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 315 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 315
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization is building a real-time recommendation engine using ML models that process live user activity data stored in BigQuery and Cloud Storage. Each new model developed is saved to Artifact Registry. This new system deploys models to Google Kubernetes Engine, and uses Pub/Sub for message queues. Recent industry news have been reporting attacks exploiting ML model supply chains. You need to enhance the security in this serverless architecture, specifically against risks to the development and deployment pipeline. What should you do?

A. Enable container image vulnerability scanning during development and pre-deployment. Enforce Binary Authorization on images deployed from Artifact Registry to your continuous integration and continuous deployment (CVCD) pipeline.

B. Thoroughly sanitize all training data prior to model development to reduce risk of poisoning attacks. Use IAM for authorization, and apply role-based restrictions to code repositories and cloud services.

C. Limit external libraries and dependencies that are used for the ML models as much as possible. Continuously rotate encryption keys that are used to access the user data from BigQuery and Cloud Storage.

D. Develop strict firewall rules to limit external traffic to Cloud Run instances. Integrate intrusion detection systems (IDS) for real-time anomaly detection on Pub/Sub message flows.

Show Suggested Answer

by abdelrahman89 at *Oct. 25, 2024, 1:49 a.m.*

Comments

Type your comment...

Submit

JohnDohertyDoe 7 months ago

Selected Answer: A

A should be the answer. Supply chain risks happen by exploiting vulnerabilities in the images. So scanning the image and blocking deployment secures against supply chain risks. This also matches with the requirement related to the deployment pipeline.

upvoted 1 times

zanhsieh 7 months, 2 weeks ago

Selected Answer: D

The question asked "...attacks exploiting ML model supply chains" and "...risks to the development and deployment pipeline", so we should look anything related to these:
A: No. Image scanning and enfore binary authorization only secure the end artifact.
B and C: No. Nothing related to secure development and deployment pipeline.
D: Yes, although this option just mentioned very shallow on how to implement them, e.g. IDS on pub/sub -> FortiSIEM, resticting network ingress for cloud run.
https://cloud.google.com/run/docs/securing/ingress#yaml

upvoted 1 times

abdelrahman89 9 months, 1 week ago

Selected Answer: A

Answer A

upvoted 2 times