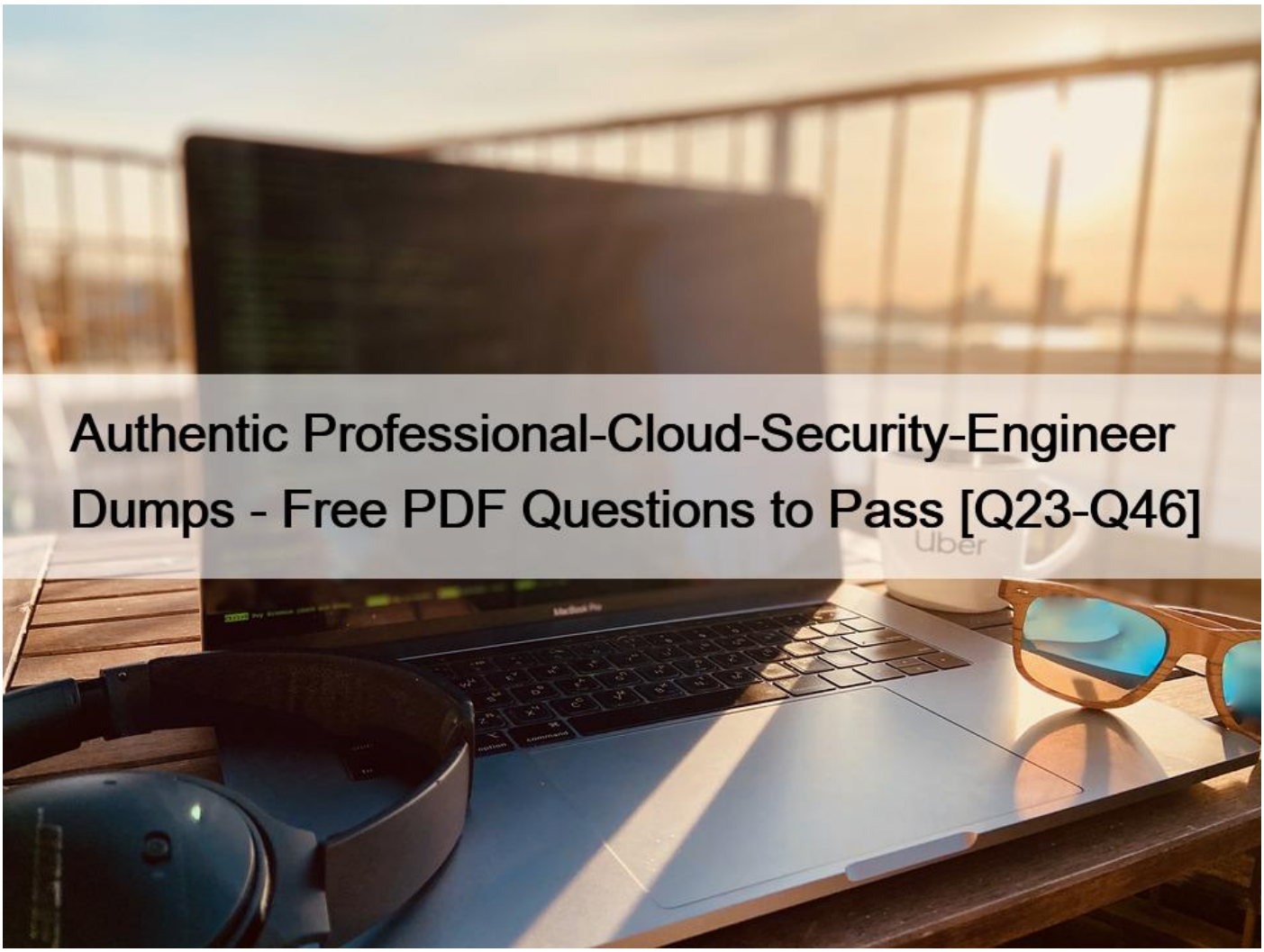
Authentic Professional-Cloud-Security-Engineer Dumps - Free PDF Questions to Pass [Q23-Q46



Authentic Professional-Cloud-Security-Engineer Dumps - Free PDF Questions to Pass
Guaranteed Accomplishment with Newest Jul-2022 FREE Professional-Cloud-Security-Engineer

Available Skill Badges

The Google skill badges are a form of training that allows candidates to demonstrate their understanding of Google concepts at this level. For the Google Professional Cloud Security Engineer exam, the most popular badges include the following: - Secure Workloads in Google Kubernetes Engine- Create and Manage Cloud Resources- Build and Secure Networks in Google Cloud- Ensure Access and Identity in Google Cloud **NEW QUESTION 23**

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?

* Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.

* Create a custom role with the permission compute.instances.listand grant the Service Account this role.
* Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
* Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

NEW QUESTION 24

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.)
* Configure the project with Cloud VPN.
* Configure the project with Shared VPC.
* Configure the project with Cloud Interconnect.
* Configure the project with VPC peering.
* Configure all Compute Engine instances with Private Access.
https://cloud.google.com/solutions/secure-data-workloads-use-cases

NEW QUESTION 25

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

NEW QUESTION 26

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?
* Create a new Service account, and give all application users the role of Service Account User.
* Create a new Service account, and add all application users to a Google Group. Give this group the role of Service Account User.
* Use a dedicated G Suite Admin account, and authenticate the application’s operations with these G Suite credentials.
* Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.
https://developers.google.com/admin-sdk/directory/v1/guides/delegation

NEW QUESTION 27

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.

How should this be accomplished?
* Create a firewall rule to block internet traffic from the VM.
* Provision a NAT Gateway to access the Cloud Storage API endpoint.
* Enable Private Google Access on the VPC.

* Mount a Cloud Storage bucket as a local filesystem on every VM.

NEW QUESTION 28

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments. How should you design the network to inspect the traffic?
* 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.
* 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.
* 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together.

2. Configure a custom route on each network pointed to the virtual appliance.
* 1. Set up two VPC networks: one trusted and the other untrusted.

2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

NEW QUESTION 29

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

Explanation/Reference:

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

NEW QUESTION 30

Your team wants to limit users with administrative privileges at the organization level.

Which two roles should your team restrict? (Choose two.)
* Organization Administrator
* Super Admin
* GKE Cluster Admin
* Compute Admin
* Organization Role Viewer
Reference:

https://cloud.google.com/resource-manager/docs/creating-managing-organization

NEW QUESTION 31

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?
* Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
* Make sure that the ERP system can validate the identity headers in the HTTP requests.
* Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
* Make sure that the ERP system can validate the user’s unique identifier headers in the HTTP requests.
Explanation/Reference:

NEW QUESTION 32

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

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

NEW QUESTION 33

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?
* Create a Folder per department under the Organization. For each department’s Folder, assign the Project Viewer role to the Google Group related to that department.
* Create a Folder per department under the Organization. For each department’s Folder, assign the Project Browser role to the Google Group related to that department.
* Create a Project per department under the Organization. For each department’s Project, assign the Project Viewer role to the Google Group related to that department.
* Create a Project per department under the Organization. For each department’s Project, assign the Project Browser role to the Google Group related to that department.

NEW QUESTION 34

An organization receives an increasing number of phishing emails.

Which method should be used to protect employee credentials in this situation?
* Multifactor Authentication
* A strict password policy
* Captcha on login pages
* Encrypted emails

NEW QUESTION 35

Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of Google Cloud user accounts being compromised. What should you do?
* Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with security keys in the Google Admin console.
* Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with verification codes via text or phone call in the Google Admin console.
* Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.
* Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with verification codes via text or phone call in the Google Admin console.

NEW QUESTION 36

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?
* Google Cloud Directory Sync (GCDS)
* Cloud Identity
* Security Assertion Markup Language (SAML)
* Pub/Sub
https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction

NEW QUESTION 37

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

NEW QUESTION 38

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?
* Cloud Data Loss Prevention with deterministic encryption using AES-SIV
* Cloud Data Loss Prevention with format-preserving encryption
* Cloud Data Loss Prevention with cryptographic hashing
* Cloud Data Loss Prevention with Cloud Key Management Service wrapped cryptographic keys

NEW QUESTION 39

You plan to deploy your cloud infrastructure using a CI/CD cluster hosted on Compute Engine. You want to minimize the risk of its credentials being stolen by a third party. What should you do?
* Create a dedicated Cloud Identity user account for the cluster. Use a strong self-hosted vault solution to store the user’s temporary credentials.
* Create a dedicated Cloud Identity user account for the cluster. Enable the constraints/iam.disableServiceAccountCreation organization policy at the project level.
* Create a custom service account for the cluster Enable the constraints/iam.disableServiceAccountKeyCreation organization policy at the project level.
* Create a custom service account for the cluster Enable the constraints/iam.allowServiceAccountCredentialLifetimeExtension organization policy at the project level.

NEW QUESTION 40

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?
* Perform data masking with the DLP API and store that data in BigQuery for later use.
* Perform data redaction with the DLP API and store that data in BigQuery for later use.
* Perform data inspection with the DLP API and store that data in BigQuery for later use.
* Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.
Explanation/Reference: https://towardsdatascience.com/bigquery-pii-and-cloud-data-loss-prevention-dlp-take-it-to-the-next-level-with-data-catalog-c47c31bcf677

NEW QUESTION 41

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?
* Shared VPC Network with a host project and service projects
* Grant Compute Admin role to the networking team for each engineering project
* VPC peering between all engineering projects using a hub and spoke model
* Cloud VPN Gateway between all engineering projects using a hub and spoke model

NEW QUESTION 42

You are the project owner for a regulated workload that runs in a project you own and manage as an Identity and Access Management (IAM) admin. For an upcoming audit, you need to provide access reviews evidence. Which tool should you use?
* Policy Troubleshooter
* Policy Analyzer
* IAM Recommender
* Policy Simulator

NEW QUESTION 43

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

NEW QUESTION 44

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?
* Use the Cloud Key Management Service to manage a data encryption key (DEK).
* Use the Cloud Key Management Service to manage a key encryption key (KEK).
* Use customer-supplied encryption keys to manage the data encryption key (DEK).
* Use customer-supplied encryption keys to manage the key encryption key (KEK).

Reference:

https://cloud.google.com/security/encryption-at-rest/default-encryption/

NEW QUESTION 45

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?
* VPC Flow Logs
* Cloud Armor
* DNS Security Extensions
* Cloud Identity-Aware Proxy

Explanation/Reference: https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

NEW QUESTION 46

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?

* Cloud Identity-Aware Proxy
* Cloud Armor
* Cloud Endpoints
* Cloud VPN