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.pass2lead.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 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 2

When an Offense is triggered, it only shows the events that triggered the Offense. The analyst wants to investigate further to see more events around the incident, not only those that triggered the Offense. The analyst clicks on the event count and sees the events belonging to the Offense.

How can the analyst proceed to see a more detailed picture of what occurred?

A. Right-click on the source IP, and choose More Options, then Information, and then Search Events.

B. Right-click on the destination IP, and choose More Options, then Raw Events.

C. Right-click on the source IP, and choose View in DSM Editor.

D. Right-click and filter on the Destination IP.

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=events-filtering

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

When an analyst sees the system notification “The appliance exceeded the EPS or FPM allocation within the last hour”, how does the analyst resolve this issue? (Choose two.)

A. Delete the volume of events and flows received in the last hour.

B. Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance.

C. Tune the system to reduce the volume of events and flows that enter the event pipeline.

D. Adjust the resource pool allocations to increase the EPS and FPM capacity for the appliance.

E. Tune the system to reduce the time window from 60 minutes to 30 minutes.

Correct Answer: BC

Explanation:

User response

Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance.

Tune the system to reduce the volume of events and flows that enter the event pipeline.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=appliances-maximum-events-flows-reached

QUESTION 5

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