C2150-612$^{Q\&As}$

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

QUESTION 1

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 2

Which information can be found under the Network Activity tab?

A. Flows

B. Events

C. Reports

D. Offenses

Correct Answer: A

QUESTION 3

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 4

What is a capability of the Network Hierarchy in QRadar?

A. Determining and identifying local and remote hosts

B. Capability to move hosts from local to remote network segments

C. Viewing real-time PCAP traffic between host groups to isolate malware

D. Controlling DHCP pools for segments groups (i.e. marketing, DMZ, VoIP)

Correct Answer: A

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

QUESTION 5

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 6

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 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

A Security Analyst was asked to search for an offense on a specific day. The requester was not sure of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.

Which filters can the Security Analyst use to search for the information requested?

A. Offense ID, Source IP, Username

B. Magnitude, Source IP, Destination IP

C. Description, Destination IP, Host Name

D. Specific Interval, Username, Destination IP

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/t_qradar_search_my_all_off_pages.html

QUESTION 9

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 10

Where could you get additional details on why the offense was triggered when working on the Offense Summary page?

A. Display > Notes

B. Display > Rules

C. Display > Flows

D. Display > Events

Correct Answer: D

QUESTION 11

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 12

Which type of search uses a structured query language to retrieve specified fields from the events, flows, and simarc tables?

A. Add Filter

B. Asset Search

C. Quick Search

D. Advanced Search

Correct Answer: D

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

c_qradar_ug_search_bar.html

QUESTION 13

What are two common uses for a SIEM? (Choose two.)

A. Managing and normalizing log source data

B. Identifying viruses based on payload MD5s

C. Blocking network traffic based on rules matched

D. Enforcing governmental compliance auditing and remediation

E. Performing near real-time analysis and observation of a network and its devices

Correct Answer: AB

QUESTION 14

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 15

What is an example of the use of a flow data that provides more information than an event data?

A. Represents a single event on the network

B. Automatically identifies and better classifies new assets found on a network

C. Performs near real-time comparisons of application data with logs sent from security devices

D. Represents network activity by normalizing IP addresses ports, byte and packet counts, as well as other details

Correct Answer: D

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