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 284 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 284
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You are responsible for a set of Cloud Functions running on your organization's Google Cloud environment. During the last annual security review, secrets were identified in environment variables of some of these Cloud Functions. You must ensure that secrets are identified in a timely manner. What should you do?

A. Implement regular peer reviews to assess the environment variables and identify secrets in your Cloud Functions. Raise a security incident if secrets are discovered.

B. Implement a Cloud Function that scans the environment variables multiple times a day, and creates a finding in Security Command Center if secrets are discovered.

C. Use Sensitive Data Protection to scan the environment variables multiple times per day, and create a finding in Security Command Center if secrets are discovered.

D. Integrate dynamic application security testing into the CI/CD pipeline that scans the application code for the Cloud Functions. Fail the build process if secrets are discovered.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:48 a.m.*

Comments

Type your comment...

Submit

nah99 8 months ago

Selected Answer: C

https://cloud.google.com/sensitive-data-protection/docs/secrets-discovery#why

upvoted 2 times

KLei 8 months, 2 weeks ago

Selected Answer: C

(Dynamic application security testing): While this can help identify secrets in the code, it does not specifically address the secrets that may be present in environment variables

upvoted 1 times

dv1 9 months, 1 week ago

Selected Answer: C

Question asks for secret identification, not blocking the cloud runs if exposed secrets are detected (what D says).

upvoted 2 times

dat987 9 months, 2 weeks ago

Selected Answer: C

I think C:

To perform secrets discovery, you create a discovery scan configuration at the organization or project level. Within your selected scope, Sensitive Data Protection periodically scans Cloud Run functions for secrets in build and runtime environment variables.

If a secret is present in an environment variable, Sensitive Data Protection sends a Secrets in environment variables vulnerability finding to Security Command Center. No data profiles are generated. Any findings are only available through Security Command Center.

Sensitive Data Protection generates a maximum of one finding per function. For example, if secrets are found in two environment variables in the same function, only one finding is generated in Security Command Center.

upvoted 2 times

brpjp 10 months, 1 week ago

Correct answer - D. For answer C, you need to integrate Sensitive Data Protection with CI/CD pipelines, which is missing here.

upvoted 4 times

yokoyan 10 months, 3 weeks ago

Selected Answer: D

I think it's D.

upvoted 4 times