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

An analyst needs to review additional information about the Offense top contributors, including notes and annotations that are collected about the Offense.

Where can the analyst review this information?

A. In the top portion of the Offense Summary window

B. In the bottom portion of the Offense main view

C. In the bottom portion of the Offense Summary window

D. In the top portion of the Offense main view

Correct Answer: C

Explanation:

In the bottom portion of the Offense Summary window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using summary-information

QUESTION 2

What is the reason for this system notification?

A. Deny ntpdate communication on port 423.

B. Deny ntpdate communication on port 223.

C. Deny ntpdate communication on port 323.

D. Deny ntpdate communication on port 123.

Correct Answer: D

Explanation:

38750129 - Time synchronization to primary or Console has failed.

The managed host cannot synchronize with the console or the secondary HA appliance cannotsynchronize with the primary appliance.

Administrators must allow ntpdatecommunication on port 123.

Reference: https://www.coursehero.com/file/p35nlom9/Process-exceeds-allowed-run-time-38750122Process-takes-too-long-to-execute-The/

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 information is displayed in the default “Log Activity” page? (Choose two.)

A. QID

B. Protocol

C. Qmap

D. Log Source

E. Event Name

Correct Answer: DE

QUESTION 5

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