Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 216 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 216

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization wants to be continuously evaluated against CIS Google Cloud Computing Foundations Benchmark v1.3.0 (CIS Google Cloud Foundation 1.3). Some of the controls are irrelevant to your organization and must be disregarded in evaluation. You need to create an automated system or process to ensure that only the relevant controls are evaluated.

What should you do?

A. Mark all security findings that are irrelevant with a tag and a value that indicates a security exception. Select all marked findings, and mute them on the console every time they appear. Activate Security Command Center (SCC) Premium.

B. Activate Security Command Center (SCC) Premium. Create a rule to mute the security findings in SCC so they are not evaluated.

C. Download all findings from Security Command Center (SCC) to a CSV file. Mark the findings that are part of CIS Google Cloud Foundation 1.3 in the file. Ignore the entries that are irrelevant and out of scope for the company.

D. Ask an external audit company to provide independent reports including needed CIS benchmarks. In the scope of the audit, clarify that some of the controls are not needed and must be disregarded.

Show Suggested Answer

by pfilourenco at *Aug. 4, 2023, 11:20 a.m.*

Comments

Type your comment...

Submit

Xoxoo 10 months, 1 week ago

Selected Answer: B

Option A is a reasonable approach, but it involves ongoing manual intervention to mute security findings and may not be the most efficient method, especially when dealing with a large number of findings.

Option B, activating Security Command Center (SCC) Premium and creating rules to mute security findings, is a more automated and scalable approach. SCC Premium allows you to create custom security rules to automatically filter or mute findings based on your organization's requirements. This can help reduce the noise and ensure that irrelevant findings are not evaluated.

upvoted 2 times

Xoxoo 10 months, 1 week ago

Answer: B

upvoted 2 times

ArizonaClassics 10 months, 4 weeks ago

The right answer is B. please disregard the former

upvoted 1 times

ArizonaClassics 10 months, 4 weeks ago

A. Mark all security findings that are irrelevant with a tag and a value that indicates a security exception. Select all marked findings, and mute them on the console every time they appear. Activate Security Command Center (SCC) Premium.

This option might require manual intervention to tag and mute findings every time they appear. This can be labor-intensive and prone to error, thus not ideal for an automated, ongoing evaluation.

upvoted 1 times

cyberpunk21 11 months, 1 week ago

Selected Answer: B

using Rules, we can automate this.

upvoted 2 times

anshad666 11 months, 1 week ago

Selected Answer: B

https://cloud.google.com/security-command-center/docs/how-to-mute-findings

upvoted 2 times

pfilourenco 11 months, 4 weeks ago

Selected Answer: B

B - Create a rule to mute!

upvoted 2 times

gcp4test 11 months, 4 weeks ago

yes rules

upvoted 1 times