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.certbus.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 are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.

What should you do?

A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.

B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.

C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.

D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

Correct Answer: A

https://cloud.google.com/vpc-service-controls/docs/overview#isolate

QUESTION 2

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.

How should this be accomplished?

A. Create a firewall rule to block internet traffic from the VM.

B. Provision a NAT Gateway to access the Cloud Storage API endpoint.

C. Enable Private Google Access on the VPC.

D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Correct Answer: C

https://cloud.google.com/vpc/docs/private-google-access

QUESTION 3

You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud. Which options should you utilize to accomplish this? (Choose two.)

A. External Key Manager

B. Customer-supplied encryption keys

C. Hardware Security Module

D. Confidential Computing and Istio

E. Client-side encryption

Correct Answer: DE

Google Cloud customers with additional requirements for encryption of data over WAN can choose to implement further protections for data as it moves from a user to an application, or virtual machine to virtual machine. These protections include IPSec tunnels, Gmail S/MIME, managed SSL certificates, and Istio.
https://cloud.google.com/docs/security/encryption-in-transit

QUESTION 4

Your organization recently activated the Security Command Center {SCO standard tier. There are a few Cloud Storage buckets that were accidentally made accessible to the public. You need to investigate the impact of the incident and remediate it.

What should you do?

A. 1 Remove the Identity and Access Management (IAM) granting access to allusers from the buckets 2 Apply the organization policy storage. unifromBucketLevelAccess to prevent regressions 3 Query the data access logs to report on unauthorized access

B. 1 Change bucket permissions to limit access 2 Query the data access audit logs for any unauthorized access to the buckets 3 After the misconfiguration is corrected mute the finding in the Security Command Center

C. 1 Change permissions to limit access for authorized users 2 Enforce a VPC Service Controls perimeter around all the production projects to immediately stop any unauthorized access 3 Review the administrator activity audit logs to report on any unauthorized access

D. 1 Change the bucket permissions to limit access 2 Query the buckets usage logs to report on unauthorized access to the data 3 Enforce the organization policy storage.publicAccessPrevention to avoid regressions

Correct Answer: D

QUESTION 5

Your organization uses the top-tier folder to separate application environments (prod and dev). The developers need to see all application development audit logs but they are not permitted to review production logs. Your security team can review all logs in production and development environments. You must grant Identity and Access Management (1AM) roles at the right resource level tor the developers and security team while you ensure least privilege.

What should you do?

A. 1 Grant logging, viewer rote to the security team at the organization resource level. 2 Grant logging, viewer rote to the developer team at the folder resource level that contains all the dev projects.

B. 1 Grant logging. viewer rote to the security team at the organization resource level. 2 Grant logging. admin role to the developer team at the organization resource level.

C. 1 Grant logging.admin role to the security team at the organization resource level. 2 Grant logging. viewer rote to the developer team at the folder resource level that contains all the dev projects.

D. 1 Grant logging.admin role to the security team at the organization resource level. 2 Grant logging.admin role to the developer team at the organization resource level.

Correct Answer: A

QUESTION 6

Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.

What should you do?

A. Temporarily disable authentication on the Cloud Storage bucket.

B. Use the undelete command to recover the deleted service account.

C. Create a new service account with the same name as the deleted service account.

D. Update the permissions of another existing service account and supply those credentials to the applications.

Correct Answer: B

https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts/undelete
https://cloud.google.com/iam/docs/creating-managing-service-accounts#undeleting_a_service_account

QUESTION 7

You manage a fleet of virtual machines (VMs) in your organization. You have encountered issues with lack of patching in many VMs. You need to automate regular patching in your VMs and view the patch management data across multiple projects.

What should you do? (Choose two.)

A. View patch management data in VM Manager by using OS patch management.

B. View patch management data in Artifact Registry.

C. View patch management data in a Security Command Center dashboard.

D. Deploy patches with Security Command Genter by using Rapid Vulnerability Detection.

E. Deploy patches with VM Manager by using OS patch management.

Correct Answer: AE

A. View patch management data in VM Manager by using OS patch management. VM Manager\\'s OS patch management feature allows you to view patch compliance and deployment data across multiple projects.

E. Deploy patches with VM Manager by using OS patch management. VM Manager\\'s OS patch management feature also allows you to automate the deployment of patches to your VMs.

QUESTION 8

You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

A. Add the host project containing the Shared VPC to the service perimeter.

B. Add the service project where the Compute Engine instances reside to the service perimeter.

C. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.

D. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.

Correct Answer: A

https://cloud.google.com/vpc-service-controls/docs/service-perimeters#secure-google-managed-resources If you\\'re using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC.

QUESTION 9

Your organization s record data exists in Cloud Storage. You must retain all record data for at least seven years This policy must be permanent. What should you do?

A. 1 Identify buckets with record data 2 Apply a retention policy and set it to retain for seven years 3 Monitor the bucket by using log-based alerts to ensure that no modifications to the retention policy occurs

B. 1 Identify buckets with record data 2 Apply a retention policy and set it to retain for seven years 3 Remove any Identity and Access Management (IAM) roles that contain the storage buckets update permission

C. 1 Identify buckets with record data 2 Enable the bucket policy only to ensure that data is retained 3 Enable bucket lock

D. 1 Identify buckets with record data 2 Apply a retention policy and set it to retain for seven years 3 Enable bucket lock

Correct Answer: D

QUESTION 10

You are designing a new governance model for your organization\\'s secrets that are stored in Secret Manager. Currently, secrets for Production and Non-Production applications are stored and accessed using service accounts. Your proposed solution must:

Provide granular access to secrets

Give you control over the rotation schedules for the encryption keys that wrap your secrets

Maintain environment separation

Provide ease of management

Which approach should you take?

A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

2.

Enforce access control to secrets using project-level identity and Access Management (IAM) bindings.

3.

Use customer-managed encryption keys to encrypt secrets.

B. 1. Use a single Google Cloud project to store both Production and Non-Production secrets.

2.

Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings.

3.

Use Google-managed encryption keys to encrypt secrets.

C. 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

2.

Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings.

3.

Use Google-managed encryption keys to encrypt secrets.

D. 1. Use a single Google Cloud project to store both Production and Non-Production secrets.

2.

Enforce access control to secrets using project-level Identity and Access Management (IAM) bindings.

3.

Use customer-managed encryption keys to encrypt secrets.

Correct Answer: A

Provide granular access to secrets: 2.Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. Give you control over the rotation schedules for the encryption keys that wrap your secrets: 3. Use customer-managed encryption keys to encrypt secrets. Maintain environment separation: 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

QUESTION 11

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 12

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.

Which two strategies should your team use to meet these requirements? (Choose two.)

A. Configure Private Google Access on the Compute Engine subnet

B. Avoid assigning public IP addresses to the Compute Engine cluster.

C. Make sure that the Compute Engine cluster is running on a separate subnet.

D. Turn off IP forwarding on the Compute Engine instances in the cluster.

E. Configure a Cloud NAT gateway.

Correct Answer: AB

QUESTION 13

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer\\'s internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP\\'s native SYN flood protection.

Which product should be used to meet these requirements?

A. Cloud Armor

B. VPC Firewall Rules

C. Cloud Identity and Access Management

D. Cloud CDN

Correct Answer: A

Reference: https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors- new-wafcapabilities

QUESTION 14

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.

B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.

C. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.

D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.

Correct Answer: A

Reference: https://cloud.google.com/kms/docs/envelope-encryption Envelope Encryption: https://cloud.google.com/kms/docs/envelope-encryption Here are best practices for managing DEKs:

1.

Generate DEKs locally.

2.

When stored, always ensure DEKs are encrypted at rest.

3.

For easy access, store the DEK near the data that it encrypts.

The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.

Here are best practices for managing KEKs:

1.

Store KEKs centrally. (KMS)

2.

Set the granularity of the DEKs they encrypt based on their use case.

For example, consider a workload that requires multiple DEKs to encrypt the workload\\'s data chunks.

You could use a single KEK to wrap all DEKs that are responsible for that workload\\'s encryption.

Rotate keys regularly, and also after a suspected incident.

QUESTION 15

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?

A. Use Cloud Build to build the container images.

B. Build small containers using small base images.

C. Delete non-used versions from Container Registry.

D. Use a Continuous Delivery tool to deploy the application.

Correct Answer: B

Small containers usually have a smaller attack surface as compared to containers that use large base images. https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build-small- container-images