◉ **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 110 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 110
Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?

  A. Use Security Health Analytics to determine user activity.

  B. Use the Cloud Monitoring console to filter audit logs by user.

  C. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.

  D. Use the Logs Explorer to search for user activity.

Show Suggested Answer

by 👤 **mT3** at *May 19, 2022, 4:08 p.m.*

Comments

Type your comment...

Submit

👤 **Medofree** Highly Voted 👍 2 years, 2 months ago
Selected Answer: D

D.

We use audit logs by searching the Service Account and checking activities in the past 2 months. (the user identity will not be seen since he used the SA identity but we can make correlations based on ip address, working hour, etc.)

👍 ↩ 🏳 upvoted 14 times

⊟ 👤 **AzureDP900** 1 year, 8 months ago

D is right, I agree

👍 ↩ 🏳 upvoted 3 times

⊟ 👤 **mikesp** `Highly Voted 👍` 2 years, 1 month ago

`Selected Answer: D`

B is intended to mislead the public. Cloud Monitoring provides only metrics. To check user activity is necessary to go to Cloud Logging and search on Audit Logs.

👍 ↩ 🏳 upvoted 8 times

⊟ 👤 **chickenstealers** `Most Recent ⊙` 1 year, 6 months ago

B is correct answer
https://cloud.google.com/docs/security/compromised-credentials
Monitor for anomalies in service account key usage using Cloud Monitoring.

👍 ↩ 🏳 upvoted 2 times

⊟ 👤 **Sammydp202020** 1 year, 5 months ago

Cloud monitoring/logging is a service enabler to capture the logs. Question asks -- How does one check for user activity:

So, the response warranted is D - logs explorer.

https://cloud.google.com/docs/security/compromised-credentials#look_for_unauthorized_access_and_resources

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **gcpengineer** 1 year, 2 months ago

2 months..is long time ti check data access logs

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **zellck** 1 year, 10 months ago

`Selected Answer: D`

D is the answer.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **mT3** 2 years, 2 months ago

`Selected Answer: B`

Correct. Answer is (B).
Investigate the potentially unauthorized activity and restore the account.
Ref.https://support.google.com/a/answer/2984349

👍 ↩ 🏳 upvoted 3 times