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 248 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 248
Topic #: 1
[All Professional Cloud Security Engineer Questions]

During a routine security review, your team discovered a suspicious login attempt to impersonate a highly privileged but regularly used service account by an unknown IP address. You need to effectively investigate in order to respond to this potential security incident. What should you do?

A. Enable Cloud Audit Logs for the resources that the service account interacts with. Review the logs for further evidence of unauthorized activity.

B. Review Cloud Audit Logs for activity related to the service account. Focus on the time period of the suspicious login attempt.

C. Run a vulnerability scan to identify potentially exploitable weaknesses in systems that use the service account.

D. Check Event Threat Detection in Security Command Center for any related alerts. Cross-reference your findings with Cloud Audit Logs.

Show Suggested Answer

by yokoyan at *Sept. 5, 2024, 9:15 a.m.*

Comments

Type your comment...

Submit

BPzen 8 months ago

Selected Answer: D

Event Threat Detection (ETD) in Security Command Center (SCC):

ETD automatically detects suspicious activity, such as anomalous service account usage or potential credential compromise, by analyzing logs in near real-time.
Checking ETD alerts can quickly surface relevant insights about the suspicious activity.
Cloud Audit Logs:

Cross-referencing findings in ETD with Cloud Audit Logs helps confirm the scope of the incident by providing a complete history of actions performed by the service account, including the time of the suspicious login attempt.

upvoted 1 times

dv1 9 months, 1 week ago

Selected Answer: B

Question does not say that SCC is enabled, does it?

upvoted 3 times

KLei 8 months, 2 weeks ago

" need to effectively investigate in order to respond to this potential security incident"

upvoted 2 times

Mr_MIXER007 10 months, 3 weeks ago

Selected Answer: D

Selected Answer: D

upvoted 1 times

1e22522 10 months, 3 weeks ago

Selected Answer: D

D. Check Event Threat Detection in Security Command Center for any related alerts. Cross-reference your findings with Cloud Audit Logs.
Explanation:

Security Command Center (SCC) is Google Cloud's security and risk management platform. Event Threat Detection within SCC is specifically designed to detect suspicious activity, such as unauthorized logins, and generates alerts based on predefined threat patterns. This tool would help you quickly identify if the suspicious login attempt is part of a known threat pattern.

After checking for alerts in Event Threat Detection, cross-referencing with Cloud Audit Logs will give you detailed insights into the actions performed by the service account, allowing you to investigate the extent of any potential breach.

upvoted 2 times

yokoyan 10 months, 3 weeks ago

Selected Answer: D

I think it's D.

upvoted 1 times