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 246 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 246
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization relies heavily on Cloud Run for its containerized applications. You utilize Cloud Build for image creation, Artifact Registry for image storage, and Cloud Run for deployment. You must ensure that containers with vulnerabilities rated above a common vulnerability scoring system (CVSS) score of "medium" are not deployed to production. What should you do?

A. Implement vulnerability scanning as part of the Cloud Build process. If any medium or higher vulnerabilities are detected, manually rebuild the image with updated components.

B. Perform manual vulnerability checks post-build, but before Cloud Run deployment. Implement a manual security-engineer-driven remediation process.

C. Configure Binary Authorization on Cloud Run to enforce image signatures. Create policies to allow deployment only for images passing a defined vulnerability threshold.

D. Utilize a vulnerability scanner during the Cloud Build stage and set Artifact Registry permissions to block images containing vulnerabilities above "medium."

Show Suggested Answer

by yokoyan at *Sept. 5, 2024, 9:14 a.m.*

Comments

Type your comment...

Submit

JohnDohertyDoe 7 months ago

Selected Answer: C

https://cloud.google.com/binary-authorization/docs/run/enabling-binauthz-cloud-run

upvoted 1 times

Mr_MIXER007 10 months, 3 weeks ago

Selected Answer: C

The best solution is C. Configure Binary Authorization on Cloud Run to enforce image signatures. Create policies to allow deployment only for images passing a defined vulnerability threshold.

Here's why this is the preferred approach:

Binary Authorization: Provides a strong, policy-based control mechanism for deploying containers. It ensures only trusted and verified images can be deployed to Cloud Run.
Vulnerability Threshold: By setting a policy within Binary Authorization, you can explicitly block the deployment of any container images that have vulnerabilities exceeding a CVSS score of "medium".
Automation: This approach enables automated enforcement of security standards at the deployment stage, preventing vulnerable images from reaching production.

upvoted 2 times

yokoyan 10 months, 3 weeks ago

Selected Answer: C

I think it's C.

upvoted 3 times