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

Which use case type is appropriate for VPN log sources? (Choose two.)

A. Advanced Persistent Threat (APT)

B. Insider Threat

C. Critical Data Protection

D. Securing the Cloud

Correct Answer: AB

Reference: https://www.ibm.com/docs/en/dsm?topic=management-threat-use-cases-by-log-source-type

QUESTION 2

What is the procedure to re-open a closed Offense?

A. A closed Offense cannot be re-opened.

B. Wait for new events/flows that will re-open the closed Offense.

C. Activate the Offense in the action/re-open drop down menu of the Offense tab.

D. Activate the Offense in action/re-open drop down menu in the Admin tab.

Correct Answer: A

Explanation:

Not possible to reopen a closed offense.

Reference: https://www.ibm.com/support/pages/qradar-closed-offense-information

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 auditor has requested a report for all Offenses that have happened in the past month. This report generates at the end of every month but the auditor needs to have it for a meeting that is in the middle of the month.

What will happen to the scheduled report if the analyst manually generates this report?

A. The scheduled report needs to be reconfigured.

B. The analyst needs to delete the scheduled report and create a new one.

C. The report will get duplicated so the analyst can then run one manually.

D. The report still generates on the schedule initially configured.

Correct Answer: B

Explanation: Shared schedules must be deleted manually using the Schedules page in the web portal or the Shared Schedules folder in Management Studio. If you delete a shared schedule that is in use, all references to it are replaced with report-specific schedules. If you delete a shared schedule that is used by multiple reports and subscriptions, the report server will create individual schedules for each report and subscription that previously used the shared schedule. Each new individual schedule will contain the date, time, and recurrence pattern that was specified in the shared schedule. Note that Reporting Services does not provide central management of individual schedules. If you delete a shared schedule, you will now have to maintain the schedule information for each individual item.

Reference: https://docs.microsoft.com/en-us/sql/reporting-services/subscriptions/create-modify-anddelete-schedules?view=sql-server-ver15

QUESTION 5

How can analyst verify if any host in the deployment is vulnerable to CVE ID: CVE-2010-000?

A. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: 2010-000

B. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: $CVE-2010000

C. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: $2010-000

D. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: CVE-2010000

Correct Answer: A

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=ap-searching-asset-profiles-from-assetpage-assets-tab