PROFESSIONAL-CLOUD-SECURITY-ENGINEER$^{Q\&As}$

Professional Cloud Security Engineer

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

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

QUESTION 1

You are deploying regulated workloads on Google Cloud. The regulation has data residency and data access requirements. It also requires that support is provided from the same geographical location as where the data resides. What should you do?

A. Enable Access Transparency Logging.

B. Deploy Assured Workloads.

C. Deploy resources only to regions permitted by data residency requirements.

D. Use Data Access logging and Access Transparency logging to confirm that no users are accessing data from another region.

Correct Answer: B

The correct answer is B. Deploy Assured Workloads.

Assured Workloads for Google Cloud allows you to deploy regulated workloads with data residency, access, and support requirements. It helps you configure your environment in a manner that aligns with specific compliance frameworks and standards.

QUESTION 2

You are working with a client who plans to migrate their data to Google Cloud. You are responsible for recommending an encryption service to manage their encrypted keys. You have the following requirements:

The master key must be rotated at least once every 45 days. The solution that stores the master key must be FIPS 140-2 Level 3 validated. The master key must be stored in multiple regions within the US for redundancy.

Which solution meets these requirements?

A. Customer-managed encryption keys with Cloud Key Management Service

B. Customer-managed encryption keys with Cloud HSM

C. Customer-supplied encryption keys

D. Google-managed encryption keys

Correct Answer: B

https://cloud.google.com/docs/security/key-management-deep-dive https://cloud.google.com/kms/docs/faq

QUESTION 3

Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity.

What should you do?

A. Use Security Health Analytics to determine user activity.

B. Use the Cloud Monitoring console to filter audit logs by user.

C. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.

D. Use the Logs Explorer to search for user activity.

Correct Answer: D

We use audit logs by searching the Service Account and checking activities in the past 2 months. (the user identity will not be seen since he used the SA identity but we can make correlations based on ip address, working hour, etc.)

QUESTION 4

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.

How should your team design this network?

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.

B. Create a different subnet for the frontend application and database to ensure network isolation.

C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.

D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Correct Answer: A

"However, even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped"

QUESTION 5

A company is using Google Kubernetes Engine (GKE) with container images of a mission-critical application. The company wants to scan the images for known security issues and securely share the report with the security team without exposing them outside Google Cloud.

What should you do?

A. 1. Enable Container Threat Detection in the Security Command Center Premium tier.

2.

Upgrade all clusters that are not on a supported version of GKE to the latest possible GKE version.

3.

View and share the results from the Security Command Center.

B. 1. Use an open source tool in Cloud Build to scan the images.

2.

Upload reports to publicly accessible buckets in Cloud Storage by using gsutil.

3.

Share the scan report link with your security department.

C. 1. Enable vulnerability scanning in the Artifact Registry settings.

2.

Use Cloud Build to build the images.

3.

Push the images to the Artifact Registry for automatic scanning.

4.

View the reports in the Artifact Registry.

D. 1. Get a GitHub subscription.

2.

Build the images in Cloud Build and store them in GitHub for automatic scanning.

3.

Download the report from GitHub and share with the Security Team.

Correct Answer: C