



Free Questions for C1000-162 by actualtestdumps

Shared by Hill on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

Question Type: MultipleChoice

Which two (2) types of categories comprise events?

Options:

- A- Unsupported
- B- Unfound
- C- Stored
- D- Found

E- Parsed

Answer:

C, E

Explanation:

While the documentation does not explicitly list 'Stored' and 'Parsed' as categories comprising events, it discusses high-level event categories and the process of categorizing incoming events for easy searching. Without specific mention of the categories 'Stored' and 'Parsed,' the provided documentation does not verify any of the options directly. Further insight into event categories is provided by discussing how events are grouped into high-level categories for organizational purposes.

Question 3

Question Type: Hotspot

New vulnerability scanners are deployed in the company's infrastructure and generate a high number of offenses. Which function in the Use Case Manager app does an analyst use to update the list of vulnerability scanners?

Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses



Tune most active rules based on offense count
QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.



Tune most active rules based on CRE event count
For rules that generate Custom Rule Engine (CRE) events, the CRE event report can help determine which rules generate the most CRE events. You can tune these rules or use the event information from the report to update your QRadar enrichment. See Learn more section at top of this report for more information about this report.

Tune your QRadar offenses by going through the most common configuration steps



Review network hierarchy
Network Hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.



Review building blocks
Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.

Tune QRadar by analyzing inactive rules



Review inactive rules
Rules that don't trigger in a certain period of time might be misconfigured and you might not be getting the most value out of your QRadar deployment. Review your inactive rules for possible tuning options.

Question 4

Question Type: MultipleChoice

A QRadar analyst develops an advanced search on the Log Activity tab and presses the shortcut "Ctrl + Space" in the search field. What information is displayed?

Options:

- A-** The full list of AQL databases, functions and fields (properties) is displayed.
- B-** The full list of AQL tables and relationships from a database is displayed.
- C-** The full list of AOL functions, fields (properties), and keywords is displayed.
- D-** The full list of AQL functions, tables, and views from a database is displayed.

Answer:

A

Explanation:

The information displayed when pressing "Ctrl + Space" in the search field in the Log Activity tab in QRadar is not explicitly mentioned in the search results. However, in general, this shortcut is often used in various software and platforms to display a list of available commands, functions, or properties. In the context of QRadar, it's likely that pressing "Ctrl + Space" in the search field would display a list of available AQL (Ariel Query Language) databases, functions, and fields (properties).

Question 5

Question Type: OrderList

Select all that apply

What is the sequence to create and save a new search called "Offense Data" that shows all the CRE events that are associated with offenses?

Unordered Options

From the QRadar Console, click Save Criteria.

Click Search.

Under Search Parameters, add Associated with Offense is True and Log Source Type is Custom Rule Engine.

From the QRadar Console, click the Log Activity tab. Click Search > New Search.

Provide the Search Name "Offense Data" and click OK.



Ordered Options



Answer:

From the QRadar Console, click the Log Activity tab, Click Search > New Search.

Provid

Question 6

Question Type: MultipleChoice

The magnitude rating of an offense in QRadar is calculated based on which values?

Options:

- A- Relevance, severity, importance
- B- Relevance, credibility, severity
- C- Criticality, severity, importance
- D- Criticality, severity, credibility

Answer:

B

Explanation:

The magnitude rating of an offense in QRadar is calculated based on relevance, severity, and credibility. Relevance determines the impact on the network, credibility indicates the integrity of the offense, and severity represents the level of threat. QRadar uses complex algorithms to calculate and periodically re-evaluate the offense magnitude rating.

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>

