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
In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

A. Hardware
B. Network Security
C. Storage Encryption
D. Access Policies
E. Boot

Answer: CD

NEW QUESTION 3
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 4
Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

A. Enforce 2-factor authentication in GSuite for all users.
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
C. Provision user passwords using GSuite Password Sync.
D. Configure Cloud VPN between your private network and GCP.

Answer: D

NEW QUESTION 5
Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.
What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.
B. Compute Network User Role at the subnet level.
C. Compute Shared VPC Admin Role at the host project level.
D. Compute Shared VPC Admin Role at the service project level.

Answer: C

NEW QUESTION 6
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 7
Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection.
The networking resources will need to be controlled by the network security team.
Which type of networking design should your team use to meet these requirements?

A. Shared VPC Network with a host project and service projects
B. Grant Compute Admin role to the networking team for each engineering project

C. VPC peering between all engineering projects using a hub and spoke model
D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

Answer: A

NEW QUESTION 8
Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process.
What should you do?

A. Use the Cloud Key Management Service to manage a data encryption key (DEK).
B. Use the Cloud Key Management Service to manage a key encryption key (KEK).
C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

Answer: A

NEW QUESTION 9
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 10
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 10
A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.
How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

NEW QUESTION 11
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 16
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 17
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 22
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 25
Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer.
What type of Load Balancing should you use?

A. Network Load Balancing
B. HTTP(S) Load Balancing
C. TCP Proxy Load Balancing
D. SSL Proxy Load Balancing

Answer: D

NEW QUESTION 27
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 29
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. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
B. Register a new domain name, and use that for the new Cloud Identity domain.
C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Answer: C

NEW QUESTION 30
A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.
What technique should the institution use?

A. Use Cloud Storage as a federated Data Source.
B. Use a Cloud Hardware Security Module (Cloud HSM).
C. Customer-managed encryption keys (CMEK).
D. Customer-supplied encryption keys (CSEK).

Answer: C

NEW QUESTION 33
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 40
You are creating an internal App Engine application that needs to access a user's Google Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google recommended practices. What should you do?

A. Create a new Service account, and give all application users the role of Service Account User.
B. Create a new Service account, and add all application users to a Google Grou
C. Give this group the role of Service Account User.
D. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
E. Create a new service account, and grant it G Suite domain-wide delegatio
F. Have the application use it to impersonate the user.

Answer: A

NEW QUESTION 44
Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account.
What should you do?

A. * 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.* 3. Click Hide Matching Entrie
B. * 4. Make sure the resulting list is empty.
C. * 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.* 3. Click Show Matching Entrie
D. * 4. Make sure the resulting list is empty.
E. * 1. In BigQuery, select the related dataset.* 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
F. * 1. Go to the IAM section on the project.* 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Answer: C

NEW QUESTION 45
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 leve
B. List the trusted project as the whitelist in an allow operation.
C. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization leve
D. List the trusted projects as the exceptions in a deny operation.
E. In Resource Manager, edit the project permissions for the trusted projec
F. Add the organization as member with the role: Compute Image User.
G. In Resource Manager, edit the organization permission
H. Add the project ID as member with the role: Compute Image User.

Answer: B

NEW QUESTION 47
You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.
What should you do?

A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
D. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
E. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
F. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

Answer: B

NEW QUESTION 48
Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.
What should you do?

A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Answer: A

NEW QUESTION 52
A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator.
What should you do?

A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucke
B. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.
C. Upload the logs to both the shared bucket and the bucket only accessible by the administrato
D. Create a job trigger using the Cloud Data Loss Prevention AP
E. Configure the trigger to delete any files from theshared bucket that contain PII.
F. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
G. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is upload
H. Use Cloud Functions to capture the trigger and delete such files.

Answer: C

NEW QUESTION 56
An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.
What solution would help meet the requirements?

A. Ensure that firewall rules are in place to meet the required controls.
B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Answer: B

NEW QUESTION 59
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 60
What are the steps to encrypt data using envelope encryption?

A. Generate a data encryption key (DEK) locally.Use a key encryption key (KEK) to wrap the DE
B. Encrypt data with the KE
C. Store the encrypted data and the wrapped KEK.
D. Generate a key encryption key (KEK) locally.Use the KEK to generate a data encryption key (DEK). Encrypt data with the DE
E. Store the encrypted data and the wrapped DEK.
F. Generate a data encryption key (DEK) locally.Encrypt data with the DEK.Use a key encryption key (KEK) to wrap the DE
G. Store the encrypted data and the wrapped DEK.
H. Generate a key encryption key (KEK) locally.Generate a data encryption key (DEK) locall
I. Encrypt data with the KE

J. Store the encrypted data and the wrapped DEK.

Answer: C

NEW QUESTION 62
......

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](link)