Professional-Cloud-Security-Engineer Dumps

Google Cloud Certified - Professional Cloud Security Engineer

https://www.certleader.com/Professional-Cloud-Security-Engineer-dumps.html

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
A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.
What should they do?

A. Use Cloud Build to build the container images.
B. Build small containers using small base images.
C. Delete non-used versions from Container Registry.
D. Use a Continuous Delivery tool to deploy the application.

Answer: D

NEW QUESTION 3
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 4
You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.

A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate one-way sync.
B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate bidirectional sync.
C. Use a management tool to sync the subset based on the email address attribut
D. Create a group in the Google domai
E. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
F. Use a management tool to sync the subset based on group object class attribut
G. Create a group in the Google domai
H. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

Answer: C

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
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 9
You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices. What should you do?

A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Answer: A

NEW QUESTION 10
A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.
Which two approaches can you take to meet the requirements? (Choose two.)

A. Configure the project with Cloud VPN.
B. Configure the project with Shared VPC.
C. Configure the project with Cloud Interconnect.
D. Configure the project with VPC peering.
E. Configure all Compute Engine instances with Private Access.

Answer: DE

NEW QUESTION 10
In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

A. App Engine
B. Cloud Functions
C. Compute Engine
D. Google Kubernetes Engine
E. Cloud Storage

Answer: AC

NEW QUESTION 11
A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs.
What should you do?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshol
B. Enable notifications.
C. Create an Alerting Policy in Stackdriver using the CPU usage metri
D. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
E. Log every execution of the script to Stackdriver Loggin
F. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
G. Log every execution of the script to Stackdriver Loggin

H. Configure BigQuery as a log sink, and create aBigQuery scheduled query to count the number of executions in a specific timeframe.

Answer: C

NEW QUESTION 14
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 19
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 24
When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

A. Ensure that the app does not run as PID 1.
B. Package a single app as a container.
C. Remove any unnecessary tools not needed by the app.
D. Use public container images as a base image for the app.
E. Use many container image layers to hide sensitive information.

Answer: BC

NEW QUESTION 29
A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE).
How should the DevOps team accomplish this?

A. Use Puppet or Chef to push out the patch to the running container.
B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
C. Update the application code or apply a patch, build a new image, and redeploy it.
D. Configure containers to automatically upgrade when the base image is available in Container Registry.

Answer: B

NEW QUESTION 30
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 35
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 36

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.
Which two strategies should your team use to meet these requirements? (Choose two.)

A. Configure Private Google Access on the Compute Engine subnet
B. Avoid assigning public IP addresses to the Compute Engine cluster.
C. Make sure that the Compute Engine cluster is running on a separate subnet.
D. Turn off IP forwarding on the Compute Engine instances in the cluster.
E. Configure a Cloud NAT gateway.

Answer: BE

NEW QUESTION 41
An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.
Which Cloud Identity password guidelines can the organization use to inform their new requirements?

A. Set the minimum length for passwords to be 8 characters.
B. Set the minimum length for passwords to be 10 characters.
C. Set the minimum length for passwords to be 12 characters.
D. Set the minimum length for passwords to be 6 characters.

Answer: C

NEW QUESTION 45
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 48
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 49
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 51
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 54
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 58
You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources. Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.
Which two actions should you take? (Choose two.)

A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

Answer: BE

NEW QUESTION 59
A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).
How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Answer: D

NEW QUESTION 60
Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

A. ISO 27001
B. ISO 27002
C. ISO 27017
D. ISO 27018

Answer: C

Explanation:
Create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

NEW QUESTION 61
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 62
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 64
An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable

their developer teams to deploy new applications without the overhead of this full review.
How should you advise this organization?

A. Use Forseti with Firewall filters to catch any unwanted configurations in production.
B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforcepolicies.
C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.
D. All production applications will run on-premise
E. Allow developers free rein in GCP as their dev and QA platforms.

Answer: B

NEW QUESTION 67
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 72
You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.
What should you do?

A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.
B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.
C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.
D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

Answer: B

NEW QUESTION 73
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 74
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 77
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 82
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 85
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your Professional-Cloud-Security-Engineer Exam with Our Prep Materials Via below:

https://www.certleader.com/Professional-Cloud-Security-Engineer-dumps.html