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

You work for an organization in a regulated industry that has strict data protection requirements. The organization backs up their data in the cloud. To comply with data privacy regulations, this data can only be stored for a specific length of

time and must be deleted after this specific period.

You want to automate the compliance with this regulation while minimizing storage costs.

What should you do?

A. Store the data in a persistent disk, and delete the disk at expiration time.

B. Store the data in a Cloud Bigtable table, and set an expiration time on the column families.

C. Store the data in a BigQuery table, and set the table\\'s expiration time.

D. Store the data in a Cloud Storage bucket, and configure the bucket\\'s Object Lifecycle Management feature.

Correct Answer: D

To miminize costs, it\\'s always GCS even though BQ comes as a close 2nd. But, since the question did not specify what kind of data it is (raw files vs tabular data), it is safe to assume GCS is the preferred option with LifeCycle enablement.

QUESTION 2

You are migrating an on-premises data warehouse to BigQuery Cloud SQL, and Cloud Storage. You need to configure security services in the data warehouse. Your company compliance policies mandate that the data warehouse must:

1.

Protect data at rest with full lifecycle management on cryptographic keys

2.

Implement a separate key management provider from data management

3.

Provide visibility into all encryption key requests

What services should be included in the data warehouse implementation?

Choose 2 answers

A. Customer-managed encryption keys

B. Customer-Supplied Encryption Keys

C. Key Access Justifications

D. Access Transparency and Approval

E. Cloud External Key Manager

Correct Answer: CE

QUESTION 3

Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements. What should you do?

A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.

B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository Verify that the image is not deprecated.

C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.

D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: A

QUESTION 4

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization\\'s risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

A. Ensure that firewall rules are in place to meet the required controls.

B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.

C. Network security is a built-in solution and Google\\'s Cloud responsibility for SaaS products like G Suite.

D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Correct Answer: C

https://gsuite.google.com/learn-more/security/security-whitepaper/page-1.html

Shared responsibility "Security of the Cloud" -GCP is responsible for protecting the infrastructure that runs all of the services offered in the GCP Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run GCP Cloud services.

QUESTION 5

You\\'re developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two

main requirements:

Least-privilege access must be enforced at all times. The DevOps team must be able to access the required resources only during the deployment issue.

How should you grant access while following Google-recommended best practices?

A. Assign the Project Viewer Identity and Access Management (1AM) role to the DevOps team.

B. Create a custom 1AM role with limited list/view permissions, and assign it to the DevOps team.

C. Create a service account, and grant it the Project Owner 1AM role. Give the Service Account User Role on this service account to the DevOps team.

D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Correct Answer: B