DUMPSHQ

Free Questions for C1000-162 by dumpshq

Shared by Chandler on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which browser is officially supported for QRadar?

Options:

A- Safari version 9.0-3

B- Chromium version 33

C- 32-bit Internet Explorer 9

D- Firefox version 38.0 ESR

Answer:

C

Question 2

Question Type: **MultipleChoice**

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

Options:

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

Answer:

C

Question 3

Question Type: MultipleChoice

How does a Device Support Module (DSM) function?

Options:

A- A DSM is a configuration file that combines received events from multiple log sources and displays them as offenses in QRadar.

B- A DSM is a background service running on the QRadar appliance that reaches out to devices deployed in a network for configuration data.

C- A DSM is a configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

D- A DSM is an installed appliance that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

Answer:

D

Question 4

Question Type: MultipleChoice

Which kind of information do log sources provide?

Options:

A- User login actions

B- Operating system updates

C- Flows generated by users

D- Router configuration exports.

Answer:

A

Question 5

Question Type: **MultipleChoice**

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?

Options:

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 6

Question Type: MultipleChoice

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

Options:

A- Sophos Enterprise console via JDBC

B- McAfee ePolicy Orchestrator via JDBC

C- McAfee ePolicy Orchestrator via SNMP

D- Solaris Basic Security Mode (BSM) via Log File Protocol

Answer:

C

Question 7

Question Type: MultipleChoice

Which QRadar component provides the user interface that delivers real-time flow views?

Options:

A- QRadar Viewer

B- QRadar Console

C- QRadar Flow Collector

D- QRadar Flow Processor

Answer:

B

Explanation:

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