# Free Questions for C1000-156 by certscare

## Shared by Moran on 29-05-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Which is a valid routing rule combination?

## Options:

**A-** Drop and Bypass Correlation

**B-** Drop and Log Only

**C-** Forward and Bypass Correlation

**D-** Bypass Correlation and Log Only

## Answer:

C

## Explanation:

Forward: Data is forwarded to a specified destination. It is also stored in the database and processed by the Custom Rules Engine (CRE).

Drop: Data is dropped, meaning it is not stored in the database and is not processed by the CRE. If you select the "Drop" option, any events that match this rule are credited back 100% to the license.

Bypass Correlation: Data bypasses the CRE but is stored in the database. This option allows events to be used in analytic apps and for historical correlation runs. It's useful when you want specific events to skip real-time rules.

Log Only (Exclude Analytics): Events are stored in the database and flagged as "Log Only." They bypass the CRE and are not available for historical correlation. These events contribute to neither offenses nor real-time analytics.

Now, let's look at the valid combinations:

Forward and Drop: Data is forwarded to a specified destination, but it is not stored in the database or processed by the CRE. Dropped events are credited back to the license.

Forward and Bypass Correlation: Data is forwarded to a destination and stored in the database, but CRE rules do not run on it. Useful for scenarios where you want events to bypass real-time rules but still be available for historical correlation.

Forward and Log Only (Exclude Analytics): Events are forwarded to a destination, stored as "Log Only," and bypass the CRE. They are not available for historical correlation and are credited back to the license.

# Question 2

**Question Type:** **MultipleChoice**

Which is a valid statement about the process of restoring a backup archive?

## Options:

**A-** A configuration restore must be performed on a console where the IP address matches the IP address of a managed host in the backup.

**B-** A backup archive can only be restored for the same software version, including fix pack versions.

**C-** When restoring all configuration items included in the backup archive, only configuration information, offense data, and asset data are restored.

**D-** A restoration might fail if you restore the configuration backup before the data backup.

## Answer:

B

## Explanation:

When restoring a backup archive in QRadar, it is essential to ensure that the software version matches exactly. This includes both the base version and any fix pack versions.

Attempting to restore a backup archive from a different software version can lead to compatibility issues, data corruption, and system instability.

Always verify that the backup archive corresponds to the same QRadar version before initiating the restoration process.

IBM QRadar SIEM V7.5 Administration documentation.

# Question 3

**Question Type:** MultipleChoice

The Report wizard provides a step-by-step guide to design, schedule, and generate reports. Which three (3) key elements does the report wizard use to help you create a report?

## Options:

**A-** Content

**B-** Format

**C-** Container

**D-** Display

**E-** Banner

**F-** Layout

## Answer:

A, B, F

## Explanation:

The Report wizard in IBM QRadar SIEM provides a structured approach to designing, scheduling, and generating reports. The three key elements used by the Report wizard to help you create a report are:

Content: This element involves selecting the specific data and metrics you want to include in the report. It can include various log sources, events, and other relevant security data.

Format: This element defines how the data will be presented in the report. It includes selecting the type of report (e.g., tabular, graphical) and the specific visualizations that will best represent the data.

Layout: This element refers to the overall structure and design of the report, including the arrangement of content and visual elements to ensure the report is easily readable and professionally formatted.

These elements together ensure that the reports generated are comprehensive, visually appealing, and tailored to the specific needs of the organization.

Reference IBM QRadar SIEM documentation

# Question 4

**Question Type:** MultipleChoice

How many vulnerability processors can you have in your deployment?

## Options:

**A-** 5

**B-** 3

**C-** 10

**D-** 1

## Answer:

D

## Explanation:

In QRadar SIEM V7.5, the number of vulnerability processors is limited to1.

These vulnerability processors are responsible for handling and processing vulnerability data within the system.

Having multiple vulnerability processors is not supported in this version of QRadar.

IBM QRadar SIEM V7.5 Administration documentation.

# Question 5

**Question Type:** MultipleChoice

When restoring backups of your apps in a QRadar environment, what information is restored?

## Options:

**A-** The last known good version of your apps configuration, your application data, and any apps that were configured on an App Host are restored.

**B-** The applications that are installed on the Console are restored, and any applications that are installed on an AppHost must be backed up separately.

**C-** The apps configuration, the console configuration, and app data are restored.

**D-** The apps configuration and app data are restored.

## Answer:

A

## Explanation:

When restoring backups of your apps in a QRadar environment, the system restores the last known good version of your apps' configuration, your application data, and any apps that were configured on an App Host. This comprehensive restoration process ensures that all critical components of your applications, including their configurations and data, are recovered to their previous states. This is crucial for maintaining the integrity and functionality of the applications after a restoration.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on Backup and Restore Procedures

# Question 6

**Question Type:** MultipleChoice

Which field is mandatory when you use the DSM Editor to map an event to a OID?

## Options:

**A-** High-level Category

**B-** Low-level Category

**C-** Event Category

**D-** Event ID

## Answer:

D

## Explanation:

When using the DSM (Device Support Module) Editor in IBM QRadar to map an event to an OID (Object Identifier), the Event ID field is mandatory. The Event ID uniquely identifies the event within QRadar and is essential for ensuring that the correct event data is associated with the appropriate OID. This mapping process allows QRadar to properly categorize and handle events based on their unique identifiers.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on DSM Editor and Event Mapping

# Question 7

**Question Type:** MultipleChoice

Which two (2) data sources can be assigned to a domain in the Domain Management function?

## Options:

**A-** Users

**B-** Rules

**C-** Flow collectors

**D-** Log sources

**E-** X-Force Integration Feed

## Answer:

C, D

## Explanation:

In the Domain Management function of IBM QRadar SIEM, two key data sources that can be assigned to a domain are Flow Collectors and Log Sources. Flow collectors capture and analyze network flow data, while log sources refer to various devices and applications that send log data to QRadar for analysis. By assigning these data sources to a domain, administrators can segment and manage the data more effectively, ensuring that the correct flow and log data are processed and analyzed within the designated domain. This segmentation enhances security and performance by isolating data handling according to domain-specific policies.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on Domain Management and Data Source Assignment

# Question 8

**Question Type:** MultipleChoice

An administrator is reviewing the system notifications and discovers this error:

Insufficient disk space to complete data export request.

The Export Directory property in the System Settings has the default configuration.

Which disk partition does the administrator need to check?

## Options:

**A-** /store/ariel/events/exports

**B-** /var/log/exports

**C-** /storetmp/exports

**D-** /store/exports

## Answer:

A

## Explanation:

When the error 'Insufficient disk space to complete data export request' is encountered, and the Export Directory property in the System Settings has the default configuration, the disk partition that needs to be checked is /store/ariel/events/exports. This directory is typically used for exporting event data in QRadar SIEM. The error indicates that the available disk space in this partition is insufficient to handle the export operation. Administrators should check the storage usage of this partition and manage the space by either cleaning up unnecessary files or expanding the storage capacity.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on System Notifications and Disk Management

# Question 9

**Question Type:** MultipleChoice

Domain assignments lake precedence over the settings of which other elements from a security profile?

## Options:

**A-** Security profiles, Networks, and Log Sources tabs

**B-** Security profiles. Networks, and Domains

**C-** Permission Precedence, and Log Sources tabs

**D-** Permission Precedence. Networks, and Log Sources tabs

## Answer:

D

## Explanation:

In IBM QRadar SIEM, domain assignments take precedence over the settings of other elements from a security profile, specifically Permission Precedence, Networks, and Log Sources tabs. This hierarchical precedence ensures that the domain settings are enforced across different security configurations. The domain settings effectively override other configurations to maintain consistency and security across the environment. This structure helps in managing access and permissions more effectively by ensuring that the domain-level policies are the primary controlling factor.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on Domain Management and Security Profiles

# Question 10

**Question Type:** MultipleChoice

How can an administrator configure a rule response to add event data to a reference set?

## Options:

**A-** Write a custom script.

**B-** Use AQL functions.

**C-** Use the 'add the following data to a reference set' rule test.

**D-** Use the 'add to reference set' rule response.

## Answer:

D

## Explanation:

Administrators can configure a rule response in QRadar to add event data to a reference set by using the 'add to reference set' rule response. This is a predefined response action in QRadar that allows specific event data to be added to a reference set when the rule conditions are met.

Navigate to the 'Offenses' tab in the QRadar console.

Select 'Rules' from the navigation pane.

Create a new rule or edit an existing rule.

In the 'Rule Response' section, add a new response.

Select the 'Add to Reference Set' response.

Specify the reference set and the data to be added.

Save and deploy the rule.

Reference IBM QRadar SIEM V7.5 Administration documentation

# Question 11

**Question Type:** **MultipleChoice**

You are using the command line interface (CLI) and need to fix a storage issue. What command do you use to verify disk usage levels?

## Options:

**A-** df -h

**B-** Is -laF

**C-** lsof -h

**D-** du -h

## Answer:

A

## Explanation:

To verify disk usage levels in a Linux environment, the df -h command is used. This command provides an overview of the disk space usage, displaying the available and used space in a human-readable format.

Open the terminal or CLI on the system.

Type df -h and press Enter.

Review the output, which will show the filesystem, size, used space, available space, and usage percentage for all mounted filesystems.

Reference IBM QRadar SIEM V7.5 Administration documentation.

# Question 12

**Question Type:** MultipleChoice

On which managed hosts is QRadar event data stored in the Ariel database?

## Options:

**A-** On the Event Collector and attached Data Node

**B-** On the Data Gateway and attached Data Node

**C-** On the Event Processor and attached Data Node

**D-** On the App Host and attached Data Node

## Answer:

C

## Explanation:

QRadar event data is stored in the Ariel database on the Event Processor and any attached Data Nodes. The Event Processor is responsible for processing incoming events, performing correlation, and storing the event data. The attached Data Nodes provide additional storage capacity and can be used to extend the storage available to the Event Processor.

Reference IBM QRadar SIEM V7.5 Administration documentation.