Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 180 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 180
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization develops software involved in many open source projects and is concerned about software supply chain threats. You need to deliver provenance for the build to demonstrate the software is untampered.

What should you do?

A. 1. Hire an external auditor to review and provide provenance.
2. Define the scope and conditions.
3. Get support from the Security department or representative.
4. Publish the attestation to your public web page.

B. 1. Review the software process.
2. Generate private and public key pairs and use Pretty Good Privacy (PGP) protocols to sign the output software artifacts together with a file containing the address of your enterprise and point of contact.
3. Publish the PGP signed attestation to your public web page.

C. 1. Publish the software code on GitHub as open source.
2. Establish a bug bounty program, and encourage the open source community to review, report, and fix the vulnerabilities.

D. 1. Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build.
2. View the build provenance in the Security insights side panel within the Google Cloud console.

Show Suggested Answer

by Sanjana2020 at *Aug. 2, 2023, 9:14 p.m.*

Comments

Type your comment...

Submit

wojtek85 Highly Voted 1 year, 5 months ago

D is correct: https://cloud.google.com/build/docs/securing-builds/view-build-provenance

upvoted 6 times

i_am_robot Most Recent 1 year, 1 month ago

Selected Answer: D

The best option would be D. Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build and view the build provenance in the Security insights side panel within the Google Cloud console.

SLSA (pronounced “salsa”) is an end-to-end framework for ensuring the integrity of software artifacts throughout the software supply chain. The SLSA assurance levels provide a scalable compromise between the security benefits and the implementation costs. Level 3 is recommended for moderately to highly critical software and should provide strong, provenance-based security guarantees.

upvoted 3 times

cyberpunk21 1 year, 5 months ago

Selected Answer: D

D it is

upvoted 2 times

akg001 1 year, 5 months ago

Selected Answer: D

D is correct.

upvoted 2 times

Sanjana2020 1 year, 5 months ago

D is correct, I think?

upvoted 4 times