Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

NEW QUESTION 1
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 2
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 3
Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

A. Enforce 2-factor authentication in GSuite for all users.
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
C. Provision user passwords using GSuite Password Sync.
D. Configure Cloud VPN between your private network and GCP.

Answer: D

NEW QUESTION 4
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 5
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 6
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 7
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 8

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 9

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 10

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 10

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 12

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 15

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 17
When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for
review by internal or external analysts for customer service trend analysis.
Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Answer: D

Explanation:
Reference; https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION 20
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 23
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 28
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 30
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 35
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 38
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 41
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 46
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 48
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 51
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 53
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 54
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 56
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 58
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 60
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 63
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 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 65
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 67
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The Professional-Cloud-Security-Engineer Practice Test Here