Free Questions for C1000-162 by vceexamstest

Shared by Pitts on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two characteristics of a SIEM? (Choose two.)

Options:

A- Log Management

B- System Deployment

C- Endpoint Software patching

D- Enterprise User management

E- Event Normalization & Correlation

Answer:

A, E

Question 2

Question Type: MultipleChoice

Which two (2) components are necessary for generating a report using the QRadar Report wizard?

Options:

A- Saved search

B- Dynamic search

C- Layout

D- Quick search

E- Email address

Answer:

A, C

Explanation:

In IBM Security QRadar SIEM, generating a report using the QRadar Report Wizard requires a 'Saved Search' and a 'Layout.' A Saved Search is a predefined search criterion that users save in QRadar to reuse for various reporting or analysis purposes. It acts as the data source for the report, defining what data will be included. The Layout component refers to the structure and presentation of the report, including how the data from the Saved Search is organized and displayed. It encompasses the formatting, charts, tables, and other visual elements that make up the final report. Together, these components ensure that reports are not only informative but also well-organized and readable, catering to the specific informational needs and preferences of the users or stakeholders.

Question 3

Question Type: MultipleChoice

Which reference set data element attribute governs who can view its value?

Options:

A- Tenant Assignment

B- Origin

C- Reference Set Management MSSP

D- Domain

Answer:

D

Explanation:

The Domain attribute governs who can view the value of a reference set data element, ensuring that only users with appropriate domain access or tenant assignments can view the data. This is essential for maintaining data visibility and access control within a multi-tenant QRadar environment.

Question 4

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.

Question 5

Question Type: MultipleChoice

What does this example of a YARA rule represent?

Options:

A- Flags containing hex sequence and str1 less than three times

B- Flags content that contains the hex sequence, and hex! at least three times

C- Flags for str1 at an offset of 25 bytes into the file

D- Flags content that contains the hex sequence, and str1 greater than three times

Answer:

C

Explanation:

A YARA rule is used for malware identification and classification, based on textual or binary patterns. The example provided suggests a rule that flags occurrences of a specific string (str1) at a precise location within a file. The 'offset' keyword in YARA rules specifies the exact byte position where the pattern (in this case, 'str1') should appear. Thus, the correct interpretation of the YARA rule example is that it flags instances where 'str1' appears 25 bytes into the file, indicating a very specific pattern match used for identifying potentially malicious files or activities that conform to this pattern.

Question 6

Question Type: MultipleChoice

What is the default number of notifications that the System Notification dashboard can display?

Options:

A- 50 notifications

B- 20 notifications

C- 10 notifications

D- 5 notifications

Answer:

C

Explanation:

The default setting for the System Notification dashboard is to display 10 notifications, providing a manageable overview of system alerts and issues. Users can adjust this setting to view fewer or more notifications based on their preferences.

Question 7

Question Type: MultipleChoice

When examining lime fields on Event Information, which one represents the time QRadar received the raw event?

Options:

A- Processing Time

B- Log Source Time

C- Start Time

D- Storage Time

Answer:

C

Explanation:

The 'Start Time' timestamp represents when an event is received by a QRadar Event Collector, marking the moment QRadar first becomes aware of the event. This is crucial for understanding the timing of event processing and potential delays in the event pipeline.

Question 8

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 9

Question Type: MultipleChoice

In Rule Response, which two (2) options are available for Offense Naming?

Options:

A- This information should be removed from the current name of the associated offenses

B- This information should contribute to (he name of the associated offenses

C- This information should set or replace the name of the associated offenses

D- This information should contribute to the dispatched event name of the associated offenses.

E- This information should contribute to the category naming of the associated offenses

Answer:

B, C

Explanation:

In Rule Response for Offense Naming, QRadar provides options to either contribute to or set/replace the name of the associated offenses. These options allow for dynamic naming of offenses based on event name information, facilitating easier identification and

categorization of offenses.

Question 10

Question Type: MultipleChoice

Events can be exported from the QRadar Log Activity tab in which file formats?

Options:

A- JSON. XML, and CSV

B- XLS and CSV

C- JSON and XML

D- XML and CSV

Answer:

D

Explanation:

Events can be exported from the QRadar Log Activity tab in XML (Extensible Markup Language) or CSV (Comma-Separated Values) formats, providing flexibility in how data is extracted and used for further analysis outside of QRadar.