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

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

QUESTION 1

Which device uses signatures for traffic analysis when deployed in a network environment to detect, allow, block, or simulated-block traffic?

A. Proxy

B. QRadar

C. Switch

D. IDS/IPS

Correct Answer: D

QUESTION 2

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 3

Which flow fields should be used to determine how long a session has been active on a network?

A. Start time and end time

B. Start time and storage time

C. Start time and last packet time

D. Last packet time and storage time

Correct Answer: C

Flow timestamps are created as traffic are detected and recored by the QRadar Flow Collector. Some flows can last seconds, ie, an email message, file upload, etc, while others may far longer - minutes, hours, or even days, such as an interactive remote session, audio/video stream (Netflix, voip call), or database application connection. As these sessions/flows continue over time, they are reported into the system. The original "start time" for each session remains the same, when first detected, while the "last packet time" will update as time passes. The best way to see this is to search for the two ip addresses involved in the session/flow, then search over a longer time window ?you should see multiple records, one that ends for each minute that the session was active. Each minute will also have the byte and packet count, for each minute the flow was active. Reference: https://developer.ibm.com/qradar/2018/01/09/qradar-flowfaq/

QUESTION 4

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 5

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