Top Exam Professional-Cloud-Security-Engineer Course - How to Prepare for Google Professional-Cloud-Security-Engineer In Short Time

P.S. Free & New Professional-Cloud-Security-Engineer dumps are available on Google Drive shared by VCEPrep: https://drive.google.com/open?id=1EBcZsW3LbzS0eNWJuo9SmXnqA9U3x3pC

We believe that every customer pays most attention to quality when he is shopping. Only high-quality goods can meet the needs of every customer better. And our Professional-Cloud-Security-Engineer study materials have such high quality, because its hit rate of test questions is extremely high. Perhaps you will find in the examination that a lot of questions you have seen many times in our Professional-Cloud-Security-Engineer Study Materials. In addition, the passing rate is the best test for quality of study materials. And we can be very proud to tell you that the passing rate of our Professional-Cloud-Security-Engineer study materials is almost 100 %.

The Professional-Cloud-Security-Engineer Exam is a challenging exam that requires the candidate to have a deep understanding of cloud security concepts and hands-on experience with Google Cloud Platform services. Professional-Cloud-Security-Engineer exam consists of multiple-choice and multiple-select questions and requires the candidate to demonstrate their ability to solve real-world security problems. Passing Professional-Cloud-Security-Engineer exam demonstrates the candidate's proficiency in cloud security and validates their ability to design and implement secure cloud solutions on the Google Cloud Platform.

Career Prospects

The specialists with the Google Professional Cloud Security Engineer certificate can take up various positions and achieve success in the industry. Thus, they can go for the following options: a Cloud Security Engineer, a Security Engineer, a Virtual Infrastructure Administrator, a Cloud Support Engineer, and a Cloud Security Operations Engineer. The salary outlook for these job roles is an average of $102,000 per annum.

>> Exam Professional-Cloud-Security-Engineer Course <<

Study Google Professional-Cloud-Security-Engineer Demo | Braindumps Professional-Cloud-Security-Engineer Pdf

For some difficult points of the Professional-Cloud-Security-Engineer exam questions which you may feel hard to understand or easy to confuse for too similar with the others. In order to help you memorize the Professional-Cloud-Security-Engineer guide materials better, we have detailed explanations of the difficult questions such as illustration, charts and referring website. Every year some knowledge of the Professional-Cloud-Security-Engineer Practice Braindumps is reoccurring over and over. You must ensure that you master them completely.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q104-Q109):

NEW QUESTION # 104
Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/ owner). The organization contains thousands of Google Cloud Projects Security Command Center Premium has surfaced multiple cpen_myscl_port findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.
What should you do?

- A. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.
- B. Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.
- C. Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.
- D. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

Answer: B

NEW QUESTION # 105
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?

- A. Cloud Data Loss Prevention with format-preserving encryption
- B. Cloud Data Loss Prevention with cryptographic hashing
- C. Cloud Data Loss Prevention with Cloud Key Management Service wrapped cryptographic keys
- D. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Answer: B

Explanation:
* Use Cloud Data Loss Prevention (DLP) with cryptographic hashing:
* Cloud DLP allows you to de-identify sensitive data using several techniques, including cryptographic hashing.
* Choose a suitable hashing algorithm like SHA-256 for non-reversible anonymization.
* This method converts the original data into a fixed-length hash that does not preserve the original data's format or character set.
* Set up a Cloud DLP job to scan your data sources, identify PHI, and apply the cryptographic hashing transformation.
References:
* Cloud DLP Overview
* De-identification with Cloud DLP

NEW QUESTION # 106
You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project.
What should you do?

- A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted projects as the exceptions in a deny operation.
- B. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.
- C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
- D. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

Answer: D

Explanation:
Objective: You want to limit the images that can be used as the source for boot disks to a set of images stored in a dedicated project.
Solution: Use the Organization Policy Service.
Steps:
Step 1: Open the Google Cloud Console.
Step 2: Navigate to the Organization Policies page.
Step 3: Create a new policy by clicking on "Create Policy".

Step 4: Select the constraint compute.trustedimageProjects.
Step 5: Set the policy to ALLOW and specify the project ID where the trusted images are stored in the whitelist.
Step 6: Save and apply the policy.
By creating a compute.trustedimageProjects constraint at the organization level and specifying the trusted project in the allow list, you ensure that only images from this project can be used for boot disks across the organization.
Reference:
GCP Organization Policy Service Documentation
Compute Trusted Image Projects Constraint

NEW QUESTION # 107
A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite.
How should you best advise the Systems Engineer to proceed with the least disruption?

- A. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.
- B. Register a new domain name, and use that for the new Cloud Identity domain.
- C. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
- D. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.

Answer: A

Explanation:
Since the domain is already being used by G Suite, the best course of action is to minimize disruption by discovering any existing uses of Google-managed services. Collaborate with the existing Super Administrator to align the setup with the company's requirements.
Step-by-Step:
Identify Existing Usage: Have the customer's management identify all current uses of the domain within Google-managed services.
Collaboration: Work closely with the existing Super Administrator of the domain.
Provision Required Accounts: Ask the Super Administrator to provision necessary accounts and permissions for the data science manager or other relevant personnel.
Integrate SAML IdP: Ensure that the existing domain integrates with the company's SAML 2.0 IdP for user authentication.
Set Up Cloud Identity: Configure Cloud Identity under the guidance of the Super Administrator without disrupting current services.
Reference:
Google Cloud Identity Administration
Google Support for Domain Issues

NEW QUESTION # 108
Your development team is launching a new application. The new application has a microservices architecture on Compute Engine instances and serverless components, including Cloud Functions. This application will process financial transactions that require temporary, highly sensitive data in memory. You need to secure data in use during computations with a focus on minimizing the risk of unauthorized access to memory for this financial application. What should you do?

- A. Store all sensitive data during processing in Cloud Storage by using customer-managed encryption keys (CMEK), and set strict bucket-level permissions.
- B. Enable Confidential VM instances for Compute Engine, and ensure that relevant Cloud Functions can leverage hardware-based memory isolation.
- C. Use data masking and tokenization techniques on sensitive financial data fields throughout the application and the application's data processing workflows.
- D. Use the Cloud Data Loss Prevention (Cloud DLP) API to scan and mask sensitive data before feeding the data into any compute environment.

Answer: B

Explanation:
Confidential VMs: Using Confidential VMs provides a strong security boundary around the memory of the VM instances, protecting

sensitive data from unauthorized access, even if the VM is compromised.
Hardware-Based Memory Isolation: Leveraging hardware-based memory isolation ensures that the data within the VM's memory is protected by hardware-enforced mechanisms, making it significantly more difficult for attackers to access.
Comprehensive Protection: This approach provides a comprehensive solution for securing data in use, as it combines both software-based (Confidential VMs) and hardware-based (memory isolation) protections.

NEW QUESTION # 109
.....

The Professional-Cloud-Security-Engineer Exam is one of the best platforms that have been helping the Google Professional-Cloud-Security-Engineer exam candidates in their preparation. Several Google Professional-Cloud-Security-Engineer exam candidates have already passed their Google Cloud Certified - Professional Cloud Security Engineer Exam exam with good scores. They all used the Exams. Professional-Cloud-Security-Engineer Exam Questions and got success in the final Google Professional-Cloud-Security-Engineer exam easily.

What's more, part of that VCEPrep Professional-Cloud-Security-Engineer dumps now are free: https://drive.google.com/open?id=1EBcZsW3LbzS0eNWJuo9SmXnqA9U3x3pC