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
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 3
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 4
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 5
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 6
An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.
Which Cloud Identity password guidelines can the organization use to inform their new requirements?

A. Set the minimum length for passwords to be 8 characters.
B. Set the minimum length for passwords to be 10 characters.
C. Set the minimum length for passwords to be 12 characters.
D. Set the minimum length for passwords to be 6 characters.

Answer: C

NEW QUESTION 7

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.
B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Answer: C

NEW QUESTION 8
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 9
Applications often require access to "secrets" - small pieces of sensitive data at build or run time. The administrator managing these secrets on GCP wants to keep a track of "who did what, where, and when?" within their GCP projects.
Which two log streams would provide the information that the administrator is looking for? (Choose two.)

A. Admin Activity logs
B. System Event logs
C. Data Access logs
D. VPC Flow logs
E. Agent logs

Answer: AC

NEW QUESTION 10
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 10
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 13
As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name.
Which cost reduction options should you recommend?

A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
D. Use FindingLimits and TimespanContfig to sample data and minimize transformation units.

Answer: C

NEW QUESTION 15

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 17
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?

A. Create a new Service account, and give all application users the role of Service Account User.
B. Create a new Service account, and add all application users to a Google Grou
C. Give this group the role of Service Account User.
D. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
E. Create a new service account, and grant it G Suite domain-wide delegatio
F. Have the application use it to impersonate the user.

Answer: A

NEW QUESTION 19
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 21
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 22
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 24
Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.
What should you do?

A. Temporarily disable authentication on the Cloud Storage bucket.
B. Use the undelete command to recover the deleted service account.
C. Create a new service account with the same name as the deleted service account.
D. Update the permissions of another existing service account and supply those credentials to the applications.

Answer: B

NEW QUESTION 25
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 30
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 33
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 35
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 40
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 42
......

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