# PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

## Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/professional-cloud-security-engineer.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

**QUESTION 1**

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.

Correct Answer: B

https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

**QUESTION 2**

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 KeyRing. Manage the IAM permissions at the Key level.

B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.

D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B

https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk

**QUESTION 3**

You want to update your existing VPC Service Controls perimeter with a new access level. You need to avoid breaking the existing perimeter with this change, and ensure the least disruptions to users while minimizing overhead. What should you do?

A. Create an exact replica of your existing perimeter. Add your new access level to the replica. Update the original perimeter after the access level has been vetted.

B. Update your perimeter with a new access level that never matches. Update the new access level to match your desired state one condition at a time to avoid being overly permissive.

C. Enable the dry run mode on your perimeter. Add your new access level to the perimeter configuration. Update the perimeter configuration after the access level has been vetted.

D. Enable the dry run mode on your perimeter. Add your new access level to the perimeter dry run configuration. Update the perimeter configuration after the access level has been vetted.

Correct Answer: D

https://cloud.google.com/vpc-service-controls/docs/dry-run-mode When using VPC Service Controls, it can be difficult to determine the impact to your environment when a service perimeter is created or modified. With dry run mode, you can better understand the impact of enabling VPC Service Controls and changes to perimeters in existing environments.

**QUESTION 4**

Your company\\'s Google Cloud organization has about 200 projects and 1,500 virtual machines. There is no uniform strategy for logs and events management, which reduces visibility for your security operations team. You need to design a logs management solution that provides visibility and allows the security team to view the environment\\'s configuration.

What should you do?

A. 1. Create a dedicated log sink for each project that is in scope.

2.

Use a BigQuery dataset with time partitioning enabled as a destination of the log sinks.

3.

Deploy alerts based on log metrics in every project.

4.

Grant the role "Monitoring Viewer" to the security operations team in each project.

B. 1. Create one log sink at the organization level that includes all the child resources.

2.

Use as destination a Pub/Sub topic to ingest the logs into the security information and event.

management (SIEM) on-premises, and ensure that the right team can access the SIEM.

3.

Grant the Viewer role at organization level to the security operations team.

C. 1. Enable network logs and data access logs for all resources in the "Production" folder.

2.

Do not create log sinks to avoid unnecessary costs and latency.

3.

Grant the roles "Logs Viewer" and "Browser" at project level to the security operations team.

D. 1. Create one sink for the "Production" folder that includes child resources and one sink for the logs ingested at the organization level that excludes child resources.

2.

As destination, use a log bucket with a minimum retention period of 90 days in a project that can be accessed by the security team.

3.

Grant the security operations team the role of Security Reviewer at organization level.

Correct Answer: B

B. 1. Create one log sink at the organization level that includes all the child resources.

2. Use as destination a Pub/Sub topic to ingest the logs into the security information and event management (SIEM) on-premises, and ensure that the right team can access the SIEM.

**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

Correct Answer: AC

Reference: https://cloud.google.com/vpc/docs/configure-private-google-access

**QUESTION 6**

You have a highly sensitive BigQuery workload that contains personally identifiable information (PII) that you want to ensure is not accessible from the internet. To prevent data exfiltration only requests from authorized IP addresses are allowed to query your BigQuery tables.

What should you do?

A. Use service perimeter and create an access level based on the authorized source IP address as the condition.

B. Use Google Cloud Armor security policies defining an allowlist of authorized IP addresses at the global HTTPS load balancer.

C. Use the Restrict allowed Google Cloud APIs and services organization policy constraint along with Cloud Data Loss Prevention (DLP).

D. Use the Restrict Resource service usage organization policy constraint along with Cloud Data Loss Prevention (DLP).

Correct Answer: A

**QUESTION 7**

Your company\\'s chief information security officer (CISO) is requiring business data to be stored in specific locations due to regulatory requirements that affect the company\\'s global expansion plans. After working on a plan to implement this requirement, you determine the following:

1.

The services in scope are included in the Google Cloud data residency requirements.

2.

The business data remains within specific locations under the same organization. The folder structure can contain multiple data residency locations.

3.

The projects are aligned to specific locations.

You plan to use the Resource Location Restriction organization policy constraint with very granular control. At which level in the hierarchy should you set the constraint?

A. Organization

B. Resource

C. Project

D. Folder

Correct Answer: C

**QUESTION 8**

You have noticed an increased number of phishing attacks across your enterprise user accounts. You want to implement the Google 2-Step Verification (2SV) option that uses a cryptographic signature to authenticate a user and verify the URL of the login page.

Which Google 2SV option should you use?

A. Titan Security Keys

B. Google prompt

C. Google Authenticator app

D. Cloud HSM keys

Correct Answer: A

https://cloud.google.com/titan-security-key

Security keys use public key cryptography to verify a user\\'s identity and URL of the login page ensuring attackers can\\'t access your account even if you are tricked into providing your username and password.

**QUESTION 9**

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 bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.

B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.

C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.

D. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded. Use Cloud Functions to capture the trigger and delete such files.

Correct Answer: A

https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0
https://www.youtube.com/watch?v=0TmO1f-Ox40

**QUESTION 10**

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.

Correct Answer: A

https://cloud.google.com/resource-manager/docs/listing-all-resources https://wideops.com/mapping-your-organization-with-the-google-cloud-platform-resource-hierarchy/

**QUESTION 11**

Your organization is using GitHub Actions as a continuous integration and delivery (CI/CD) platform. You must enable access to Google Cloud resources from the CI/CD pipelines in the most secure way. What should you do?

A. Create a service account key and add it to the GitHub pipeline configuration file.

B. Create a service account key and add it to the GitHub repository content.

C. Configure a Google Kubernetes Engine cluster that uses Workload Identity to supply credentials to GitHub.

D. Configure workload identity federation to use GitHub as an identity pool provider.

Correct Answer: D

**QUESTION 12**

You recently joined the networking team supporting your company\\'s Google Cloud implementation. You are tasked with familiarizing yourself with the firewall rules configuration and providing recommendations based on your networking and Google Cloud experience. What product should you recommend to detect firewall rules that are overlapped by attributes from other firewall rules with higher or equal priority?

A. Security Command Center

B. Firewall Rules Logging

C. VPC Flow Logs

D. Firewall Insights

Correct Answer: D

https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview#shadowed- firewall-rules Firewall Insights analyzes your firewall rules to detect firewall rules that are shadowed by other rules. A shadowed rule is a firewall rule that has all of its relevant attributes, such as its IP address and port ranges, overlapped by attributes from one or more rules with higher or equal priority, called shadowing rules.

**QUESTION 13**

You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud

environment in the daily ETL process from an on-premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re-identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)

A. Secret Manager

B. Cloud Key Management Service

C. Cloud Data Loss Prevention with cryptographic hashing

D. Cloud Data Loss Prevention with automatic text redaction

E. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Correct Answer: BE

B: you need KMS to store the CryptoKey
https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#crypt

E: for the de-identity you need to use CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig
https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#cryptodet erministicconfig
https://cloud.google.com/dlp/docs/deidentify-sensitive-data

**QUESTION 14**

Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and

determine the user activity.

What should you do?

A. Use Security Health Analytics to determine user activity.

B. Use the Cloud Monitoring console to filter audit logs by user.

C. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.

D. Use the Logs Explorer to search for user activity.

Correct Answer: D

We use audit logs by searching the Service Account and checking activities in the past 2 months. (the user identity will not be seen since he used the SA identity but we can make correlations based on ip address, working hour, etc. )

**QUESTION 15**

Which Google Cloud service should you use to enforce access control policies for applications and resources?

A. Identity-Aware Proxy

B. Cloud NAT

C. Google Cloud Armor

D. Shielded VMs

Correct Answer: A

https://cloud.google.com/iap/docs/concepts-overview "Use IAP when you want to enforce access control policies for applications and resources."