Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

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

NEW QUESTION 1
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 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 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
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 7
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 8
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 9
A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.
How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

NEW QUESTION 10
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 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 13
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 18
You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.
What should you do?

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

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

Answer: A

NEW QUESTION 21
Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks
B. Non-transitive peered networks; where only directly peered networks can communicate
C. Ability to peer networks that belong to different Google Cloud Platform organizations
D. Firewall rules that can be created with a tag from one peered network to another peered network
E. Ability to share specific subnets across peered networks

Answer: AD

NEW QUESTION 26
A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.
Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.
Which type of access should your team grant to meet this requirement?

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

Answer: C

NEW QUESTION 27
Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer.
What type of Load Balancing should you use?

A. Network Load Balancing
B. HTTP(S) Load Balancing
C. TCP Proxy Load Balancing
D. SSL Proxy Load Balancing

Answer: D

NEW QUESTION 28
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 29
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 34
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 39
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 44
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 48
Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.
What should you do?

A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Answer: A

NEW QUESTION 51
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 53
A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.
Which product should be used to meet these requirements?

A. Cloud Armor
B. VPC Firewall Rules
C. Cloud Identity and Access Management
D. Cloud CDN

Answer: A

NEW QUESTION 58
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 59
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 61
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 63
Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.
What should you do?

A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
B. Use the Cloud Key Management Service to manage the 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 68
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 73
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 75
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 80
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 81
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

Professional-Cloud-Security-Engineer Practice Exam Features:

* Professional-Cloud-Security-Engineer Questions and Answers Updated Frequently

* Professional-Cloud-Security-Engineer Practice Questions Verified by Expert Senior Certified Staff

* Professional-Cloud-Security-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Professional-Cloud-Security-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year