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 306 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 306

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You must ensure that the keys used for at-rest encryption of your data are compliant with your organization's security controls. One security control mandates that keys get rotated every 90 days. You must implement an effective detection strategy to validate if keys are rotated as required. What should you do?

A. Analyze the crypto key versions of the keys by using data from Cloud Asset Inventory. If an active key is older than 90 days, send an alert message through your incident notification channel.

B. Assess the keys in the Cloud Key Management Service by implementing code in Cloud Run. If a key is not rotated after 90 days, raise a finding in Security Command Center.

C. Define a metric that checks for timely key updates by using Cloud Logging. If a key is not rotated after 90 days, send an alert message through your incident notification channel.

D. Identify keys that have not been rotated by using Security Health Analytics. If a key is not rotated after 90 days, a finding in Security Command Center is raised.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:15 p.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: D

https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics-findings#kms_key_not_rotated

upvoted 3 times

BPzen 8 months ago

Selected Answer: A

Why A is Correct:
Cloud Asset Inventory:

Cloud Asset Inventory offers a detailed view of cryptographic keys, including the age of each key version.
By periodically analyzing this data, you can determine if a key version has been in use for more than 90 days.
Proactive Monitoring:

This approach allows you to set up automated checks and send alerts to incident notification channels (e.g., email, Slack, PagerDuty) when keys exceed the allowed age.

upvoted 1 times

MoAk 8 months, 1 week ago

Selected Answer: D

D - https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics-findings#kms_key_not_rotated

upvoted 2 times

jmaquino 9 months ago

Selected Answer: A

https://cloud.google.com/secret-manager/docs/analyze-resources?hl=es-419

upvoted 1 times

koo_kai 9 months, 2 weeks ago

Selected Answer: D

It's D
https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics-findings#kms_key_not_rotated

upvoted 4 times

siheom 9 months, 3 weeks ago

Selected Answer: A

VOTE A

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

D - Security Health Analytics: Security Health Analytics is a specialized tool designed to assess the security posture of your Google Cloud environment. It can effectively identify keys that have not been rotated within the specified timeframe.
Finding in Security Command Center: Raising a finding in Security Command Center ensures that the non-compliance issue is clearly documented and can be addressed promptly.
Efficiency: Security Health Analytics provides a streamlined and efficient way to monitor key rotation compliance without requiring custom code or manual analysis.

upvoted 4 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses