EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 298 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 298
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A security audit uncovered several inconsistencies in your project's Identity and Access Management (IAM) configuration. Some service accounts have overly permissive roles, and a few external collaborators have more access than necessary. You need to gain detailed visibility into changes to IAM policies, user activity, service account behavior, and access to sensitive projects. What should you do?

A. Configure Google Cloud Functions to be triggered by changes to IAM policies. Analyze changes by using the policy simulator, send alerts upon risky modifications, and store event details.

B. Enable the metrics explorer in Cloud Monitoring to follow the service account authentication events and build alerts linked on it.

C. Use Cloud Audit Logs. Create log export sinks to send these logs to a security information and event management (SIEM) solution for correlation with other event sources.

D. Deploy the OS Config Management agent to your VMs. Use OS Config Management to create patch management jobs and monitor system modifications.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 9:53 p.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: C

This approach allows you to monitor and analyze IAM changes comprehensively, ensuring that you can detect and respond to any security issues effectively
https://cloud.google.com/iam/docs/audit-logging

upvoted 1 times

json4u 9 months, 2 weeks ago

Selected Answer: C

It's C

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

C - Comprehensive Logging: Cloud Audit Logs capture a wide range of activities, including IAM policy changes, user logins, API calls, and resource access. This provides a comprehensive view of your organization's IAM activity.
Log Export: By creating log export sinks, you can send Cloud Audit Logs to a SIEM solution, where they can be correlated with other event sources to identify potential security threats.
Detailed Analysis: SIEM solutions can provide advanced analytics and reporting capabilities, allowing you to analyze IAM changes, detect anomalies, and identify potential security risks.

upvoted 3 times