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.passapply.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

Why would an analyst update host definition building blocks in QRadar?

A. To reduce false positives.

B. To narrow a search.

C. To stop receiving events from the host.

D. To close an Offense

Correct Answer: D

Explanation:

Building blocks to reduce the number of offenses that are generated by high volume traffic servers.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=phase-qradar-building-blocks

QUESTION 2

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

QUESTION 3

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

QUESTION 4

An analyst is investigating a user\\'s activities and sees that they have repeatedly executed an action which triggers a rule that emails the SOC team and creates an Offense, indexed on Username.

The SOC team complained that they have received 15 emails in the space of 10 minutes, but the analyst can only see one Offense in the Offenses tab.

How is this explained?

A. There is a Rule Limiter on the Rule Action which creates the Offense, this should also be applied to the Rule Responses.

B. This is expected behavior, the offense will contain the information about all 15 events.

C. An Offense rule has been configured to send multiple emails upon Offense creation.

D. The Custom Rules Engine (CRE) has fallen behind and the additional Offenses will be created shortly.

Correct Answer: C

QUESTION 5

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

Latest C1000-018 Dumps C1000-018 Study Guide C1000-018 Braindumps