Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/

NEW QUESTION 1
A customer's company has multiple business units. Each business unit operates independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions.
Which strategy should you use to meet these needs?

A. Create an organization node, and assign folders for each business unit.
B. Establish standalone projects for each business unit, using gmail.com accounts.
C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.
D. Assign GCP resources in a VPC for each business unit to separate network access.

Answer: A

NEW QUESTION 2
You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.
What should you do?

A. Set up an ACL with OWNER permission to a scope of allUsers.
B. Set up an ACL with READER permission to a scope of allUsers.
C. Set up a default bucket ACL and manage access for users using IAM.
D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Answer: A

NEW QUESTION 3
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 4
A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

A. Run each tier in its own Project, and segregate using Project labels.
B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
C. Run each tier in its own subnet, and use subnet-based firewall rules.
D. Run each tier with its own VM tags, and use tag-based firewall rules.

Answer: C

NEW QUESTION 5
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 6
An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in Google Cloud Platform (GCP), and where Google's responsibility lies. They are mostly running workloads using Google Cloud's Platform-as-a-Service (PaaS) offerings, including App Engine primarily.
Which one of these areas in the technology stack would they need to focus on as their primary responsibility when using App Engine?

A. Configuring and monitoring VPC Flow Logs
B. Defending against XSS and SQLi attacks
C. Manage the latest updates and security patches for the Guest OS
D. Encrypting all stored data

Answer: D

NEW QUESTION 7

A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication
Which GCP product should the customer implement to meet these requirements?

A. Cloud Identity-Aware Proxy
B. Cloud Armor
C. Cloud Endpoints
D. Cloud VPN

Answer: D

NEW QUESTION 8
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 9
You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.
What should you do?

A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryptionkey (KEK) in Cloud KMS to encrypt the DE
B. Store both the encrypted data and the encrypted DEK.
C. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DE
D. Store both the encrypted data and the KEK.
E. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the ke
F. Store both the encrypted data and the encrypted DEK.
G. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the ke
H. Store both the encrypted data and the KEK.

Answer: A

NEW QUESTION 10
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 10
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 12
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 peer networks that belong to different Google Cloud Platform organizations
D. Firewall rules that can be created with a tag from one peered network to another peered network
E. Ability to share specific subnets across peered networks

Answer: AD

NEW QUESTION 15
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 18
A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.
Which connectivity option should be implemented?

A. VPC peering
B. Cloud VPN
C. Cloud Interconnect
D. Shared VPC

Answer: B

NEW QUESTION 20
A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.
Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.
Which type of access should your team grant to meet this requirement?

A. Organization Administrator
B. Security Reviewer
C. Organization Role Administrator
D. Organization Policy Administrator

Answer: C

NEW QUESTION 21
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 26
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 28
A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location.
How should the company accomplish this?

A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.
B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic basedon location.
C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

Answer: D

NEW QUESTION 29
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 33
A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity- Aware Proxy.
What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Answer: A

NEW QUESTION 35
An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.
Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses
Which solution should your team implement to meet these requirements?

A. Cloud Armor
B. Network Load Balancing
C. SSL Proxy Load Balancing
D. NAT Gateway

Answer: A

NEW QUESTION 37
A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.
What should you do to meet these requirements?

A. Create a Folder per department under the Organizatio
B. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
C. Create a Folder per department under the Organizatio
D. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
E. Create a Project per department under the Organizatio
F. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
G. Create a Project per department under the Organizatio
H. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Answer: C

NEW QUESTION 39
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 44
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 45
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 current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on-premises for an indefinite time. The organization wants a scalable and cost-efficient solution.
Which GCP solution should the organization use?

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

Answer: A

NEW QUESTION 47
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Security-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Security-Engineer Product From:

https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/

Money Back Guarantee

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