PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs.

What should you do?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.

B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.

C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.

D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Correct Answer: A

Reference: https://cloud.google.com/logging/docs/logs-based-metrics/

QUESTION 2

Your organization develops software involved in many open source projects and is concerned about software supply chain threats. You need to deliver provenance for the build to demonstrate the software is untampered. What should you do?

A. 1. Hire an external auditor to review and provide provenance.

2.

Define the scope and conditions.

3.

Get support from the Security department or representative.

4.

Publish the attestation to your public web page.

B. 1. Review the software process.

2.

Generate private and public key pairs and use Pretty Good Privacy (PGP) protocols to sign the output software artifacts together with a file containing the address of your enterprise and point of contact.

3.

Publish the PGP signed attestation to your public web page.

C. 1. Publish the software code on GitHub as open source.

2. Establish a bug bounty program, and encourage the open source community to review, report, and fix the vulnerabilities.

D. 1. Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build.

2. View the build provenance in the Security insights side panel within the Google Cloud console.

Correct Answer: D

https://cloud.google.com/build/docs/securing-builds/view-build-provenance

QUESTION 3

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery What should you do?

A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.

B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.

C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.

D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Correct Answer: B

https://cloud.google.com/bigquery/docs/scan-with-dlp

Cloud Data Loss Prevention API allows to detect and redact or remove sensitive data before the comments or reviews are published. Cloud DLP will read information from BigQuery, Cloud Storage or Datastore and scan it for sensitive data.

QUESTION 4

A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.

Which connectivity option should be implemented?

A. VPC peering

B. Cloud VPN

C. Cloud Interconnect

D. Shared VPC

Correct Answer: A

Peering two VPCs does permit traffic to flow between the two shared networks, but it\\'s only bi-directional. Peered VPC networks remain administratively separate.

QUESTION 5

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties