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 269 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 269
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization is using Security Command Center Premium as a central tool to detect and alert on security threats. You also want to alert on suspicious outbound traffic that is targeting domains of known suspicious web services. What should you do?

A. Create a DNS Server Policy in Cloud DNS and turn on logs. Attach this policy to all Virtual Private Cloud networks with internet connectivity.

B. Forward all logs to Chronicle Security Information and Event Management. Create an alert for suspicious egress traffic to the internet.

C. Create a Cloud Intrusion Detection endpoint. Connect this endpoint to all Virtual Private Cloud networks with internet connectivity.

D. Create an egress firewall policy with Threat Intelligence as the destination. Attach this policy to all Virtual Private Cloud networks with internet connectivity.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:36 a.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: D

https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview#cases-overview

upvoted 1 times

Zek 7 months, 3 weeks ago

Selected Answer: D

D seems right to me.
https://cloud.google.com/firewall/docs/firewall-policies-rule-details#threat-intelligence-fw-policy

Firewall policy rules let you secure your network by allowing or blocking traffic based on Google Threat Intelligence data. For egress rules, specify the destination by using one or more destination Google Threat Intelligence lists.

upvoted 1 times

cachopo 7 months, 3 weeks ago

Selected Answer: D

The correct option is D.
Since it is not necessary to send logs to Chronicle if you are already paying for SCC Premium, which can alert on any outbound traffic that triggers the Threat Intelligence firewall rule. Otherwise, I don't see any point in them explicitly telling you that you have contracted SCC Premium.

upvoted 1 times

MoAk 8 months ago

Selected Answer: D

https://cloud.google.com/firewall/docs/firewall-policies-rule-details#threat-intelligence-fw-policy

upvoted 1 times

BondleB 8 months, 4 weeks ago

Selected Answer: B

https://cloud.google.com/chronicle/docs/overview

Option B addresses the alert on suspicious outbound traffic while option D does not.

upvoted 3 times

sanmeow 9 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

brpjp 10 months, 1 week ago

Answer D is correct as per Gemini:
Subscribe to threat intelligence feeds that provide updated lists of known suspicious domains and IP addresses.
Integrate these feeds with your security solutions to identify and block outbound connections to these resources.

upvoted 3 times

Pach1211 10 months, 2 weeks ago

I´m thinking D

upvoted 2 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 1 times