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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

A customer\\'s data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite.

How should you best advise the Systems Engineer to proceed with the least disruption?

A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.

B. Register a new domain name, and use that for the new Cloud Identity domain.

C. Ask Google to provision the data science manager\\'s account as a Super Administrator in the existing domain.

D. Ask customer\\'s management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Correct Answer: D

https://support.google.com/cloudidentity/answer/7389973

QUESTION 2

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 3

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 4

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."

QUESTION 5

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.

Correct Answer: C

https://cloud.google.com/dlp/docs/concepts-image-redaction

PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps | PROFESSIONAL-CLOUD-SECURITY-ENGINEER Practice Test | PROFESSIONAL-CLOUD-SECURITY-ENGINEER Study Guide