C2150-612Q&As

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

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-flow-faq/

QUESTION 2

Which QRadar rule could detect a possible potential data loss?

A. Apply "Potential data loss" on event of flows which are detected by the local system and when any IP is part of any of the following XForce premium Premium_Malware

B. Apply "Potential data loss" on flows which are detected by the local system and when at least 1000 flows are seen with the same Destination IP and different Source IP in 2 minutes

C. Apply "Potential data loss" on events which are detected by the local system and when the event category for the event is one of the following Authentication and when any of Username are contained in any of Terminated_User

D. Apply "Potential data loss" on flows which are detected by the local system and when the source bytes is greater than 200000 and when at least 5 flows are seen with the same Source IP, Destination IP, Destination Port in 12 minutes

Correct Answer: D

QUESTION 3

What is an effective method to fix an event that is parsed and determined to be unknown or in the wrong QRadar category?

A. Create a DSM extension to extract the category from the payload

B. Create a Custom Property to extract the proper Category from the payload

C. Open the event details, select map event, and assign it to the correct category

D. Write a Custom Rule, and use Rule Response to send a new event in the proper category

Correct Answer: C

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=269b4eff-81ad-4ac59f2b-cdeab14a2500

QUESTION 4

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 5

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