C1000-018$^{\text{Q\&As}}$

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

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

An analyst needs to investigate why an Offense was created. How can the analyst investigate?

A. Review the Offense summary to investigate the flow and event details.

B. Review the X-Force rules to investigate the Offense flow and event details.

C. Review pages of the Asset tab to investigate Offense details.

D. Review the Vulnerability Assessment tab to investigate Offense details.

Correct Answer: A

QUESTION 3

An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.

How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Navigate, and then Destination Summary

B. Right-click on the destination address, More Options, then IP Owner

C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup

D. Right-click on the destination address, More Options, then Information, and then DNS Lookup

Correct Answer: A

Explanation:

Navigate > View Destination Summary Displays the offenses that are associated with the selected

destination IP address.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 4

An analyst needs to map a geographic location on all the internal IP addresses.

Which option defines the functions where the analyst can-setup a geographic location of the network object in Network Hierarchy?

A. GPS location and Map

B. Group and IP address

C. Log Activity and Network Activity

D. Longitude and Latitude

Correct Answer: B

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy

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

Latest C1000-018 Dumps   C1000-018 PDF Dumps   C1000-018 Study Guide