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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which three could be considered a log source type? (Choose three.)

A. Red Hat Network

B. IBM ISS Proventia

C. QRadar Event Processor

D. Check Point Firewall-1

E. Sourcefire Flow Injector

F. McAfee ePolicy Orchestrator

Correct Answer: BDF

QUESTION 2

When using the right click event filtering functionality on a Source IP, one can filter by "Source IP is not [*]". Which two other filters can be shown using the right click event filtering functionality? (Choose two.)

A. Filter on DNS entry [*]

B. Filter on Source IP is [*]

C. Filter on Time and Date is [*]

D. Filter on Source or Destination IP is [*]

E. Filter on Source or Destination IP is not [*]

Correct Answer: BD

QUESTION 3

What is the difference between TCP and UDP?

A. They use different port number ranges

B. UDP is connectionless, whereas TCP is connection based

C. TCP is connectionless, whereas UDP is connection based

D. TCP runs on the application layer and UDP uses the Transport layer

Correct Answer: B

QUESTION 4

What can be considered a log source type?

A. ICMP

B. SNMP

C. Juniper IDP

D. Microsoft SMBtail

Correct Answer: C

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/ c_LogSourceGuide_ExtDocs_typeIDs.html

QUESTION 5

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