



Vendor: IBM

Exam Code: C1000-162

Exam Name: IBM Security QRadar SIEM V7.5 Deployment

Version: DEMO

QUESTION 1

Create a list that stores Username as the first key. Source IP as the second key with an assigned cidr data type, and Source Port as the value. The example above refers to what kind of reference data collections?

- A. Reference map of sets
- B. Reference store
- C. Reference table
- D. Reference map

Answer: C

Explanation:

The example provided refers to a "Reference table," which is a type of reference data collection in QRadar that can store complex structured data. A reference table allows for multiple keys and values, supporting the storage of data like Usernames, Source IPs with a specific data type (e.g., cidr for IP addresses), and Source Ports as values.

QUESTION 2

What type of custom property should be used when an analyst wants to combine extraction-based URLs, virus names, and secondary user names into a single property?

- A. AOL-based property
- B. Absolution-based property
- C. Extraction-based property
- D. Calculation-based property

Answer: A

Explanation:

When an analyst wants to combine multiple extraction and calculation-based properties into a single property, such as URLs, virus names, and secondary user names, an AOL-based property should be used. AOL (Ariel Query Language)-based properties allow for the aggregation of diverse data types into a unified custom property, facilitating more flexible and comprehensive data analysis within QRadar.

QUESTION 3

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

- 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 4

Which statement regarding saved event search criteria is true?

- 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

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 5

Which two (2) aggregation types are available for the pie chart in the Pulse app?

- A. Last
- B. Total
- C. Average
- D. First
- E. Middle

Answer: BC

Explanation:

For pie charts in the Pulse app of QRadar, the available aggregation types include "Total" and "Average." These aggregation types allow for the representation of data in a manner that summarizes the total sum of the data points or their average value, respectively, providing insightful and concise visualizations of the data within the Pulse app dashboards. This information is implied from the general capabilities of dashboard items in QRadar, as detailed in the provided documentation, which typically includes such aggregation options for data visualization.

QUESTION 6

How does a Device Support Module (DSM) function?

- 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 7

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

- 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 8

Which browser is officially supported for QRadar?

- 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 9

A Security Analyst was asked to search for an offense on a specific day. The requester was not sure of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username. Which filters can the Security Analyst use to search for the information requested?

- A. Offense ID, Source IP, Username
- B. Magnitude, Source IP, Destination IP
- C. Description, Destination IP, Host Name
- D. Specific Interval, Username, Destination IP

Answer: D

QUESTION 10

What is an effective method to fix an event that is parsed and determined to be unknown or in the wrong QRadar category?

- A. Create a DSM extension to extract the category from the payload
- B. Create a Custom Property to extract the proper Category from the payload
- C. Open the event details, select map event, and assign it to the correct category
- D. Write a Custom Rule, and use Rule Response to send a new event in the proper category

Answer: B

QUESTION 11

Which type of rule requires a saved search that must be grouped around a common parameter?

- A. Flow Rule
- B. Event Rule
- C. Common Rule
- D. Anomaly Rule

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14