Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.
What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberoscompliant identity provider.
D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Answer: B

NEW QUESTION 3
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 4
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 5
Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services.
Which two settings must remain disabled to meet these requirements? (Choose two.)

A. Public IP
B. IP Forwarding
C. Private Google Access
D. Static routes
E. IAM Network User Role

Answer: CD

NEW QUESTION 6
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 7
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 8
Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

A. Organization Administrator
B. Super Admin
C. GKE Cluster Admin
D. Compute Admin
E. Organization Role Viewer

Answer: AB

NEW QUESTION 9
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 10
An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier.
Which Cloud Data Loss Prevention API technique should you use to accomplish this?

A. Generalization
B. Redaction
C. CryptoHashConfig
D. CryptoReplaceFfxFpeConfig

Answer: B

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 11
You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.
How should you prevent and fix this vulnerability?

A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Answer: D

NEW QUESTION 12
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 14
In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard
Which options should you recommend to meet the requirements?

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

Answer: D

NEW QUESTION 18
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 20
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 24
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 26
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 30
Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement.
How should your team meet these requirements?

A. Enable Private Access on the VPC network in the production project.
B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.
C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

Answer: C

NEW QUESTION 31
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 35
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 38
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 42
A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.
Which Storage solution are they allowed to use?

A. Cloud Bigtable
B. Cloud BigQuery
C. Compute Engine SSD Disk
D. Compute Engine Persistent Disk

Answer: B

NEW QUESTION 47
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 49
You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow thee application frontend to access the data in the application's mysql instance on port 3306.
What should you do?

A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.

B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet
D. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe-tag.
E. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet
F. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Answer: B

NEW QUESTION 53
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 54
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
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 61
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
Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.
Which two tasks should your team perform to handle this request? (Choose two.)

A. Remove all users from the Project Creator role at the organizational level.
B. Create an Organization Policy constraint, and apply it at the organizational level.
C. Grant the Project Editor role at the organizational level to a designated group of users.
D. Add a designated group of users to the Project Creator role at the organizational level.
E. Grant the billing account creator role to the designated DevOps team.

Answer: BD

NEW QUESTION 63

.....

Relate Links

100% Pass Your Professional-Cloud-Security-Engineer Exam with Exambible Prep Materials

https://www.exambible.com/Professional-Cloud-Security-Engineer-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/