Free Professional-Cloud-Security-Engineer Braindumps & Professional-Cloud-Security-Engineer New Braindumps

DOWNLOAD the newest Exams4Collection Professional-Cloud-Security-Engineer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1x35-i2XgicEf_zVylTz_JKUDEV-8szjq

Exams4Collection owns the most popular reputation in this field by providing not only the best ever Professional-Cloud-Security-Engineer study guide but also the most efficient customers' servers. We can lead you the best and the fastest way to reach for the Professional-Cloud-Security-Engineer certification and achieve your desired higher salary. Our Professional-Cloud-Security-Engineer Exam Preparation can improve your grade and change your states of life for our Professional-Cloud-Security-Engineer Learning Questions are the accumulation of professional knowledge. You will be more successful with our Professional-Cloud-Security-Engineer braindump.

Google Professional-Cloud-Security-Engineer Exam is a certification test that measures the candidate's ability to design and implement secure Google Cloud Platform solutions. Professional-Cloud-Security-Engineer exam is designed to test the candidate's knowledge and expertise in cloud security, data protection, compliance, and network security. Professional-Cloud-Security-Engineer Exam is intended for cloud security professionals and engineers who are responsible for securing data and applications on Google Cloud Platform.

>> Free Professional-Cloud-Security-Engineer Braindumps <<

Professional-Cloud-Security-Engineer New Braindumps - Latest Professional-Cloud-Security-Engineer Exam Pattern

We are popular not only because our outstanding Professional-Cloud-Security-Engineer practice dumps, but also for our well-praised after-sales service. After purchasing our Professional-Cloud-Security-Engineer practice materials, the free updates will be sent to your mailbox for one year long if our experts make any of our Professional-Cloud-Security-Engineer Guide materials. They are also easily understood by exam candidates.Our Professional-Cloud-Security-Engineer actual exam can secedes you from tremendous materials with least time and quickest pace based on your own drive and practice to win.

The Professional-Cloud-Security-Engineer exam measures the candidate's ability to secure cloud infrastructure, data, and applications using various Google Cloud Platform services. Professional-Cloud-Security-Engineer exam covers topics such as configuring access controls, managing network security, implementing data encryption, and designing secure application architectures. Professional-Cloud-Security-Engineer exam also evaluates the candidate's understanding of compliance and regulatory requirements and their ability to implement security policies and procedures to meet these requirements.

Google Professional-Cloud-Security-Engineer Exam is a certification offered by Google for professionals who are responsible for ensuring the security of data and infrastructure in the cloud. Professional-Cloud-Security-Engineer exam is designed to test the candidate’s knowledge and skills in implementing security controls and maintaining compliance in the Google Cloud Platform (GCP). Google Cloud Certified - Professional Cloud Security Engineer Exam certification is intended for security engineers, security architects, and other professionals who have experience in cloud security.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q75-Q80):

NEW QUESTION # 75
You are implementing data protection by design and in accordance with GDPR requirements. As part of design reviews, you are told that you need to manage the encryption key for a solution that includes workloads for Compute Engine, Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub. Which option should you choose for this implementation?

- A. Customer-supplied encryption keys
- B. Customer-managed encryption keys
- C. Cloud External Key Manager
- D. Google default encryption

Answer: B

Explanation:
To comply with GDPR requirements and manage encryption keys for workloads across multiple Google Cloud services, customer-managed encryption keys (CMEK) offer a suitable solution.
* Customer-managed encryption keys (B):
* CMEK allows you to create and manage encryption keys using Google Cloud Key Management Service (KMS). You maintain full control over the key lifecycle, including key rotation and destruction.
* CMEK can be used with various Google Cloud services, such as Compute Engine, Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub, ensuring consistent and compliant encryption across your environment.
* Using CMEK, you can implement data protection by design, aligning with GDPR requirements by ensuring that encryption keys are appropriately managed and secured.
References
* Customer-Managed Encryption Keys Documentation
* Encryption at Rest in Google Cloud

NEW QUESTION # 76
What is the most effective way to automatically scan environment variables in Cloud Functions for sensitive data and create security findings?

- A. Use Sensitive Data Protection to scan the environment variables multiple times per day. and create a finding in Security Command Center if secrets are discovered.
- B. Implement regular peer reviews to assess the environment variables and identify secrets in your Cloud Functions. Raise a security incident if secrets are discovered.
- C. Implement a Cloud Function that scans the environment variables multiple times a day. and creates a finding in Security Command Center if secrets are discovered.
- D. Integrate dynamic application security testing into the CI/CD pipeline that scans the application code for the Cloud Functions. Fail the build process if secrets are discovered.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The problem is the detection of secrets (sensitive data patterns) within the environment variables of deployed resources (Cloud Functions) in a timely, automated manner.
Sensitive Data Protection (SDP), formerly Cloud DLP, is the purpose-built Google Cloud service for scanning and classifying sensitive data patterns. It can be configured to scan code, configuration, or environment variables and integrate its findings directly with Security Command Center (SCC).
Extracts:
"Sensitive Data Protection provides highly configurable, automated detection of sensitive data, including API keys, passwords, and other credentials, using both pre-built and custom infoTypes." (Source 8.1)
"SDP can be integrated with Cloud Functions and other resource configurations to scan environment variables or configuration files for secrets. Violations can be automatically routed to Security Command Center as findings." (Source 8.2) Option D (DAST) scans the application code or running application logic, but the requirement specifies the secrets are in the environment variables, which are part of the configuration/deployment metadata, making SDP the correct detection tool.

NEW QUESTION # 77
Which two security characteristics are related to the use of VPC peering to connect two VPC networks?
(Choose two.)

- A. Central management of routes, firewalls, and VPNs for peered networks
- B. Non-transitive peered networks; where only directly peered networks can communicate
- C. Ability to share specific subnets across peered networks
- D. Ability to peer networks that belong to different Google Cloud Platform organizations
- E. Firewall rules that can be created with a tag from one peered network to another peered network

Answer: B,D

Explanation:
Explanation
https://cloud.google.com/vpc/docs/vpc-peering#key_properties

NEW QUESTION # 78
You are responsible for managing your company's identities in Google Cloud. Your company enforces 2-Step Verification (2SV) for all users. You need to reset a user's access, but the user lost their second factor for 2SV.
You want to minimize risk. What should you do?

- A. On the Google Admin console, select the appropriate user account, and temporarily disable 2SV for this account Ask the user to update their second factor, and then re-enable 2SV for this account.
- B. On the Google Admin console, temporarily disable the 2SV requirements for all users. Ask the user to log in and add their new second factor to their account. Re-enable the 2SV requirement for all users.
- C. On the Google Admin console, select the appropriate user account, and generate a backup code to allow the user to sign in. Ask the user to update their second factor.
- D. On the Google Admin console, use a super administrator account to reset the user account's credentials. Ask the user to update their credentials after their first login.

Answer: C

Explanation:
Explanation
https://support.google.com/a/answer/9176734
Use backup codes for account recovery If you need to recover an account, use backup codes. Accounts are still protected by 2-Step Verification, and backup codes are easy to generate.

NEW QUESTION # 79
You need to audit the network segmentation for your Google Cloud footprint. You currently operate Production and Non-Production infrastructure-as-a-service (IaaS) environments. All your VM instances are deployed without any service account customization.
After observing the traffic in your custom network, you notice that all instances can communicate freely - despite tag-based VPC firewall rules in place to segment traffic properly - with a priority of 1000. What are the most likely reasons for this behavior?

- A. All VM instances are configured with the same network route.
- B. All VM instances are residing in the same network subnet.
- C. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 1001.
- D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999.
- E. All VM instances are missing the respective network tags.

Answer: D

Explanation:
* Firewall Rule Analysis: Analyze the existing VPC firewall rules to identify any rules that might allow traffic between VM instances based on the same service account.
* Priority Check: Check the priority of these rules. A rule with a priority lower than 1000 (such as 999) will take precedence over your tag-based rules.
* Service Account Configuration: Since your VM instances are deployed without any service account customization, they are likely

using the default service account. A firewall rule allowing traffic between instances using this default service account will override the tag-based rules if it has a higher priority.
* Testing and Validation: Disable or adjust the priority of the rule with priority 999 to test if the tag- based segmentation works correctly. Validate that the traffic is segmented according to your intended configuration. References:
* Google Cloud - VPC Firewall Rules
* Google Cloud - Service Accounts

NEW QUESTION # 80
.....

https://drive.google.com/open?id=1x35-i2XgicEf_zVyITz_JKUDEV-8szjq