offenses from different perspectives. For example, select

By Source IP or By Destination IP.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 3

An analyst has to perform an export of events within a timeframe, but not all the columns are present in the log view for the time period the analyst has selected. The analyst only needs specific columns exported for an external analysis.

How can the analyst accomplish this task?

A. Edit the search and select the extra columns, then export the result with Action/Export to XML/Full Export. This export is only supported in XML.

B. Edit the search and select the extra columns, then export the result with Action/Export to XML/Visible Columns. This export is only supported in XML.

C. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Full Export.

D. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Visible Columns.

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-exporting-events

QUESTION 4

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

QUESTION 5

An analyst needs to map a geographic location on all the internal IP addresses.

Which option defines the functions where the analyst can-setup a geographic location of the network object in Network Hierarchy?

A. GPS location and Map

B. Group and IP address

C. Log Activity and Network Activity

D. Longitude and Latitude

Correct Answer: B

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy