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

QUESTION 1

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 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 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 4

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 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