Free Questions for Professional-Cloud-Security-Engineer by certsdeals

Shared by Hahn on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

Options:

A- Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.

B- Enable the constraints/storage.publicAccessPrevention constraint at the organization level.

C- Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.

D- Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Answer:

B

Question 2

Question Type: MultipleChoice

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.)

Options:

A- External Key Manager

B- Customer-supplied encryption keys

C- Hardware Security Module

D- Confidential Computing and Istio

E- Client-side encryption

Answer:

A, B

Question 3

Question Type: MultipleChoice

You are working with protected health information (PHI) for an electronic health record system. The privacy officer is concerned that sensitive data is stored in the analytics system. You are tasked with anonymizing the sensitive data in a way that is not reversible. Also, the anonymized data should not preserve the character set and length. Which Google Cloud solution should you use?

Options:

A- Cloud Data Loss Prevention with deterministic encryption using AES-SIV

B- Cloud Data Loss Prevention with format-preserving encryption

C- Cloud Data Loss Prevention with cryptographic hashing

D- Cloud Data Loss Prevention with Cloud Key Management Service wrapped cryptographic keys

Answer:

D

Question 4

Question Type: MultipleChoice

You need to connect your organization's on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?

Options:

A- 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.
2. Configure private access using the restricted googleapis.com domains in on-premises DNS configurations.

B- 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.
2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.

C- 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.
2. Configure private access for both VPC subnets.

D- 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.
2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.

Answer:

C

Question 5

Question Type: MultipleChoice

Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that meets the following requirements:

Only allows communication between the Web and App tiers.

Enforces consistent network security when autoscaling the Web and App tiers.

Prevents Compute Engine Instance Admins from altering network traffic.

What should you do?

Options:

A- 1. Configure all running Web and App servers with respective network tags.
2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.

B- 1. Configure all running Web and App servers with respective service accounts.
2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

C- 1. Re-deploy the Web and App servers with instance templates configured with respective network tags.
2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.

D- 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts.

2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

Answer:

A

Question 6

Question Type: MultipleChoice

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your Google Cloud VPCs based on packet header information. However, you want the capability to explore network flows and their payload to aid investigations. Which Google Cloud product should you use?

Options:

A- Marketplace IDS

B- VPC Flow Logs

C- VPC Service Controls logs

D- Packet Mirroring

E- Google Cloud Armor Deep Packet Inspection

Answer:

D

Question 7

Question Type: MultipleChoice

You need to enable VPC Service Controls and allow changes to perimeters in existing environments without preventing access to resources. Which VPC Service Controls mode should you use?

Options:

A- Cloud Run

B- Native

C- Enforced

D- Dry run

Answer:

D

Question 8

Question Type: MultipleChoice

You are a member of your company's security team. You have been asked to reduce your Linux bastion host external attack surface by removing all public IP addresses. Site Reliability Engineers (SREs) require access to the bastion host from public locations so they can access the internal VPC while off-site. How should you enable this access?

Options:

A- Implement Cloud VPN for the region where the bastion host lives.

B- Implement OS Login with 2-step verification for the bastion host.

C- Implement Identity-Aware Proxy TCP forwarding for the bastion host.

D- Implement Google Cloud Armor in front of the bastion host.

Answer:

C