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
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
A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.
The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

Answer: C

NEW QUESTION 5
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 6
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 7

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 8
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 9
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 10
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 10
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 14
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 18
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 20
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 22
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 24
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 29
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 30
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 34
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 37
Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.
How should your team design this network?

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
B. Create a different subnet for the frontend application and database to ensure network isolation.
C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Answer: A

NEW QUESTION 39
You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.
What should you do?

A. Migrate the application into an isolated project using a “Lift & Shift” approac
B. Enable all internal TCP traffic using VPC Firewall rule
C. Use VPC Flow logs to determine what traffic should be allowed for theapplication to work properly.
D. Migrate the application into an isolated project using a “Lift & Shift” approach in a custom network.Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
E. Refactor the application into a micro-services architecture in a GKE cluste
F. Disable all traffic from outside the cluster using Firewall Rule
G. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
H. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project.Disable all traffic from outside your project using Firewall Rule
I. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Answer: C

NEW QUESTION 43
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 44
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?

A. Create a firewall rule to block internet traffic from the VM.
B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
C. Enable Private Google Access on the VPC.
D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Answer: B

NEW QUESTION 47
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 48
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 52
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?

A. VPC Flow Logs
B. Cloud Armor
C. DNS Security Extensions
D. Cloud Identity-Aware Proxy

Answer: C

NEW QUESTION 53
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 55
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 56
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 61
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 uploade
H. Use Cloud Functions to capture the trigger and delete such files.

Answer: C

NEW QUESTION 64
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 65
A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.
How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Answer: D

NEW QUESTION 67
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 71
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 74
Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.
What should your team do to meet these requirements?

A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Answer: B

NEW QUESTION 79
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 82
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 84
You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.
What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
B. Manage the IAM permissions at the Key level.
C. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
D. Manage the IAM permissions at the KeyRing level.
E. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke
F. Manage the IAM permissions at the Key level.
G. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke
H. Manage the IAM permissions at the KeyRing level.

Answer: C

NEW QUESTION 89
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 90
.....

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/