Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 307 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 307
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization is developing a sophisticated machine learning (ML) model to predict customer behavior for targeted marketing campaigns. The BigQuery dataset used for training includes sensitive personal information. You must design the security controls around the AI/ML pipeline. Data privacy must be maintained throughout the model's lifecycle and you must ensure that personal data is not used in the training process. Additionally, you must restrict access to the dataset to an authorized subset of people only. What should you do?

A. De-identify sensitive data before model training by using Cloud Data Loss Prevention (DLP)APIs. and implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

B. Implement Identity-Aware Proxy to enforce context-aware access to BigQuery and models based on user identity and device.

C. Implement at-rest encryption by using customer-managed encryption keys (CMEK) for the pipeline. Implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

D. Deploy the model on Confidential VMs for enhanced protection of data and code while in use. Implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:18 p.m.*

Comments

Type your comment...

Submit

532b5da 8 months ago

Selected Answer: A

Ans is A
We want data privacy through out lifecycle.
C is at rest
D is in use
B says nothing about data privacy

upvoted 2 times

json4u 9 months, 2 weeks ago

Selected Answer: A

It's A
Well explained below.

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

A - Data De-identification: De-identifying sensitive data using Cloud DLP APIs ensures that the data used for model training does not contain personally identifiable information (PII). This protects data privacy and reduces the risk of unauthorized access or misuse.
IAM Policies: Implementing strict IAM policies controls access to BigQuery, ensuring that only authorized personnel can access and use the dataset. This further protects data privacy and reduces the risk of unauthorized access.
Comprehensive Approach: This approach combines data de-identification and IAM controls to provide a robust and effective security solution for the AI/ML pipeline.

upvoted 1 times