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 199 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 199

Topic #: 1

[All Professional Cloud Security Engineer Questions]

As part of your organization's zero trust strategy, you use Identity-Aware Proxy (IAP) to protect multiple applications. You need to ingest logs into a Security Information and Event Management (SIEM) system so that you are alerted to possible intrusions.

Which logs should you analyze?

A. Data Access audit logs

B. Policy Denied audit logs

C. Cloud Identity user log events

D. Admin Activity audit logs

Show Suggested Answer

by gcp4test at *Aug. 4, 2023, 3:29 p.m.*

Comments

Type your comment...

Submit

gcp4test Highly Voted 1 year, 11 months ago

Selected Answer: A

The data_access log name only appears if there was traffic to your resource after you enabled Cloud Audit Logs for IAP.

Click to expand the date and time of the access you want to review.

Authorized access has a blue i icon.
Unauthorized access has an orange !! icon.
"

https://cloud.google.com/iap/docs/audit-log-howto

upvoted 8 times

zanhsieh Most Recent 7 months, 2 weeks ago

Selected Answer: A

I will choose A. Not B because we won't get the valuable information - it just reports what were denied. We are looking for what were not get denied so those can be formed as alerts.

upvoted 1 times

Pime13 7 months, 3 weeks ago

Selected Answer: B

B. Policy Denied audit logs

Policy Denied audit logs are crucial because they record instances where access to resources was denied based on your IAP policies. These logs can help you identify and investigate unauthorized access attempts, which are critical for detecting potential intrusions.

While Data Access and Admin Activity audit logs provide valuable information about resource access and administrative actions, Policy Denied logs specifically highlight security-related events that could indicate malicious activity.

upvoted 2 times

BPzen 8 months ago

Selected Answer: B

Policy Denied Audit Logs:
These logs capture access attempts denied by Identity-Aware Proxy (IAP) policies.
They indicate potential unauthorized or suspicious activity, such as users attempting to access resources they are not authorized for.
These logs are critical for identifying possible intrusions or misconfigurations in your zero-trust strategy.

upvoted 1 times

Mr_MIXER007 10 months, 4 weeks ago

Selected Answer: A

https://cloud.google.com/iap/docs/audit-log-howto#viewing_audit
A

upvoted 1 times

3d9563b 1 year ago

Selected Answer: B

To effectively monitor and detect possible intrusions related to IAP-protected applications, focusing on Policy Denied audit logs provides the most relevant insights into access control and denial events. These logs help you track access violations and unauthorized attempts, aligning with your zero trust strategy and enabling timely alerts in your SIEM system.

upvoted 1 times

jujanoso 1 year ago

Selected Answer: B

B. Policy Denied audit logs can show when unauthorized users or devices tried to access protected applications and were blocked, which is crucial for identifying and responding to threats. As part of a zero trust strategy, leveraging Identity-Aware Proxy (IAP) involves closely monitoring and analyzing logs to detect potential intrusions and unauthorized activities.

upvoted 1 times

glb2 1 year, 4 months ago

Selected Answer: B

B. Policy Denied audit logs: These logs contain records of access attempts that were denied by IAP policies. Analyzing these logs can help identify unauthorized access attempts and potential intrusion attempts blocked by IAP.

upvoted 2 times

desertlotus1211 1 year, 5 months ago

Answer is B

upvoted 2 times

cyberpunk21 1 year, 11 months ago

cyberpunk21 1 year, 11 months ago

Selected Answer: A

A is fire

upvoted 2 times

Mithung30 1 year, 11 months ago

Selected Answer: A

https://cloud.google.com/iap/docs/audit-log-howto#viewing_audit

upvoted 2 times

EXAMTOPICS

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses