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 227 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 227
Topic #: 1
[All Professional Cloud Security Engineer Questions]

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.

Show Suggested Answer

by ppandher at *Aug. 3, 2023, 2:49 p.m.*

Comments

Type your comment...

Submit

i_am_robot Highly Voted 1 year, 10 months ago

Selected Answer: A

Correct anwers are A & 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.

upvoted 9 times

ymkk Highly Voted 1 year, 11 months ago

B and E
Set an organizational policy for OAuth 2.0 access token with a shorter duration is a good approach to reduce the time during which a stolen access token could be exploited. Shortening the access token duration helps mitigate the impact of cookie replay attacks. OAuth 2.0 access tokens are commonly used to authenticate API requests. By reducing their duration, you limit the time frame in which an attacker could potentially abuse a stolen token.

Enforce Security Key Authentication with 2SV adds strong authentication to user sessions. Security keys are hardware-based tokens that provide strong authentication and help prevent unauthorized access, including cookie replay attacks. By requiring Security Key Authentication with 2SV (Two-Step Verification), you enhance the security of user accounts.

upvoted 5 times

BPzen Most Recent 8 months ago

Selected Answer: A

A and B

A. Configure Google session control to a shorter duration.

Reducing the session duration decreases the time a session cookie remains valid, thus limiting the risk of a replay attack. Shorter session times force more frequent reauthentication and can prevent attackers from leveraging stolen session cookies effectively.
B. Set an organizational policy for OAuth 2.0 access token with a shorter duration.

OAuth 2.0 access tokens are used for authenticating requests to Google Cloud APIs. By setting a shorter expiration time for these tokens, you reduce the window of opportunity for attackers to exploit stolen tokens in replay attacks.

upvoted 1 times

Mr_MIXER007 10 months, 3 weeks ago

Missing missing missing

upvoted 1 times

Sundar_Pichai 11 months, 1 week ago

B&E,

Limiting the session duration itself, doesn't do except give a malicious attacker a shorter time to do the 'bad thing', however, limiting the time that the cookie is actually usable could prevent an attacker from impersonating a user. Additionally, 2SV is nearly always a right answer.

upvoted 1 times

dija123 1 year, 4 months ago

Selected Answer: A

A,C are correct

upvoted 1 times

acloudgurrru 1 year, 5 months ago

You shorten the session duration by setting the reauthentication policy so the answer is C and not A.

upvoted 1 times

rglearn 1 year, 10 months ago

Selected Answer: C

AC
keeping shorter session and enforcing reauthentication after certain period of time will help to address the issue

upvoted 3 times

desertlotus1211 1 year, 10 months ago

The question is not about validating a user identity- it's about mitigating a risk of open sessions.

Answers B&C are correct. Answer C is A.

upvoted 3 times

anshad666 1 year, 11 months ago

I will go for A and C

A - For Google Web services like Gmail
https://support.google.com/a/answer/9368756?hl=en

C - for Google Cloud Services and SDK
https://support.google.com/a/answer/9368756?hl=en

Enforce Security Key Authentication with 2SV adds strong authentication to user sessions. but it doesn't help if the attacker has already gained access.

To mitigate cookie replay attacks, a web application should:

- Invalidate a session after it exceeds the predefined idle timeout, and after the user logs out.
- Set the lifespan for the session to be as short as possible.
- Encrypt the session data.
- Have a mechanism to detect when a cookie is seen by multiple clients

upvoted 4 times

akg001 1 year, 11 months ago

A and E

upvoted 4 times

Mithung30 1 year, 11 months ago

A, C
A. Configure Google session control to a shorter duration. This will make it more difficult for attackers to use stolen cookies to access user accounts, as the cookies will expire more quickly.
C. Set a reauthentication policy for Google Cloud services to a shorter duration. This will also make it more difficult for attackers to use stolen cookies to access user accounts, as they will need to reauthenticate more frequently.

upvoted 3 times

cyberpunk21 1 year, 11 months ago

I don't A is good fit cuz we don't want users to lose their work because of short session duration.

upvoted 1 times

ppandher 1 year, 12 months ago

Options A, C, and D are not directly related to mitigating cookie replay attacks or enhancing security against such threats. They address different aspects of session control, reauthentication policy, and identity provider configuration, but they do not directly tackle the issue of cookie replay attacks.

Therefore, the best choices in this scenario are B and E.

upvoted 2 times