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 201 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 201

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your company's Google Cloud organization has about 200 projects and 1,500 virtual machines. There is no uniform strategy for logs and events management, which reduces visibility for your security operations team. You need to design a logs management solution that provides visibility and allows the security team to view the environment's configuration.

What should you do?

A. 1. Create a dedicated log sink for each project that is in scope.
2. Use a BigQuery dataset with time partitioning enabled as a destination of the log sinks.
3. Deploy alerts based on log metrics in every project.
4. Grant the role "Monitoring Viewer" to the security operations team in each project.

B. 1. Create one log sink at the organization level that includes all the child resources.
2. Use as destination a Pub/Sub topic to ingest the logs into the security information and event. management (SIEM) on-premises, and ensure that the right team can access the SIEM.
3. Grant the Viewer role at organization level to the security operations team.

C. 1. Enable network logs and data access logs for all resources in the "Production" folder.
2. Do not create log sinks to avoid unnecessary costs and latency.
3. Grant the roles "Logs Viewer" and "Browser" at project level to the security operations team.

D. 1. Create one sink for the "Production" folder that includes child resources and one sink for the logs ingested at the organization level that excludes child resources.
2. As destination, use a log bucket with a minimum retention period of 90 days in a project that can be accessed by the security team.
3. Grant the security operations team the role of Security Reviewer at organization level.

D. Grant the security operations team the role of Security Reviewer at organization level.

Show Suggested Answer

by K1SMM at *Aug. 4, 2023, 1:17 a.m.*

Comments

Type your comment...

Submit

zanhsieh 7 months, 1 week ago

Selected Answer: B

B.
A: No. Granting monitoring.viewer to security team doesn't help to see the log since log to BQ.
C: No. How does the security team to view logs if no log sink created? This option means no log streaming in.
D: No. "90 days retention period" and "Security Reviewer" are not the question asked for.

upvoted 1 times

BPzen 8 months ago

Selected Answer: B

D. Revised for a No-Folder Scenario:

Create a single organization-level log sink:

Include all child resources (projects) to centralize logging for the entire organization.
Configure log filters:

If you want to scope the logs (e.g., for "production" projects only), use labels or other identifiers on projects to filter relevant logs into the sink.
Destination:

Use a log bucket in a dedicated project accessible to the security team.
Ensure the log bucket has a minimum retention period of 90 days (or longer if required).
Grant Access:

Assign the Security Reviewer role to the security operations team at the organization level. This role provides read access to logs across all resources in the organization.

upvoted 1 times

b6f53d8 1 year, 5 months ago

Selected Answer: D

B required external on prem SIEM it is not recommended solution

upvoted 1 times

b6f53d8 1 year, 5 months ago

For sure not A, but I'm not sure B, because it required external SIEM, in my opinion D is the best option

upvoted 1 times

Andrei_Z 1 year, 10 months ago

Selected Answer: B

It is B because you need a SIEM to actually analyse the configurations of the environments

upvoted 2 times

ArizonaClassics 1 year, 11 months ago

B. 1. Create one log sink at the organization level that includes all the child resources.
2. Use as destination a Pub/Sub topic to ingest the logs into the security information and event management (SIEM) on-premises, and ensure that the right team can access the SIEM.

upvoted 2 times

cyberpunk21 1 year, 11 months ago

Selected Answer: B

B is good

upvoted 1 times

upvoted 1 times

pfilourenco 1 year, 11 months ago

Selected Answer: B

B makes sense

upvoted 1 times

a190d62 1 year, 11 months ago

Selected Answer: B

B

https://github.com/GoogleCloudPlatform/community/blob/master/archived/exporting-security-data-to-your-siem/index.md

upvoted 1 times

K1SMM 1 year, 11 months ago

B makes sense cuz viewer role permits view environments configuration

upvoted 1 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses