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
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
A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.
Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

Answer: C

NEW QUESTION 4
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 5
A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and rotate the encryption keys.
Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)
B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)
C. Encryption by default
D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Answer: B

Explanation:
Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

NEW QUESTION 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
You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.

What should you do?

A. Query Data Access logs.
B. Query Admin Activity logs.
C. Query Access Transparency logs.
D. Query Stackdriver Monitoring Workspace.

Answer: A

NEW QUESTION 8
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 9
A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.
Which two steps should the company take to meet these requirements? (Choose two.)

A. Create a project with multiple VPC networks for each environment.
B. Create a folder for each development and production environment.
C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
D. Create an Organizational Policy constraint for each folder environment.
E. Create projects for each environment, and grant IAM rights to each engineering user.

Answer: BD

NEW QUESTION 10
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 12
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 17
Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.
What should you do?

A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
B. Store the data in a single BigQuery table and set the appropriate table expiration time.

C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
D. Store the data in a single BigTable table and set an expiration time on the column families.

Answer: B

NEW QUESTION 19
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 23
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 26
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 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 33
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 36
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 41
A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity- Aware Proxy.
What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Answer: A

NEW QUESTION 43
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 44
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 49
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 50
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 53
.....

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