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

You need to implement an encryption at-rest strategy that reduces key management complexity for non- sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types.

What should you do?

A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.

B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service

C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.

D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Correct Answer: D

Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of controlling the key residency and rotation schedule, use google provided key for non- sensitive and encrypt sensitive data with Cloud Key Management Service

QUESTION 2

A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication

Which GCP product should the customer implement to meet these requirements?

A. Cloud Identity-Aware Proxy

B. Cloud Armor

C. Cloud Endpoints

D. Cloud VPN

Correct Answer: A

Cloud IAP is integrated with Google Sign-in which Multi-factor authentication can be enabled.
https://cloud.google.com/iap/docs/concepts-overview

QUESTION 3

Your company\\'s cloud security policy dictates that VM instances should not have an external IP address. You need to identify the Google Cloud service that will allow VM instances without external IP addresses to connect to the internet

to

update the VMs.

Which service should you use?

A. Identity Aware-Proxy

B. Cloud NAT

C. TCP/UDP Load Balancing

D. Cloud DNS

Correct Answer: B

https://cloud.google.com/nat/docs/overview "Cloud NAT (network address translation) lets certain resources without external IP addresses create outbound connections to the internet."

QUESTION 4

You are migrating your users to Google Cloud. There are cookie replay attacks with Google web and Google Cloud CLI SDK sessions on endpoint devices. You need to reduce the risk of these threats. What should you do? (Choose two.)

A. Configure Google session control to a shorter duration.

B. Set an organizational policy for OAuth 2.0 access token with a shorter duration.

C. Set a reauthentication policy for Google Cloud services to a shorter duration.

D. Configure a third-party identity provider with session management.

E. Enforce Security Key Authentication with 2SV.

Correct Answer: AE

Correct anwers are A and E.

A. Configuring Google session control to a shorter duration reduces the time window in which an attacker can use a replayed cookie to gain unauthorized access, thereby enhancing security.

E. Enforcing Security Key Authentication with 2-Step Verification (2SV) adds an additional layer of security by requiring users to verify their identity using a physical security key, making it more difficult for attackers to gain unauthorized access even if they have a replayed cookie.

QUESTION 5

Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements. What should you do?

A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.

B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository Verify that the image is not deprecated.

C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.

D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: A