



IBM C1000-162 Practice Questions

Shared by James on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which two high level Event Categories are used by QRadar? (Choose two.)

Options:

- A- Policy
- B- Direction
- C- Localization
- D- Justification
- E- Authentication

P2P
exams

Answer:

A, E

Question 2

Question Type: MultipleChoice

Which statement regarding saved event search criteria is true?

Options:

- A- Saved search criteria expires
- B- Saved search criteria does not expire
- C- Saved search criteria cannot be reused
- D- You cannot define the name of the saved search criteria

P2P
exams

Answer:

B

Explanation:

In QRadar, when you save search criteria, especially on the Offenses tab, the configured search criteria are retained for future use and do not expire. This permanence ensures that users can quickly access and reuse their preferred search configurations, thereby streamlining the process of monitoring and investigating offenses over time.

Question 3

Question Type: MultipleChoice

What is the effect of toggling the Global/Local option to Global in a Custom Rule?

Options:

- A- It allows a rule to compare events & flows in real time.
- B- It allows a rule to analyze the geographic location of the event source.
- C- It allows rules to be tracked by the central processor for detection by any Event Processor.
- D- It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Answer:

D

Question 4

Question Type: MultipleChoice

The Use Case Manager app has an option to see MITRE heat map.

Which two (2) factors are responsible for the different colors in MITRE heat map?

Options:

- A- Number of offenses generated
- B- Number of events associated to offense
- C- Number of rules mapped
- D- Level of mapping confidence
- E- Number of log sources associated

Answer:

C, D

Explanation:

The MITRE heat map in the Use Case Manager app within QRadar uses several factors to determine the colors displayed, among which the number of rules mapped to MITRE ATT&CK tactics and techniques and the level of mapping confidence are crucial. These factors help visualize the coverage and reliability of rule mappings against the comprehensive MITRE ATT&CK framework, aiding in the identification of potential gaps or areas for improvement in threat detection capabilities.

Question 5

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 6

Question Type: MultipleChoice

AQRadar analyst can check the rule coverage of MITRE ATT&CK tactics and techniques by using Use Case Manager.

In the Use Case Manager app, how can a QRadar analyst check the offenses triggered and mapped to MITRE ATT&CK framework?

Options:

- A- By navigating to 'CRE Report'
- B- From Offenses tab
- C- By clicking on 'Tuning Home'
- D- By navigating to 'Detected in timeframe'

Answer:

D

Explanation:

To check the offenses triggered and mapped to the MITRE ATT&CK framework using the Use Case Manager app, an analyst can navigate through the Offenses tab, click on All Offenses, and then utilize the All Offenses Summary toolbar to display rules contributing to an offense. This process allows for an investigation into how offenses correlate with the MITRE ATT&CK framework. However, the exact option 'Detected in timeframe' is not explicitly mentioned in the provided documentation, and the described procedure offers a broader approach to reviewing offenses and their associated rules within the MITRE ATT&CK context.

Question 7

Question Type: MultipleChoice

Reports can be generated by using which file formats in QRadar?

Options:

- A- PDF, HTML, XML, XLS
- B- JPG, GIF, BMP, TIF
- C- TXT, PNG, DOC, XML
- D- CSV, XLSX, DOCX, PDF

Answer:

A

Explanation:

QRadar supports generating reports in various file formats, including PDF, HTML, XML, and XLS. These formats provide flexibility in how reports are viewed and shared, catering to different needs and preferences for report presentation and analysis.

Question 8

Question Type: MultipleChoice

What happens when you select "False Positive" from the right-click menu in the Log Activity tab?

Options:

- A- You can tune out events that are known to be false positives.
- B- You can investigate an IP address or a user name.
- C- Items are filtered that match or do not match the selection.
- D- The selected event is filtered based on the selected parameter in the event.

Answer:

A

Explanation:

Selecting 'False Positive' from the right-click menu in the Log Activity tab opens a window that enables users to tune out events that are known to be false positives, preventing them from generating offenses. This feature is crucial for minimizing noise and focusing on genuine threats, thereby enhancing the efficiency of threat detection and response processes within QRadar.

Question 9

Question Type: MultipleChoice

A task is set up to identify events that were missed by the Custom Rule Engine. Which two (2) types of events does an analyst look for?

Options:

- A- Log Only Events sent to a Data Store
- B- High Level Category: User Defined Events
- C- Forwarded Events to different destination
- D- High Level Category Unknown Events
- E- Low Level Category: Stored Events

Answer:

A, D

Explanation:

To identify events that were missed by the Custom Rule Engine (CRE) in IBM Security QRadar SIEM, an analyst would primarily look for 'Log Only Events sent to a Data Store' and 'High Level Category Unknown Events.' Log Only Events are those that are stored directly without being processed by the CRE, indicating they might have been overlooked or not matched by any existing rules. High Level Category Unknown Events are those that do not fit into any of the predefined categories in QRadar, suggesting that the CRE might not have rules to handle or categorize these events properly. These types of events are crucial for analysts to review to ensure that no significant incidents are missed and to refine the rule set for better detection in the future.

Question 10

Question Type: MultipleChoice

What right-click menu option can an analyst use to find information about an IP or URL?

Options:

- A- IBM Advanced Threat lookup

- B- Watson Advisor AI IOC Lookup
- C- QRadar Anomaly lookup
- D- X-Force Exchange Lookup

Answer:

D

Explanation:

To find information about an IP or URL within QRadar, analysts can use the right-click menu option 'X-Force Exchange Lookup.' This option is available when right-clicking an IP address or URL from the Offenses tab or event details windows, providing direct access to the X-Force Exchange interface for detailed threat intelligence and contextual information.

Question 11

Question Type: MultipleChoice

How long does QRadar store payload indexes by default?

Options:

- A- 7 days
- B- 30 days
- C- 14 days
- D- 90 days

Answer:

B

Explanation:

By default, QRadar stores payload indexes for a duration of 30 days. This retention period is configurable, allowing administrators to adjust how long specific data is retained based on their requirements.

Question 12

Question Type: MultipleChoice

On the Offenses tab, which column explains the cause of the offense?

Options:

- A- Description
- B- Offense Type
- C- Magnitude
- D- IPs

Answer:

B

Explanation:

On the Offenses tab within QRadar, the 'Offense Type' column explains the cause of the offense. The offense type is determined by the rule that triggered the offense, and it dictates the kind of information displayed in the Offense Source Summary pane. This helps analysts understand the nature and origin of the offense, facilitating more effective investigation and response actions.

Question 13

Question Type: MultipleChoice

On which lab can an analyst perform a "Flow Bias" Quick Search?

Options:

- A- Asset Management app
- B- Log Activity tab
- C- Log Source Management app
- D- Network Activity tab

Answer:

D

Explanation:

A 'Flow Bias' Quick Search can be performed from the Network Activity tab in QRadar, providing insights into network flows and potential anomalies or biases in the traffic patterns.



To Get Premium Files for C1000-162 Visit

<https://www.p2pexams.com/products/c1000-162>

For More Free Questions Visit

<https://www.p2pexams.com/ibm/pdf/c1000-162>

20%
DISCOUNT

P2P
exams