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 321 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 321
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization strives to be a market leader in software innovation. You provided a large number of Google Cloud environments so developers can test the integration of Gemini in Vertex AI into their existing applications or create new projects. Your organization has 200 developers and a five-person security team. You must prevent and detect proper security policies across the Google Cloud environments. What should you do? (Choose two.)

A. Apply organization policy constraints. Detect and monitor drifts by using Security Health Analytics.

B. Publish internal policies and clear guidelines to securely develop applications.

C. Use Cloud Logging to create log filters to detect misconfigurations. Trigger Cloud Run functions to remediate misconfigurations.

D. Apply a predefined AI-recommended security posture template for Gemini in Vertex AI in Security Command Center Enterprise or Premium tiers.

E. Implement the least privileged access Identity and Access Management roles to prevent misconfigurations.

Show Suggested Answer

by abdelrahman89 at *Oct. 25, 2024, 2:58 a.m.*

Comments

Type your comment...

Submit

YourFriendlyNeighborhoodSpider 4 months, 1 week ago

Selected Answer: AD

I agree with nah99, A and D seems reasonable given Vertex AI is mentioned.

upvoted 1 times

nah99 8 months ago

Selected Answer: AD

Specifically mentions gemini/vertex, so definitely D.

https://cloud.google.com/security-command-center/docs/security-posture-essentials-secure-ai-template

A & E are both good, but the requirement is prevent and detect, which better lines to A.

upvoted 2 times

MoAk 8 months ago

A & D for sure.

upvoted 1 times

BPzen 8 months ago

Selected Answer: AE

A. Apply organization policy constraints. Detect and monitor drifts by using Security Health Analytics.
Organization Policies:

Enforcing organization policies (e.g., constraints on resource locations, API access, or service usage) helps standardize security practices across all environments.
Developers can create and test environments without bypassing critical security controls.
Security Health Analytics (SHA):

SHA, available in Security Command Center Premium, detects and alerts on violations of security best practices and misconfigurations, such as overly permissive roles or public resource exposure.

E. Implement the least privileged access Identity and Access Management roles to prevent misconfigurations.
Least Privileged Access:

Assigning IAM roles based on the principle of least privilege prevents users from making changes outside their scope of work, reducing misconfiguration risks.

upvoted 1 times

abdelrahman89 9 months, 1 week ago

Selected Answer: AD

Answer A D

upvoted 1 times