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 210 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 210

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your company uses Google Cloud and has publicly exposed network assets. You want to discover the assets and perform a security audit on these assets by using a software tool in the least amount of time.

What should you do?

A. Run a platform security scanner on all instances in the organization.

B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.

C. Contact a Google approved security vendor to perform the audit.

D. Notify Google about the pending audit, and wait for confirmation before performing the scan.

Show Suggested Answer

by pfilourenco at *Aug. 4, 2023, 10:54 a.m.*

Comments

Type your comment...

Submit

Bettoxicity 9 months, 4 weeks ago

Selected Answer: B

B is correct!

upvoted 1 times

Xoxoo 1 year, 4 months ago

Selected Answer: B

The most efficient approach to discover publicly exposed network assets and perform a security audit on them in the least amount of time is:

B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.

Here's why Option B is the recommended choice:

Cloud Asset Inventory: Using Cloud Asset Inventory allows you to quickly identify all the external assets and resources in your Google Cloud environment. This includes information about your projects, instances, storage buckets, and more. This step is crucial for understanding the scope of your audit.

Network Security Scanner: Once you have identified the external assets, you can run a network security scanner to assess the security of these assets. Network security scanners can help identify vulnerabilities and potential security risks quickly.

upvoted 1 times

Xoxoo 1 year, 4 months ago

Option A (Running a platform security scanner on all instances) might be time-consuming, especially if you have a large number of instances, and it doesn't address other types of publicly exposed assets besides instances.

Option C (Contacting a Google-approved security vendor) is a valid option, but it may introduce delays as you wait for the vendor's availability. It's also likely to involve additional costs.

Option D (Notifying Google about the pending audit) is not a typical step for performing a security audit on your own network assets. It's more applicable if you're engaging with Google for a security review or penetration testing but not for a self-initiated audit.

upvoted 1 times

cyberpunk21 1 year, 5 months ago

Selected Answer: B

B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.

Cloud Asset Inventory allows you to see all of your Google Cloud assets. By using it, you can quickly identify which assets are externally accessible. Once identified, you can then run a specialized network security scanner against only these assets, making the process efficient.
C. Contact a Google approved security vendor to perform the audit.

While using an external vendor can be beneficial for thoroughness, it may not meet the criteria of accomplishing the task in the "least amount of time."

upvoted 2 times

anshad666 1 year, 5 months ago

Selected Answer: B

Should be B

upvoted 1 times

pfilourenco 1 year, 5 months ago

Selected Answer: B

B is the correct.

upvoted 3 times