



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

Which capability is common to both Rules and Building Blocks?

- A. Rules and Building Blocks both set the Magnitude of an Event.
- B. Rules and Building Blocks both have the same selection of sets.
- C. Rules and Building Blocks can both be Enabled/Disabled through the GUI.
- D. Rules and Building Blocks both have Actions; Building Blocks do not have Responses.

Correct Answer: B

QUESTION 2

When reviewing Network Activity, a flow shows a communication between a local server on port 443, and a random, remote port. The bytes from the local destination host are 2 GB, and the bytes from the remote, source host address are 40KB.

What is the flow bias of this session?

- A. Other
- B. Mostly in
- C. Near-same
- D. Mostly out

Correct Answer: D

QUESTION 3

Which column shows information as icons on the Reports tab?

- A. Owner
- B. Formats
- C. Schedule
- D. Report Name

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_qradar_view_gen_rpt.html



QUESTION 4

What is a capability of the Network Hierarchy in QRadar?

- A. Determining and identifying local and remote hosts
- B. Capability to move hosts from local to remote network segments
- C. Viewing real-time PCAP traffic between host groups to isolate malware
- D. Controlling DHCP pools for segments groups (i.e. marketing, DMZ, VoIP)

Correct Answer: A

Reference: http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_gs_ntwrk_hrchy.html

QUESTION 5

Which three options are available on the New Search on the My Offenses and All Offenses pages? (Choose three.)

- A. Notes
- B. Source IP
- C. Magnitude
- D. Attack Name
- E. Malware Name
- F. Specific Interval

Correct Answer: BDF

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/t_qradar_search_my_all_off_pages.html

[Latest C2150-612 Dumps](#)

[C2150-612 Study Guide](#)

[C2150-612 Brindumps](#)