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 255 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 255
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization's financial modeling application is already deployed on Google Cloud. The application processes large amounts of sensitive customer financial data. Application code is old and poorly understood by your current software engineers. Recent threat modeling exercises have highlighted the potential risk of sophisticated side-channel attacks against the application while the application is running. You need to further harden the Google Cloud solution to mitigate the risk of these side-channel attacks, ensuring maximum protection for the confidentiality of financial data during processing, while minimizing application problems. What should you do?

A. Enforce stricter access controls for Compute Engine instances by using service accounts, least privilege IAM policies, and limit network access.

B. Implement a runtime library designed to introduce noise and timing variations into the application's execution which will disrupt side-channel attack.

C. Migrate the application to Confidential VMs to provide hardware-level encryption of memory and protect sensitive data during processing.

D. Utilize customer-managed encryption keys (CMEK) to ensure complete control over the encryption process.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:24 a.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: C

https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview

https://cloud.google.com/confidential-computing/confidential-vm/docs

upvoted 1 times

BondleB 8 months, 4 weeks ago

Selected Answer: C

Reference:
https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview

https://cloud.google.com/confidential-computing/confidential-vm/docs

upvoted 1 times

BondleB 8 months, 4 weeks ago

Migrate application to Confidential VMs in Google Cloud to provide hardware-level encryption, this can be achieved by:
1) Creating a Confidential VM instance in a sole-tenant node
2) Encrypting a new disk and enforcing Confidential VM use
3) Creating a new node pool with Confidential GKE Nodes enabled.
Confidential VMs help protect sensitive data by providing a trusted execution environment for AI workloads thereby reducing the risk of unauthorized access, even by privileged users or malicious actors within the system.
Since the application processes large and sensitive data while code is old and poorly understood by the current software engineers, this makes it more prone to unsuspecting attacks considering the highlighted potential risks of sophisticated side channel attacks while the application is running.

upvoted 1 times

1e22522 10 months, 3 weeks ago

Selected Answer: C

Should be C

upvoted 1 times