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.leads4pass.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

Where can a user add a note to an offense in the user interface?

A. Dashboard and Offenses Tab

B. Offenses Tab and Offense Detail Window

C. Offenses Detail Window, Dashboard, and Admin Tab

D. Dashboard, Offenses Tab, and Offense Detail Window

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 34

QUESTION 2

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 3

What is indicated by an event on an existing log in QRadar that has a Low Level Category of "Unknown"?

A. That event could not be parsed

B. That event arrived out of order from the original device

C. That event was from a device that is not supported by QRadar

D. That the event was parsed, but not mapped to an existing QRadar category

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.dsm.doc/

c_DSM_guide_UniversalLEEF_eventmap.html#c_dsm_guide_universalleef_eventmap

QUESTION 4

What is the definition of asset profile on QRadar?

A. It is any network endpoint that sends or receives data across a network infrastructure.

B. It is all the information that IBM Security QRadar SIEM collected over time about a specific asset.

C. It is the information servers and hosts in a network provide to assist users when resolving security issues.

D. It is an application used to configure and distribute settings to devices and computers in an organization, school, or business.

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/ c_qradar_ug_asset_prof_about.html

QUESTION 5

Which list is only Rule Actions?

A. Modify Credibility; Send SNMP trap; Drop the Detected Event; Dispatch New Event.

B. Modify Credibility; Annotate Event; Send to Forwarding Destinations; Dispatch New Event.

C. Modify Severity; Annotate Event; Drop the Detected Event; Ensure the detected event is part of an offense.

D. Modify Severity; Send to Forwarding Destinations; Drop the Detected Event; Ensure the detected event is part of an offense.

Correct Answer: A

Reference: http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/ t_qradar_create_cust_rul.html

C2150-612 VCE Dumps C2150-612 Study Guide C2150-612 Exam Questions