

🔗 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 17 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 17

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier.

Which Cloud Data Loss Prevention API technique should you use to accomplish this?

- A. Generalization
- B. Redaction
- C. CryptoHashConfig
- D. CryptoReplaceFfxFpeConfig

Show Suggested Answer

by [xhova](#) at April 3, 2020, 9:38 a.m.

Comments

Type your comment...

Submit

[xhova](#) Highly Voted 4 years, 9 months ago

Answer is D

<https://cloud.google.com/dlp/docs/pseudonymization>

   upvoted 17 times

  **smart123** 4 years, 7 months ago


Option D is correct because it is reversible whereas option B is not.

   upvoted 3 times

  **SilentSec** 4 years, 6 months ago

Also the same usecase in the url that you post. D is right.

   upvoted 1 times

  **gcp_learner** Highly Voted  4 years, 6 months ago

The answer is A.

By bucketing or generalizing, we achieve a reversible pseudonymised data that can still yield the required analysis.

<https://cloud.google.com/dlp/docs/concepts-bucketing>

   upvoted 6 times

  **Sheeda** 4 years, 5 months ago

Completely wrong

The answer is D for sure. The example was even in google docs but replaced for some reasons.

http://price2meet.com/gcp/docs/dlp_docs_pseudonymization.pdf

   upvoted 7 times

  **crazycosmos** Most Recent  8 months ago

Selected Answer: D

it is reversible for D

   upvoted 1 times

  **ManuelY** 8 months, 3 weeks ago

Selected Answer: D

Reversible

   upvoted 1 times

  **Kiroo** 9 months, 3 weeks ago

Selected Answer: D

For sure is D

<https://cloud.google.com/sensitive-data-protection/docs/transformations-reference#fpe>

I was in doubt about C but the hash can't be returned into the original value

   upvoted 1 times

  **ketoza** 1 year ago

Selected Answer: D

<https://cloud.google.com/dlp/docs/transformations-reference#fpe>

   upvoted 1 times

  **okhascorpio** 1 year, 3 months ago

A. seems like good fit here. Preserve data utility while also reducing the identifiability of the data.

<https://cloud.google.com/dlp/docs/concepts-bucketing>

   upvoted 1 times

  **okhascorpio** 1 year, 3 months ago

I take it back. its not reversible.

   upvoted 1 times

  **aashishh** 1 year, 9 months ago

Selected Answer: A

Generalization is a technique that replaces an original value with a similar, but not identical, value. This technique can be used to help protect sensitive data while still allowing statistical analysis.

In this scenario, the employer can use generalization to replace the actual bonus compensation values with generalized values that are statistically similar but not identical. This allows the employer to perform analysis on the data without exposing the sensitive compensation data for any individual employee.

Using Generalization can be reversible to identify outliers. The employer can then use the original data to investigate further

and correct any earning disparities.

Redaction is another DLP API technique that can be used to protect sensitive data, but it is not suitable for this scenario since it would remove the data completely and make statistical analysis impossible. CryptoHashConfig and CryptoReplaceFfxFpeConfig are also not suitable for this scenario since they are encryption techniques and do not allow statistical analysis of data.

   upvoted 3 times

  **aashissh** 1 year, 9 months ago

Answer is A:



Generalization is a technique that replaces an original value with a similar, but not identical, value. This technique can be used to help protect sensitive data while still allowing statistical analysis.

In this scenario, the employer can use generalization to replace the actual bonus compensation values with generalized values that are statistically similar but not identical. This allows the employer to perform analysis on the data without exposing the sensitive compensation data for any individual employee.

Using Generalization can be reversible to identify outliers. The employer can then use the original data to investigate further and correct any earning disparities.

Redaction is another DLP API technique that can be used to protect sensitive data, but it is not suitable for this scenario since it would remove the data completely and make statistical analysis impossible. CryptoHashConfig and CryptoReplaceFfxFpeConfig are also not suitable for this scenario since they are encryption techniques and do not allow statistical analysis of data.

   upvoted 1 times

  **Lyfedge** 1 year, 10 months ago

Correct Answer is (D): De-identifying sensitive data

Cloud Data Loss Prevention (DLP) can de-identify sensitive data in text content, including text stored in container structures such as tables. De-identification is the process of removing identifying information from data. The API detects sensitive data such as personally identifiable information (PII), and then uses a de-identification transformation to mask, delete, or otherwise obscure the data.

For example, de-identification techniques can include any of the following:

Masking sensitive data by partially or fully replacing characters with a symbol, such as an asterisk (*) or hash (#).

   upvoted 1 times

  **mahi9** 1 year, 11 months ago

Selected Answer: D

D is the most viable option

   upvoted 1 times

  **null32sys** 1 year, 11 months ago

The Answer is A


   upvoted 1 times

  **Ishu_awsuguy** 2 years ago

Correct answer is D. But,

The answer does not have a CryptoDeterministicConfig . We recommend using CryptoDeterministicConfig for all use cases which do not require preserving the input alphabet space and size, plus warrant referential integrity.

https://cloud.google.com/dlp/docs/transformations-reference#transformation_methods

   upvoted 1 times

  **zanhsieh** 2 years, 1 month ago

Answer D. Note that `CryptoReplaceFfxFpeConfig` might not be used in a real exam; they might change to `format preserve encryption`.

   upvoted 5 times

  **Littleivy** 2 years, 2 months ago

The answer is D

https://cloud.google.com/dlp/docs/transformations-reference#transformation_methods



   upvoted 2 times

  **Premumar** 2 years, 3 months ago

Selected Answer: D

D is the only option that is reversible.

   upvoted 3 times

  **GCP72** 2 years, 5 months ago

Selected Answer: D

D. CryptoReplaceFfxFpeConfig is the correct answer for sure, it allows you to recover the original data.

   upvoted 1 times

[Load full discussion...](#)



Platform

> [Home](#)

> [All Exams](#)

> [Examtopics PRO](#)

> [Training Courses](#)



© 2024 ExamTopics