Snowflake
SEA-C01
Snowflake Certified SnowPro Advanced - Security Engineer

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

A Security Engineer needs to generate multiple sets of synthetic data for a machine learning model that will be used to detect fraudulent financial transactions. How can the Engineer ensure join key values will remain consistent across all runs?

A. Add the similarity filter parameter and set it to true: 'similarity_filter': True
B. Create a dedicated secret, and reference the consistency_secret': SYSTEM$REFERENCE('SECRET', 'MY_SECRET')) in the procedure call.
C. In the columns parameter, set the join key argument to true: 'columns': {'<column_name>': {'join_key': True}}
D. Add the replace output tables parameter set to true: 'replace_output_tables': TRUE

Answer: B

Question: 2

An organization wants to automatically classify sensitive columns such as personally identifiable information (PII) within Snowflake datasets. Which Snowflake capability supports this functionality?

A. Resource monitor configuration identifying sensitive data using compute metrics
B. Dynamic data masking policies automatically applied during warehouse execution
C. Automated data classification using Snowflake classification services and governance tools
D. Network policy configuration identifying sensitive data based on login attributes

Answer: C

Question: 3

A governance pipeline has been configured to ingest AI decisions only if they match a JSON schem
a. Which is the MOST direct way to generate the LLM return schema-conformant JSON WITHOUT writing a custom validator?
A. Wrap the output string with OBJECT_CONSTRUCT before performing the insert.
B. Use CLASSIFY_TEXT to identify the categories and rebuild the JSON in SQL.
C. Set a session parameter to force the JSON mode.
D. Use the SNOWFLAKE.CORTEX.COMPLETE command with the => {'response_format': <JSON schema>} argument.

Answer: D

Question: 4

A Snowflake security engineer must implement mitigation strategies following a security risk assessment. Which actions help reduce security risks?
(Choose two)

A. Increase warehouse compute capacity used by sensitive workloads
B. Rotate authentication credentials and API keys associated with service accounts
C. Implement least-privilege access controls across Snowflake roles and privileges
D. Enable automatic clustering for frequently accessed tables

Answer: B,C

Question: 5

A security engineer must protect sensitive customer information in a Snowflake table so that analysts only see masked values unless they have an approved security role. Which feature should be implemented?

A. Dynamic data masking policy
B. Row access policy
C. Network policy
D. Warehouse resource monitor

Answer: A

Question: 6

During a security investigation, a Snowflake administrator must determine which tables were accessed by a compromised user. Which view provides this information?

A. WAREHOUSE_LOAD_HISTORY view identifying compute workload statistics
B. LOGIN_HISTORY view identifying authentication attempts and session metadata
C. RESOURCE_MONITOR_HISTORY view identifying warehouse credit consumption
D. ACCESS_HISTORY view identifying objects accessed during query execution

Answer: D

Question: 7

A security engineer wants to audit how classification tags are applied to Snowflake objects. Which view provides visibility into tag usage and assignments?

A. TAG_REFERENCES view providing information about tag assignments to objects
B. QUERY_HISTORY view providing information about executed SQL statements
C. LOGIN_HISTORY view providing authentication event records for user sessions
D. WAREHOUSE_LOAD_HISTORY view providing compute workload statistics

Answer: A

Question: 8

An audit identified that there may be user and custom roles that are over-privileged at the Snowflake account level. Which combination of steps should be implemented to monitor this situation? (Select THREE).

A. Check the ACCESS_HISTORY view to identify which users have accessed which data.
B. Check the GRANTS_TO_USERS view to identify users who have access to system roles.
C. Check the GRANTS_TO_ROLES view to identify roles that have been granted the MANAGE GRANTS privilege.
D. Check the CREDENTIALS view to see which authentication methods have been used by users.
E. Check the QUERY_HISTORY view to identify if unexpected GRANT, REVOKE, CREATE USER, or ALTER_USER queries have been run.
F. Check the ROLES view to see who owns the existing roles.

Answer: B,C,E

Question: 9

A Security Engineer is designing a role hierarchy for a multi-team environment that has these requirements:
1. Data Scientists need read-only access to sensitive data sets in SECURE_DB.SCIENCE_DATA.
2. Data Engineers need to create and manage objects in the same data set but should not be able to access sensitive data.
3. Compliance Officers must have audit access and be able to manage grants without modifying or querying data.
4. All roles must be custom, follow least privilege best practice, and support future scalability.
Which implementation should be used?

A. Assign system roles and restrict access using network policies and warehouse-level controls.
B. Create individual custom roles and assign them directly to users, eliminating privilege inheritance vulnerabilities.
C. Use masking policies and schema-level grants to control access, assigning all users a shared role.

D. Create three custom roles with scoped privileges and nest them under a parent role, giving the custom roles limited access.

Answer: D

Question: 10

As part of a security investigation, a Security Engineer identified a suspicious query (QUERY_ID = '01c-b3a-d3c') in the ACCOUNT_USAGE.QUERY_HISTORY view. The query executed a complex, multi-layered secure view.
The Engineer must provide definitive proof of all underlying tables that were read by that single, specific execution of the query. How should this requirement be met?

A. Query ACCOUNT_USAGE.VIEWS to find the view definition, and manually parse the DDL text to list all referenced tables.
B. Query the ACCOUNT_USAGE.OBJECT_DEPENDENCIES view to recursively find all tables that the secure view is linked to.
C. Query the ACCOUNT_USAGE.ACCESS_HISTORY view, filtering WHERE QUERY_ID = '01c-b3a-d3c', and inspect the BASE_OBJECTS_ACCESSED.
D. Monitor the SNOWFLAKE.TRUST_CENTER views for login anomalies associated with the user who ran the query.

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/