PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.

Which option meets the requirement of your team?

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance\\'s IP address and allows the application to read from the bucket without credentials.

B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.

C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.

D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Correct Answer: C

If the environment variable GOOGLE_APPLICATION_CREDENTIALS is set, ADC uses the service account key or configuration file that the variable points to. If the environment variable GOOGLE_APPLICATION_CREDENTIALS isn\\'t set, ADC uses the service account that is attached to the resource that is running your code. https://cloud.google.com/docs/authentication/ production#passing_the_path_to_the_service _account_key_in_code

QUESTION 2

Your security team uses encryption keys to ensure confidentiality of user data. You want to establish a process to reduce the impact of a potentially compromised symmetric encryption key in Cloud Key Management Service (Cloud KMS).

Which steps should your team take before an incident occurs? (Choose two.)

A. Disable and revoke access to compromised keys.

B. Enable automatic key version rotation on a regular schedule.

C. Manually rotate key versions on an ad hoc schedule.

D. Limit the number of messages encrypted with each key version.

E. Disable the Cloud KMS API.

Correct Answer: BD

As per document "Limiting the number of messages encrypted with the same key version helps prevent attacks enabled by cryptanalysis." https://cloud.google.com/kms/docs/key-rotation

QUESTION 3

Which Identity-Aware Proxy role should you grant to an Identity and Access Management (IAM) user to access HTTPS resources?

A. Security Reviewer

B. lAP-Secured Tunnel User

C. lAP-Secured Web App User

D. Service Broker Operator

Correct Answer: C

IAP-Secured Tunnel User: Grants access to tunnel resources that use IAP. IAP-Secured Web App User:

Access HTTPS resources which use Identity-Aware Proxy, Grants access to App Engine, Cloud Run, and Compute Engine resources. https://cloud.google.com/iap/docs/managing-access#roles

QUESTION 4

Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements: Scans must run at least once per week Must be able to detect cross-site scripting vulnerabilities Must be able to authenticate using Google accounts Which solution should you use?

A. Google Cloud Armor

B. Web Security Scanner

C. Security Health Analytics

D. Container Threat Detection

Correct Answer: B

Reference: https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner- overview

Web Security Scanner identifies security vulnerabilities in your App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications. https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

QUESTION 5

A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time.

What should you do?

A. Use Resource Manager on the organization level.

B. Use Forseti Security to automate inventory snapshots.

C. Use Stackdriver to create a dashboard across all projects.

D. Use Security Command Center to view all assets across the organization.

Correct Answer: B

Only Forseti security can have both \\'past\\' and \\'present\\' (i.e. historical) records of the resources. https://forsetisecurity.org/about/