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

Which three optional items can be added to the Default and Custom Dashboards without requiring additional licensing? (Choose three.)

A. Offenses

B. Log Activity

C. Risk change

D. Flow Search

E. Risk Monitoring

F. Asset Management

Correct Answer: ABF

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 2

Which browser is officially supported for QRadar?

A. Safari version 9.0.3

B. Chromium version 33

C. 32-bit Internet Explorer 9

D. Firefox version 38.0 ESR

Correct Answer: D

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

QUESTION 3

Which Anomaly Detection Rule type can test events or flows for volume changes that occur in regular patterns to detect outliers?

A. Outlier Rule

B. Anomaly Rule

C. Threshold Rule

D. Behavioral Rule

Correct Answer: D

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

QUESTION 4

Which three log sources are supported by QRadar? (Choose three.)

A. Log files via SFTP

B. Barracuda Web Filter

C. TLS multiline Syslog

D. Oracle Database Listener

E. Sourcefire Defense Center

F. Java Database Connectivity (JDBC)

Correct Answer: DEF

QUESTION 5

What is accessible from the Offenses Tab but is not used to present a sorted list of offenses?

A. Rules

B. Category

C. Source IP

D. Destination IP

Correct Answer: A

QUESTION 6

What are the two available formats for exporting event and flow data for external analysis? (Choose two.)

A. XML

B. DOC

C. PDF

D. CSV

E. HTML

Correct Answer: AD

QUESTION 7

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 8

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 9

What is the difference between an offense and a triggered rule?

A. Offenses are created every time a rule\\'s tests are satisfied, but a rule may only trigger if the response limiter allows.

B. The first time a rule triggers, it will create an offense, after than to new offense will be created for the same index type.

C. A rule will always trigger if its tests are satisfied, but an offense may only be created if the event magnitude is greater than 6.

D. An offense may be created or updated by a triggered rule, but a rule will always trigger when the tests are satisfied.

Correct Answer: C

QUESTION 10

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 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

In a distributed QRadar deployment with multiple Event Collectors, from where can syslog and JDBC log sources collected?

A. Syslog log sources and JDBC log sources may be collected by any Event Collector.

B. One Event Collector must collect ALL syslog events and another Event Collector must collect ALL JDBC events.

C. Syslog log sources and JDBC log sources are always collected by the collector assigned in the log source definition.

D. Syslog log sources may be collected by any Event Collector, but JDBC log sources will always be collected by the collector assigned in the log source definition.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_siem_deployment.pdf (12)

QUESTION 13

What is a difference between Rule Actions and Rule Responses?

A. Rule Actions are executed when the Rule is Disabled; Rule Responses require the Rule to be Enabled.

B. Rule Actions are only available for Event and Flow Rules; Rule Responses are available for all Rules.

C. Rule Actions only directly affect the SIEM internals; Rule Responses may send information to external systems.

D. Rule Responses are always processed; Rule Actions may be throttled to ensure they are not executed too frequently.

Correct Answer: C

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=bf259e09-ef91-46b89c1a-08ea47f11a16andps=100

QUESTION 14

What is the largest differentiator between a flow and event?

A. Events occur at a moment in time while flows have a duration.

B. Events can be forwarded to another destination, but flows cannot.

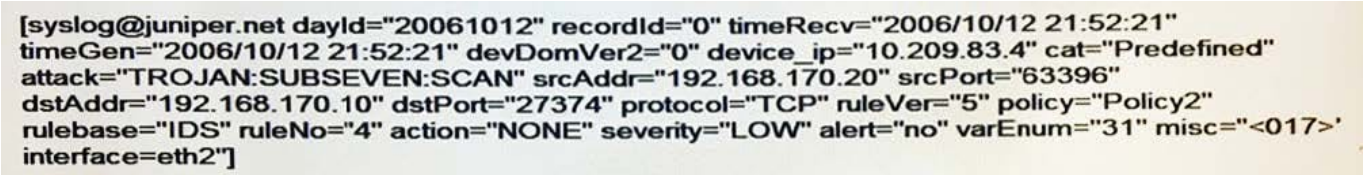
C. Events allow for the creation of custom properties, but flows cannot.

D. Flows only contribute to local correlated rules, while events are global.

Correct Answer: A

QUESTION 15

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