



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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

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 2

What is the purpose of Anomaly detection rules?

- A. They inspect other QRadar rules.
- B. They detect if QRadar is operating at peak performance and error free.
- C. They detect unusual traffic patterns in the network from the results of saved flow and events.
- D. They run past events and flows through the Custom Rules Engine (CRE) to identify threats or security incidents that already occurred.

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/topics/concept/conceptjsa-user-anomaly-detection-rules.html#:~:text=Anomaly%20detection%20rules%20test%20the,patterns%20occur%20in%20your%20network.andtext=Typically%20the%20search%20needs%20to,%2C%20thresholds%2C%20or%20behavior%20changes

QUESTION 3



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 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

What could be a possible reason that events are routed directly to storage by the custom rule engine (CRE)?

- A. System is under high load
- B. A rule is processing 20,000 EPS
- C. Event normalization issue
- D. Event Parsing issue

Correct Answer: A



VCE & PDF

GeekCert.com

<https://www.geekcert.com/c1000-018.html>

2024 Latest geekcert C1000-018 PDF and VCE dumps Download

[C1000-018 VCE Dumps](#)

[C1000-018 Practice Test](#)

[C1000-018 Braindumps](#)