100% Money Back Guarantee

Vendor:IBM

Exam Code:C2150-612

Exam Name:IBM Security QRadar SIEM V7.2.6 Associate Analyst

Version: Demo

QUESTION 1

Which type of tests are recommended to be placed first in a rule to increase efficiency?

A. Custom property tests

B. Normalized property tests

C. Reference set lookup tests

D. Payload contains regex tests

Correct Answer: B

QUESTION 2

What is the correct procedure to both assign and add a note to an offense from the Graphical User Interface (GUI)?

A. Both tasks must be done independently and can only be done on the Offenses Tab.

B. With the new release of 7.2.6 this can now be done in one step from the Offenses Tab only.

C. Both tasks must be done independently but can be completed from both the Offenses Tab and the Offense Summary Page.

D. With the new release 7.2.6 this can be done in one step, both the Offenses Tab and the Offense Summary Page.

Correct Answer: B

QUESTION 3

Which Anomaly Detection Rule type is designed to test event and flow traffic for changes in short term events when compared against a longer time frame?

A. Outlier Rule

B. Anomaly Rule

C. Threshold Rule

D. Behavioral Rule

Correct Answer: B

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 advantage of a report helps distinguish it from a search?

A. Scheduling is available.

B. It can be added as a dashboard item.

C. It can be labeled for later use.

D. A report can be assigned to specific users.

Correct Answer: A

QUESTION 5

When QRadar processes an event it extracts normalized properties and custom properties.

Which list includes only Normalized properties?

A. Start time, Source IP, Username, Unix Filename

B. Start time, Username, Unix Filename, RACF Profile

C. Start time, Low Level Category, Source IP, Username

D. Low Level Category, Source IP, Username, RACF Profile

Correct Answer: C

QUESTION 6

Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC

B. McAfee ePolicy Orchestrator via JDBC

C. McAfee ePolicy Orchestrator via SNMP

D. Solaris Basic Security Mode (BSM) via Log File Protocol

Correct Answer: C

QUESTION 7

Which two are top level options when right clicking on an IP Address within the Offense Summary page? (Choose two.)

A. WHOIS

B. Navigate

C. DNS Lookup

D. Information

E. Asset Summary Page

Correct Answer: BD

QUESTION 8

Which filter in the Log and Network Activity tabs is supported by both flows and events?

A. Source Payload Contains is [Pattern]

B. Application [Indexed] matches [Application]

C. Source ID [Indexed] equals any of [IP Address]

D. Username [Indexed] equals any of [Username]

Correct Answer: B

QUESTION 9

Which saved searches can be included on the Dashboard?

A. Event and Flow saved searches

B. Asset and Network saved searches

C. User and Vulnerability saved searches

D. Network Activity and Risk saved searches

Correct Answer: A

QUESTION 10

Which QRadar component provides the user interface that delivers real-time flow views?

A. QRadar Viewer

B. QRadar Console

C. QRadar Flow Collector

D. QRadar Flow Processor

Correct Answer: B

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

QUESTION 11

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 12

Which QRadar component is designed to help increase the search speed in a deployment by allowing more data to remain uncompressed?

A. QRadar Data Node

B. QRadar Flow Processor

C. QRadar Event Collector

D. Qradar Event Processor

Correct Answer: A