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.pass2lead.com/c2150-612.html

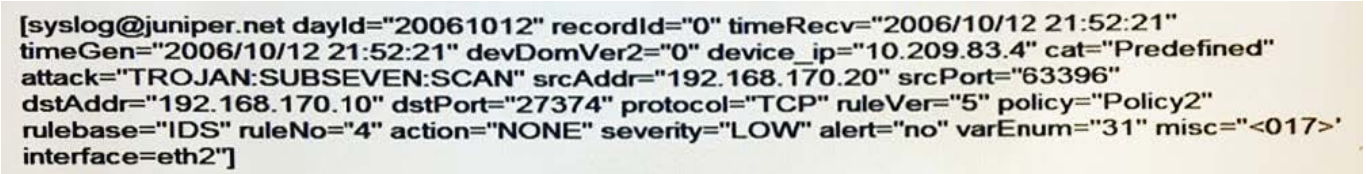
100% Passing Guarantee
100% Money Back Assurance

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

Given the following supplied payload of a supported Juniper device:



Which QRadar normalized fields will be populated?

A. Policy, Attack, Source IP, Username

B. Source IP, Destination IP, Destination Port, Protocol

C. Source Port, Destination Port, Domain, Source Bytes

D. Source IP, Destination IP, Destination Port, Destination Bytes

Correct Answer: B

QUESTION 2

Which QRadar add-on component can quickly retrace the step-by-step actions of an attacker?

A. QRadar Risk Manager

B. QRadar Flow Connector

C. QRadar Incident Forensics

D. QRadar Vulnerability Manager

Correct Answer: C

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_siem_deployment.pdf (30)

QUESTION 3

Which set of information is provided on the asset profile page on the assets tab in addition to ID?

A. Asset Name, MAC Address, Magnitude, Last user

B. IP Address, Asset Name, Vulnerabilities, Services

C. IP Address, Operating System, MAC Address, Services

D. Vulnerabilities, Operative System, Asset Name, Magnitude

Correct Answer: C

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_qradar_ug_asset_sum.html

QUESTION 4

While on the Offense Summary page, a specific Category of Events associated with the Offense can be

investigated.

Where should a Security Analyst click to view them?

A. Click on Events, then filter on Flows

B. Highlight the Category and click the Events icon

C. Scroll down to Categories and view Top 10 Source IPs

D. Right Click on Categories and choose Filter on Network Activity

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 42

QUESTION 5

How does a Device Support Module (DSM) function?

A. A DSM is a configuration file that combines received events from multiple log sources and displays them as offenses in QRadar.

B. A DSM is a background service running on the QRadar appliance that reaches out to devices deployed in a network for configuration data.

C. A DSM is a configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

D. A DSM is an installed appliance that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

Correct Answer: C

Reference: ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/ b_qradar_tuning_guide.pdf (32)