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
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 2
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 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
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 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
Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.
What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.
B. Compute Network User Role at the subnet level.
C. Compute Shared VPC Admin Role at the host project level.
D. Compute Shared VPC Admin Role at the service project level.

Answer: C

NEW QUESTION 7
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 8
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 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 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
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
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 13

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 15
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 18
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 20
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 22
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
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 29
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 33
A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).
How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Answer: D

NEW QUESTION 37
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 40
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 43
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 45
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 47
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 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 52
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 55
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 59
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 62
A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

A. Create a Folder per department under the Organizatio
B. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
C. Create a Folder per department under the Organizatio
D. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
E. Create a Project per department under the Organizatio
F. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
G. Create a Project per department under the Organizatio
H. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Answer: C

NEW QUESTION 64
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 68
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 73
......

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