C2150-612^{Q&As}

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/c2150-612.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

Which three data sources contribute to the creation and updates of assets? (Choose three.)

A. Log Sources

B. Flow Sources

C. Reference set imports

D. Vulnerability scanners

E. QRadar log source auto-updates

F. X-Force reference list integration

Correct Answer: ABC

QUESTION 2

What is the purpose of coalescing?

A. To reduce the number of events which count against EPS licenses

B. To reduce the amount of data received by QRadar event collectors

C. To reduce the amount of data going through the pipeline and stored onto disk

D. To reduce the number of offenses generated by QRadar as part of the tuning process

Correct Answer: A

Reference: https://developer.ibm.com/answers/questions/438469/out-eps-licence-is-10k-im-attaching-twoscreenshot/

QUESTION 3

Which QRadar component is designed to help increase the search speed in a deployment by allowing more data to remain uncompressed?

A. QRadar Data Node

B. QRadar Flow Processor

C. QRadar Event Collector

D. Qradar Event Processor

Correct Answer: A

QUESTION 4

A Security Analyst was asked to search for an offense on a specific day. The requester was not sure of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.

Which filters can the Security Analyst use to search for the information requested?

A. Offense ID, Source IP, Username

B. Magnitude, Source IP, Destination IP

C. Description, Destination IP, Host Name

D. Specific Interval, Username, Destination IP

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/
t_qradar_search_my_all_off_pages.html

QUESTION 5

What is an example of the use of a flow data that provides more information than an event data?

A. Represents a single event on the network

B. Automatically identifies and better classifies new assets found on a network

C. Performs near real-time comparisons of application data with logs sent from security devices

D. Represents network activity by normalizing IP addresses ports, byte and packet counts, as well as other details

Correct Answer: D

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21682445

C2150-612 Practice Test   C2150-612 Study Guide   C2150-612 Braindumps