Free Questions for C1000-162 by certscare

Shared by Michael on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What process is used to perform an IP address X-Force Exchange Lookup in QRadar?

Options:

A- Offense summary tab > right-click IP address > Plugin Option > X-Force Exchange Lookup

B- Copy the IP address and go to X-Force Exchange to perform the lookup

C- Run Autoupdate

D- Run a query on maxmind db

Answer:

A

Explanation:

To perform an IP address X-Force Exchange Lookup in QRadar, you can follow these steps2:

Select the Log Activity or the Network Activity tab.

Right-click the IP address that you want to view in X-Force Exchange.

Select More Options > Plugin Options > X-Force Exchange Lookup to open the X-Force Exchange interface2.

The procedure to perform an IP address X-Force Exchange Lookup in QRadar involves selecting either the Log Activity or the Network Activity tab, right-clicking the IP address of interest, and then navigating through More Options > Plugin Options > X-Force Exchange Lookup to access the X-Force Exchange interface.

Question 2

Question Type: **MultipleChoice**

Which two (2) types of data can be displayed by default in the Application Overview dashboard?

Options:

A- Login Failures by User {real-time)

B- Flow Rate (Flows per Second - Peak 1 Min)

C- Top Applications (Total Bytes)

D- Outbound Traffic by Country (Total Bytes)

E- ICMP Type/Code (Total Packets)

Answer:

C, D

Explanation:

The Application Overview dashboard in QRadar includes various default items1.Two of these items areTop Applications (Total Bytes)andOutbound Traffic by Country (Total Bytes)1.

Default dashboards - IBM Documentation

According to the IBM Security QRadar SIEM V7.5 documentation, the Application Overview dashboard by default includes items such as 'Inbound Traffic by Country (Total Bytes),' 'Outbound Traffic by Country (Total Bytes),' and 'Top Applications (Total Bytes)' among others. This confirms that options C and D are displayed by default on the Application Overview dashboard.

Question 3

Question Type: MultipleChoice

What Is the result of the following AQL statement?

```
SELECT * FROM events WHERE username ILIKE '%ERS%'
```

Options:

A- Returns all fields where the username contains the ERS string and is case-sensitive

B- Returns all fields where the username contains the ERS string and is case-insensitive

C- Returns all fields where the username is different from the ERS string and is case-insensitive

D- Returns all fields where the username is different from the ERS string and is case-sensitive

Answer:

B

Explanation:

The AQL (Ariel Query Language) statement provided would return all fields from the 'events' table where the 'username' column contains the string 'ERS', regardless of case. The 'ILIKE' operator in AQL is used for case-insensitive pattern matching, which means that it will match 'ers', 'Ers', 'ErS', etc.

Question 4

Question Type: MultipleChoice

After how much time will QRadar mark an Event offense dormant if no new events or flows occur?

Options:

A- 2 hours

B- 30 minutes

C- 24 hours

D- 5 minutes

Answer:

B

Explanation:

QRadar will mark an Event offense as dormant if no new events or flows occur within 30 minutes. However, if QRadar did not process any events within 4 hours, this also triggers the offense to become dormant. Once dormant, the offense remains in this state for 5 days unless new events or flows are added.

Question 5

Question Type: MultipleChoice

Which two (2) options are used to search offense data on the By Networks page?

Options:

A- Raw/Flows

B- Events/Flows

C- NetIP

D- Severity

E- Network

Answer:

B, E

Explanation:

To search offense data on the By Networks page, an analyst can use the options 'Events/Flows' to filter based on the types of data points, and 'Network' to specify the network they want to search for. This allows for a focused search on specific networks and types of data.

Question 6

Question Type: MultipleChoice

When searching for all events related to "Login Failure", which parameter should a security analyst use to filter the events?

Options:

A- Event Asset Name

B- Event Collector

C- Anomaly Detection Event

D- Event Name

Answer:

D

Explanation:

When searching for all events related to 'Login Failure,' a security analyst should use the Event Name parameter to filter the events. This allows the analyst to specifically target events with descriptions such as 'Database Login Failure,' which indicates that a database login attempt failed.