IBM

Exam C2150-612

IBM Security QRadar SIEM V7.2.6, Associate Analyst

Verson: Demo

[Total Questions: 10]

Question No : 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

Answer: D

Question No : 2

Which QRadar component is designed to help increase the search speed in a deployment by allowing more data to remain uncompressed?

A. QRadar Data Node
B. QRadar Flow Processor
C. QRadar Event Collector
D. Qradar Event Processor

Answer: A

Question No : 3

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

Answer: D

Explanation:

References:

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

Question No : 4

Which information can be found under the Network Activity tab?

A. Flows
B. Events
C. Reports
D. Offenses

Answer: A

Question No : 5

A Security Analyst found multiple connection attempts from suspicious remote IP addresses to a local host on the DMZ over port 80. After checking related events no successful exploits were detected.

Upon checking international documentation, this activity was part of an expected penetration test which requires no immediate investigation.

How can the Security Analyst ensure results of the penetration test are retained?

A. Hide the offense and add a note with a reference to the penetration test findings
B. Protect the offense to not allow it to delete automatically after the offense retention period has elapsed
C. Close the offense and mark the source IP for Follow-Up to check if there are future events from the host
D. Email the Offense Summary to the penetration team so they have the offense id, add a note, and close the Offense

Answer: B

Explanation:

References:

http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_Off_Retention.html

Question No : 6

What is the key difference between Rules and Building Blocks in QRadar?

A. Rules have Actions and Responses; Building Blocks do not.
B. The Response Limiter is available on Building Blocks but not on Rules.
C. Building Blocks are built-in to the product; Rules are customized for each deployment.
D. Building Blocks are Rules which are evaluated on both Flows and Events; Rules are evaluated on Offenses of Flows or Events.

Answer: A

Question No : 7

An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username.

What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

A. Each matching event will be tagged with the Rule name, but only one Offense will be created.
B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.
C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfied. Only one offense will be created.
D. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Answer: C

Question No : 8

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

Answer: A

Explanation:

References:

IBM Security QRadar SIEM Users Guide. Page: 201

Question No : 9

How does flow data contribute to the Asset Database?

A. Correlated Flows are used to populate the Asset Database.
B. It provides administrators visibility on how systems are communicating on the network.
C. Flows are used to enrich the Asset Database except for the assets that were discovered by scanners.
D. It delivers vulnerability and ports information collected from scanners responsible for evaluating network assets.

Answer: C

Question No : 10

Which three log sources are supported by QRadar? (Choose three.)

A. Log files via SFTP
B. Barracuda Web Filter
C. TLS multiline Filter
D. Oracle Database Listener
E. Sourcefire Defense Center
F. Java Database Connectivity (JDBC)

Answer: D,E,F