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

QUESTION 1

How does flow data contribute to the Asset Database?

A. Correlated Flows are used to populate the Asset Database.

B. It provides administrators visibility on how systems are communicating on the network.

C. Flows are used to enrich the Asset Database except for the assets that were discovered by scanners.

D. It delivers vulnerability and ports information collected from scanners responsible for evaluating network assets.

Correct Answer: C

QUESTION 2

What is the effect of toggling the Global/Local option to Global in a Custom Rule?

A. It allows a rule to compare events and flows in real time.

B. It allows a rule to analyze the geographic location of the event source.

C. It allows rules to be tracked by the central processor for detection by any Event Processor.

D. It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Correct Answer: C

QUESTION 3

What are the various timestamps related to a flow?

A. First Packet Time, Storage Time, Log Source Time

B. First Packet Time, Storage Time, Last Packet Time

C. First Packet Time, Log Source Time, Last Packet Time

D. First Packet Time, Storage Time, Log Source Time, End Time

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 101

QUESTION 4

Which kind of information do log sources provide?

A. User login actions

B. Operating system updates

C. Flows generated by users

D. Router configuration exports.

Correct Answer: A

QUESTION 5

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 6

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 7

Which three things can be found under the Information menu when right clicking an IP address? (Choose three.)

A. Asset Profile

B. DNS Lookup

C. Hide Offense

D. WHOIS Lookup

E. Annotation View

F. Username Lookup

Correct Answer: ABD

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

QUESTION 8

What is one of the major differences between event and network data (flow)?

A. Flows can replay a whole packet by packet sessions, while events are just a snapshot.

B. A flow can have a life span that can last seconds, minutes, hours or days, while events are only a snapshot.

C. An event can have a life span that can last seconds, minutes, hours or days, while flows can only span 1 minute.

D. Events represent network activity by normalizing IP addresses, ports, byte and packet counts, while flows do not.

Correct Answer: B

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21682445

QUESTION 9

What is a primary benefit of building blocks?

A. They can notify users of strange behavior.

B. They allow the execution of its test within all rules.

C. They generate new events into the pipeline before rules fire.

D. They allow for report result to be used in custom rules tests.

Correct Answer: C

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=77777777-0000-00000000-000014969067

QUESTION 10

Where are events related to a specific offense found?

A. Offenses Tab and Event List window

B. Dashboard and List of Events window

C. Offense Summary Page and List of Events window

D. Under Log Activity, search for Events associated with an Offense

Correct Answer: A

QUESTION 11

What is a Device Support Module (DSM) function within QRadar?

A. Unites data received from logs

B. Provides Vendor specific configuration information

C. Scans log information based on a set of rules to output offenses

D. Parses event information for SIEM products received from external sources

Correct Answer: D

QUESTION 12

Which QRadar component stores and forwards events from local and remote log sources?

A. QRadar Data Node

B. QRadar Event Collector

C. QRadar Event Processor

D. QRadar Distributes Console

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/shc_qradar_comps.html

QUESTION 13

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 14

What is a common purpose for looking at flow data?

A. To see which users logged into a remote system

B. To see which users were accessing report data in QRadar

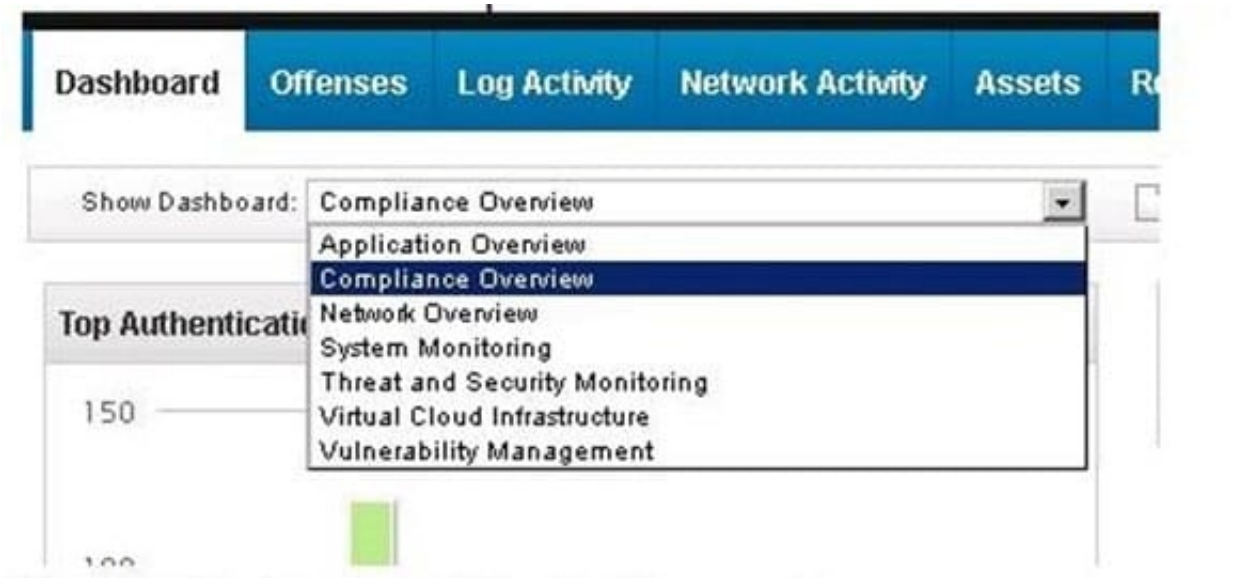
C. To see application versions installed on a network endpoint

D. To see how much information was sent from a desktop to a remote website

Correct Answer: D

QUESTION 15

Given these default options for dashboards on the QRadar Dashboard Tab: Which will display a list of offenses?



A. Network Overview

B. System Monitoring

C. Vulnerability Management

D. Threat and Security Monitoring

Correct Answer: D

C2150-612 PDF Dumps C2150-612 Exam Questions C2150-612 Braindumps