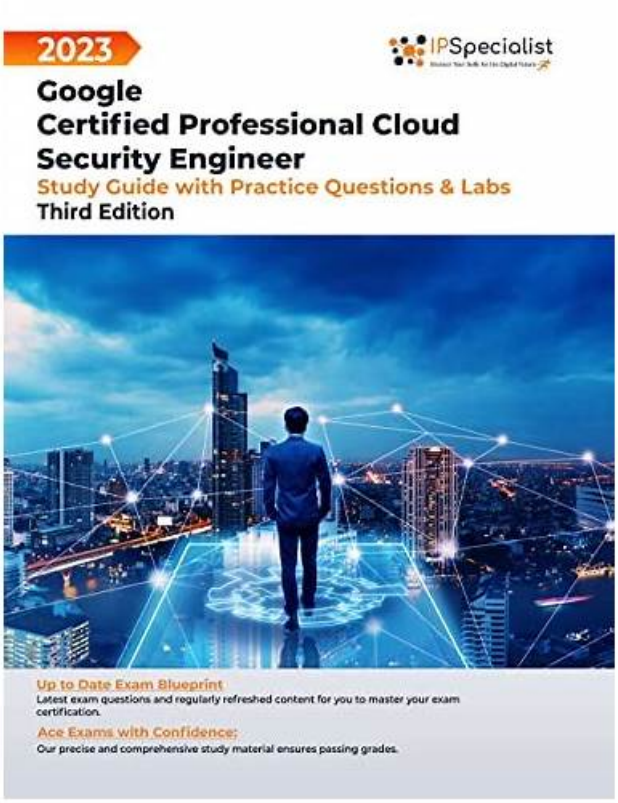
Valid Braindumps Google Professional-Cloud-Security-Engineer Ebook, Professional-Cloud-Security-Engineer Free Download



2026 Latest TestSimulate Professional-Cloud-Security-Engineer PDF Dumps and Professional-Cloud-Security-Engineer Exam Engine Free Share: https://drive.google.com/open?id=1uUFaHZ6fzETyKTA3KE5dnC9P38ORyncJ

The study material to get Google Cloud Certified - Professional Cloud Security Engineer Exam should be according to individual's learning style and experience. Real Google Professional-Cloud-Security-Engineer Exam Questions certification makes you more dedicated and professional as it will provide you complete information required to work within a professional working environment. These questions will familiarize you with the Professional-Cloud-Security-Engineer Exam Format and the content that will be covered in the actual test. You will not get a passing score if you rely on outdated practice questions.

Google Cloud Certified Professional Cloud Security Engineer exam is a globally recognized certification that validates an individual's knowledge and expertise in securing applications, data, and infrastructure on the Google Cloud Platform. Professional-Cloud-Security-Engineer Exam is designed to test the candidate's knowledge of Google Cloud Platform security features, compliance, and best practices for securing applications and infrastructure.

>> Valid Braindumps Google Professional-Cloud-Security-Engineer Ebook <<

Prepare for the Google Exam on the Go with Professional-Cloud-Security-Engineer PDF Dumps

Google Cloud Certified - Professional Cloud Security Engineer Exam (Professional-Cloud-Security-Engineer) practice exam went through real-world testing with feedback from more than 90,000 global professionals before reaching its latest form. The Google Professional-Cloud-Security-Engineer Exam Dumps are similar to real exam questions. Our Professional-Cloud-Security-Engineer practice test TestSimulate is suitable for computer users with a Windows operating system.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q136-Q141):

NEW QUESTION # 136
You have been tasked with configuring Security Command Center for your organization's Google Cloud environment. Your security team needs to receive alerts of potential crypto mining in the organization's compute environment and alerts for common Google Cloud misconfigurations that impact security. Which Security Command Center features should you use to configure these alerts? (Choose two.)

- A. Container Threat Detection
- B. Event Threat Detection
- C. Cloud Data Loss Prevention
- D. Security Health Analytics
- E. Google Cloud Armor

Answer: B,D

Explanation:
Security Command Center (SCC) in Google Cloud provides several features to help organizations detect and respond to security threats and misconfigurations.
Event Threat Detection: This feature continuously monitors and analyzes system logs to detect potential threats such as crypto mining. It uses machine learning and threat intelligence to identify suspicious activities and generate alerts.
Security Health Analytics: This feature helps identify common misconfigurations and compliance violations that could impact security. It provides visibility into security posture and helps remediate issues related to misconfigurations in your Google Cloud environment.
By using both Event Threat Detection and Security Health Analytics, you can effectively monitor for crypto mining activities and detect common misconfigurations that could compromise security.
Reference:
Security Command Center Documentation
Event Threat Detection
Security Health Analytics

NEW QUESTION # 137
You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to-know basis to the HR team. What should you do?

- A. Perform data masking with the DLP API and store that data in BigQuery for later use.
- B. Perform data inspection with the DLP API and store that data in BigQuery for later use.
- C. Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.
- D. Perform data redaction with the DLP API and store that data in BigQuery for later use.

Answer: B

NEW QUESTION # 138
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?

- A. Dry run
- B. Native
- C. Cloud Run
- D. Enforced

Answer: A

Explanation:
Reference: https://cloud.google.com/vpc-service-controls/docs/service-perimeters In dry run mode, requests that violate the perimeter policy are not denied, only logged. Dry run mode is used to test perimeter configuration and to monitor usage of services without preventing access to resources.
https://cloud.google.com/vpc-service-controls/docs/dry-run-mode

NEW QUESTION # 139
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 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: C

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 # 140
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 project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
- C. In Resource Manager, edit the organization permissions. Add the project ID 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.
References:
* GCP Organization Policy Service Documentation
* Compute Trusted Image Projects Constraint

NEW QUESTION # 141

......

Customers of TestSimulate can claim their money back (terms and conditions apply) if they fail to pass the Professional-Cloud-Security-Engineer accreditation test despite using the product. To assess the practice material, try a free demo. Download actual Google Cloud Certified - Professional Cloud Security Engineer Exam (Professional-Cloud-Security-Engineer) questions and start upgrading your skills with TestSimulate right now!

Professional-Cloud-Security-Engineer Free Download: https://www.testsimulate.com/Professional-Cloud-Security-Engineer-study-materials.html

BTW, DOWNLOAD part of TestSimulate Professional-Cloud-Security-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1uUFaHZ6fzETyKTA3KE5dnC9P38ORyncJ