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

Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active

B. Custom rule equals device stopped sending events

C. Log source type does not equal active

D. Log source status does not equal error

Correct Answer: A

QUESTION 2

An analyst needs to find events coming from unparsed log sources in the Log Activity tab. What is the log source type of unparsed events?

A. SIM Generic

B. SIM Unparsed

C. SIM Error

D. SIM Unknown

Correct Answer: A

Explanation:

SIM Generic log source or by using the Event is Unparsed filter.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

QUESTION 3

How does an analyst view the base64 encoded string of an event\\'s raw payload that contains unprintable characters?

A. Copy the raw payload and use an external tool to view base64 data

B. Right click on the event –andgt; view base64 data

C. Log Activity –andgt; Under Payload Information, click base64 tab

D. Admin –andgt; Under Payload Information, click base64 tab

Correct Answer: B

QUESTION 4

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 5

How many normalized timestamp field(s) does an event contain?

A. 2

B. 3

C. 4

D. 1

Correct Answer: B

Explanation:

There are 3 timestamp fields on events in Qradar.

Reference: https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-differenttime-stamps-for-qradar-events?language=en_US