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.passapply.com/c2150-612.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

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 2

Which three pages can be accessed from the Navigation menu on the Offenses tab? (Choose three.)

A. Rules

B. By Category

C. My Offenses

D. By Event Name

E. Create Offense

F. Closed Offenses

Correct Answer: ABC

QUESTION 3

What are two benefits of using a netflow flow source? (Choose two.)

A. They can include data payload.

B. They can include router interface information.

C. They can include usernames involved in the flow.

D. They can include ASN numbers of remote addresses.

E. They can include authentication methods used to access the network.

Correct Answer: BD

Reference: https://developer.ibm.com/qradar/2018/01/09/qradar-flow-faq/

QUESTION 4

Given the following window:

What are the steps to get this window within an offense?

A. Right click on the IP > Information > DNS Lookup

B. Right click on the IP > Information > Reverse DNS

C. Right click on the IP > Information > WHOIS Lookup

D. Right click on the IP > Information > Asset Profile

Correct Answer: A

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21690480

QUESTION 5

Which QRadar add-on component can generate a list of the unencrypted protocols that can communicate from a DMZ to an internal network?

A. QRadar Risk Manager

B. QRadar Flow Collector

C. QRadar Incident Forensics

D. QRadar Vulnerability Manager

Correct Answer: A

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