Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 238 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 238
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your company is concerned about unauthorized parties gaining access to the Google Cloud environment by using a fake login page. You must implement a solution to protect against person-in-the-middle attacks.

Which security measure should you use?

A. Security key

B. Google prompt

C. Text message or phone call code

D. Google Authenticator application

Show Suggested Answer

by MisterHairy at *Nov. 21, 2023, 11 p.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: A

Key Differences:
Security Key (A): Uses cryptographic proof of identity and the FIDO standard, making it highly resistant to phishing and person-in-the-middle attacks. It requires physical possession of the key, adding an extra layer of security.
Google Authenticator (D): Generates time-based one-time passwords (TOTP) that are more secure than SMS codes but can still be vulnerable to phishing if the attacker manages to intercept the code.

upvoted 1 times

3d9563b 1 year ago

Selected Answer: A

To mitigate the risk of man-in-the-middle attacks and enhance the security of your Google Cloud environment, security keys provide the highest level of protection by using strong cryptographic methods and requiring physical access for authentication.

upvoted 1 times

Bettoxicity 1 year, 3 months ago

Selected Answer: D

- MFA: Google Authenticator is a MFA tool that generates unique, time-based one-time passcodes (OTP) on your mobile device. Even if an attacker steals your login credentials, they wouldn't have the valid OTP generated by the Google Authenticator app, significantly reducing the risk of unauthorized access.
- Out-of-band Authentication: MFA with Google Authenticator provides an extra layer of security because the verification code is generated on a separate device (your phone) rather than being sent via SMS or a phone call, which can be intercepted in person-in-the-middle attacks.

Why not A?: Security keys offer strong two-factor authentication, but they require physical possession of the key, which might not be suitable for all situations.

upvoted 1 times

dija123 1 year, 4 months ago

Selected Answer: A

A. Security key

upvoted 1 times

Crotofroto 1 year, 6 months ago

Selected Answer: A

A is the only one that validates physically the person who is trying to access.

upvoted 1 times

MisterHairy 1 year, 8 months ago

Selected Answer: A

The correct answer is A. Security key.

A security key is a physical device that you can use for two-step verification, providing an additional layer of security for your Google Account. Security keys can defend against phishing and man-in-the-middle attacks, making your login process more secure.

upvoted 2 times