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.leads4pass.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

Your application is deployed as a highly available cross-region solution behind a global external HTTP(S) load balancer. You notice significant spikes in traffic from multiple IP addresses but it is unknown whether the IPs are malicious. You are concerned about your application\\'s availability. You want to limit traffic from these clients over a specified time interval.

What should you do?

A. Configure a rate_based_ban action by using Google Cloud Armor and set the ban_duration_sec parameter to the specified time interval.

B. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.

C. Configure a throttle action by using Google Cloud Armor to limit the number of requests per client over a specified time interval.

D. Configure a firewall rule in your VPC to throttle traffic from the identified IP addresses.

Correct Answer: C

QUESTION 2

Your organization wants full control of the keys used to encrypt data at rest in their Google Cloud environments. Keys must be generated and stored outside of Google and integrate with many Google Services including BigQuery. What should you do?

A. Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems. Provide the raw CSEK as part of the API call.

B. Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM). Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.

C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

D. Create a Cloud Key Management Service (KMS) key with imported key material. Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.

Correct Answer: C

The correct answer is C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

Cloud EKM allows you to use encryption keys that are stored and managed in a third-party key management system deployed outside of Google\\'s infrastructure. This gives your organization full control over the keys used to encrypt data at rest in Google Cloud environments, including BigQuery.

QUESTION 3

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.

Correct Answer: BC

QUESTION 4

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google Cloud resources. Your export must meet the following requirements:

Export related logs for all projects in the Google Cloud organization.

Export logs in near real-time to an external SIEM.

What should you do? (Choose two.)

A. Create a Log Sink at the organization level with a Pub/Sub destination.

B. Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.

C. Enable Data Access audit logs at the organization level to apply to all projects.

D. Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.

E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Correct Answer: BD

Reference:

https://www.datadoghq.com/blog/monitoring-gcp-audit-logs/ https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#services "Google Workspace Login Audit: Login Audit logs track user sign-ins to your domain. These logs only

record the login event. They don\\'t record which system was used to perform the login action."

QUESTION 5

You are a security administrator at your company and are responsible for managing access controls (identification, authentication, and authorization) on Google Cloud. Which Google-recommended best practices should you follow when configuring authentication and authorization? (Choose two.)

A. Use Google default encryption.

B. Manually add users to Google Cloud.

C. Provision users with basic roles using Google\\'s Identity and Access Management (1AM) service.

D. Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management.

E. Provide granular access with predefined roles.

Correct Answer: DE

https://cloud.google.com/iam/docs/using-iam-securely#least_privilege Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative. Instead, grant the most limited predefined roles or custom roles that meet your needs.