Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

NEW QUESTION 1
You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls. Which document should you review to find the information?

A. Google Cloud Platform: Customer Responsibility Matrix
B. PCI DSS Requirements and Security Assessment Procedures
C. PCI SSC Cloud Computing Guidelines
D. Product documentation for Compute Engine

Answer: C

NEW QUESTION 2
A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.
Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

Answer: C

NEW QUESTION 3
Which two implied firewall rules are defined on a VPC network? (Choose two.)

A. A rule that allows all outbound connections
B. A rule that denies all inbound connections
C. A rule that blocks all inbound port 25 connections
D. A rule that blocks all outbound connections
E. A rule that allows all inbound port 80 connections

Answer: AB

NEW QUESTION 4
A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and rotate the encryption keys.
Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)
B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)
C. Encryption by default
D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Answer: B

Explanation:
Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

NEW QUESTION 5
An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well- established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the "source of truth" directory for identities.
Which solution meets the organization's requirements?

A. Google Cloud Directory Sync (GCDS)
B. Cloud Identity
C. Security Assertion Markup Language (SAML)
D. Pub/Sub

Answer: B

NEW QUESTION 6
You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.
What should you do?

A. Query Data Access logs.
B. Query Admin Activity logs.
C. Query Access Transparency logs.
D. Query Stackdriver Monitoring Workspace.

Answer: A

NEW QUESTION 7
A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned.
What should the customer do?

A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Answer: C

NEW QUESTION 8
A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.
Which two steps should the company take to meet these requirements? (Choose two.)

A. Create a project with multiple VPC networks for each environment.
B. Create a folder for each development and production environment.
C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
D. Create an Organizational Policy constraint for each folder environment.
E. Create projects for each environment, and grant IAM rights to each engineering user.

Answer: BD

NEW QUESTION 9
For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on "in- scope" Nodes only. These Nodes can only contain the "in-scope" Pods.
How should the organization achieve this objective?

A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
D. Run all in-scope Pods in the namespace "in-scope-pci".

Answer: C

NEW QUESTION 10
A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery
What should you do?

A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Answer: D

NEW QUESTION 10
You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards.
What should you do?

A. Use multi-factor authentication for admin access to the web application.
B. Use only applications certified compliant with PA-DSS.
C. Move the cardholder data environment into a separate GCP project.
D. Use VPN for all connections between your office and cloud environments.

Answer: D

NEW QUESTION 14
When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for
review by internal or external analysts for customer service trend analysis.
Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Answer: D

Explanation:
Reference; https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION 16
A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.
What should they do?

A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

Answer: A

NEW QUESTION 19
How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.
B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Answer: C

NEW QUESTION 23
Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.
Which logging export strategy should you use to meet the requirements?

A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM projec
B. 2. Subscribe SIEM to the topic.
C. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM projec
D. 2. Process Cloud Storage objects in SIEM.
E. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM projec
F. 2. Subscribe SIEM to the topic.
G. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each projec
H. 2. Process Cloud Storage objects in SIEM.

Answer: B

NEW QUESTION 28
A company's application is deployed with a user-managed Service Account key. You want to use Google- recommended practices to rotate the key.
What should you do?

A. Open Cloud Shell and run gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT.
B. Open Cloud Shell and run gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT--key=NEW_KEY.
C. Create a new key, and use the new key in the applicatio
D. Delete the old key from the Service Account.
E. Create a new key, and use the new key in the applicatio
F. Store the old key on the system as a backup key.

Answer: C

NEW QUESTION 32
As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name.
Which cost reduction options should you recommend?

A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
D. Use FindingLimits and TimespanContfig to sample data and minimize transformation units.

Answer: C

NEW QUESTION 37
An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.
Which GCP solution should the organization use?

A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
B. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

Answer: B

NEW QUESTION 41
An organization receives an increasing number of phishing emails.
Which method should be used to protect employee credentials in this situation?

A. Multifactor Authentication
B. A strict password policy

C. Captcha on login pages
D. Encrypted emails

Answer: D

NEW QUESTION 44
A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.
How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Answer: D

NEW QUESTION 47
A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries.
Where should you export the logs?

A. BigQuery datasets
B. Cloud Storage buckets
C. StackDriver logging
D. Cloud Pub/Sub topics

Answer: C

NEW QUESTION 52
An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.
Which option meets the requirement of your team?

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Answer: C

NEW QUESTION 56
A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time.
What should you do?

A. Use Resource Manager on the organization level.
B. Use Forseti Security to automate inventory snapshots.
C. Use Stackdriver to create a dashboard across all projects.
D. Use Security Command Center to view all assets across the organization.

Answer: C

NEW QUESTION 59
A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.
Which Google Cloud Service should be used to achieve this?

A. Cloud Key Management Service
B. Cloud Data Loss Prevention API
C. BigQuery
D. Cloud Security Scanner

Answer: D

NEW QUESTION 62
You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.
What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
B. Manage the IAM permissions at the Key level.
C. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
D. Manage the IAM permissions at the KeyRing level.
E. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke
F. Manage the IAM permissions at the Key level.
G. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke

H. Manage the IAM permissions at the KeyRing level.

Answer: C

NEW QUESTION 63
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

Professional-Cloud-Security-Engineer Practice Exam Features:

* Professional-Cloud-Security-Engineer Questions and Answers Updated Frequently

* Professional-Cloud-Security-Engineer Practice Questions Verified by Expert Senior Certified Staff

* Professional-Cloud-Security-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Professional-Cloud-Security-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The Professional-Cloud-Security-Engineer Practice Test Here](#)