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.pass4itsure.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

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

QUESTION 2

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 3

Which key elements does the Report Wizard use to help create a report?

A. Layout, Container, Content

B. Container, Orientation, Layout

C. Report Classification, Time, Date

D. Pagination Option, Orientation, Date

Correct Answer: A

Reference:

IBM Security QRadar SIEM Users Guide. Page: 201

QUESTION 4

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 5

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 6

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 7

What is a main function of a Cisco Adaptive Security Appliance (ASA)?

A. A Proxy

B. A Switch

C. A Firewall

D. An Authentication device

Correct Answer: C

QUESTION 8

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 9

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 10

A Security Analyst, looking at a Log Activity search result, wants to limit the results to one Log Source.

Which right-click method would be the fastest way for the Security Analyst to ensure this?

A. Right click on a Log Source name, then select Filter on Log Source is

B. Right click on a Source IP Address, then select Filter on Log Source is

C. Right click on the Log Source Type name, then select Filter on Log Source Group is

D. Right click on the Log Source Group name, then select Filter on Log Source Group is

Correct Answer: A

QUESTION 11

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 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

Which two actions can be performed on the Offense tab? (Choose two.)

A. Adding notes

B. Deleting notes

C. Hiding offenses

D. Deleting offenses

E. Creating offenses

Correct Answer: AC

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_off_mgmt_tasks.html

QUESTION 14

When might a Security Analyst want to review the payload of an event?

A. When immediately after login, the dashboard notifies the analyst of payloads that must be investigated

B. When "Review payload" is added to the offense description automatically by the "System: Notification" rule

C. When the event is associated with an active offense, the payload may contain information that is not normalized or extracted fields

D. When the event is associated with an active offense with a magnitude greater than 5, the payload should be reviewed, otherwise it is not necessary

Correct Answer: C

QUESTION 15

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