QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

IBM

C2150-612

IBM Security QRadar SIEM V7.2.6 Associate Analyst

QUESTION: 4 7
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.

Answer: A

QUESTION: 48
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

Answer: D

QUESTION: 49
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

Answer: B

QUESTION: 50
What are two characteristics of a SIEM? (Choose two.)

A. Log Management
B. System Deployment
C. Endpoint Software patching
D. Enterprise User management
E. Event Normalization & Correlation

Answer: A, E

QUESTION: 51
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

Answer: B

QUESTION: 52
Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC
B. McAfee ePoIicy Orchestrator via JDBC
C. McAfee ePoIicy Orchestrator via SNMP
D. Solaris Basic Security lVIode (BSM) via Log File Protocol

Answer: C

QUESTION: 53
A mapping of a username to a user's manager can be stored in a Reference Table and output in a search or a report. Which mechanism could be used to do this?

A. Quick Search filters can select users based on their manager's name.
B. Reference Table lookup values can be accessed in an advanced search.
C. Reference Table lookup values can be accessed as custom event properties.

D. Reference Table lookup values are automatically used whenever a saved search is run .

Answer: B

QUESTION: 54
Which kind of information do log sources provide?

A. User login actions
B. Operating system updates
C. Flows generated by users
D. Router configuration exports.

Answer: A