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.pass4itsure.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 customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.

How should this be accomplished?

A. Create a firewall rule to block internet traffic from the VM.

B. Provision a NAT Gateway to access the Cloud Storage API endpoint.

C. Enable Private Google Access on the VPC.

D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Correct Answer: C

https://cloud.google.com/vpc/docs/private-google-access

QUESTION 2

Your organization wants to protect all workloads that run on Compute Engine VM to ensure that the instances weren\\'t compromised by boot-level or kernel-level malware. Also, you need to ensure that data in use on the VM cannot be read by

the underlying host system by using a hardware-based solution.

What should you do?

A. 1 Use Google Shielded VM including secure boot Virtual Trusted Platform Module (vTPM) and integrity monitoring 2 Create a Cloud Run function to check for the VM settings generate metrics and run the function regularly

B. 1 Activate Virtual Machine Threat Detection in Security Command Center (SCO Premium 2 Monitor the findings in SCC

C. 1 Use Google Shielded VM including secure boot Virtual Trusted Platform Module (vTPM) and integrity monitoring 2 Activate Confidential Computing 3 Enforce these actions by using organization policies

D. 1 Use secure hardened images from the Google Cloud Marketplace 2 When deploying the images activate the Confidential Computing option 3 Enforce the use of the correct images and Confidential Computing by using organization policies

Correct Answer: C

QUESTION 3

Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements. What should you do?

A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.

B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository Verify that the image is not deprecated.

C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.

D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: A

QUESTION 4

Your organization\\'s Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

A. Deploy a Cloud NAT Gateway in the service project for the MIG.

B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.

C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.

D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

Correct Answer: C

QUESTION 5

A customer terminates an engineer and needs to make sure the engineer\\'s Google account is automatically deprovisioned.

What should the customer do?

A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.

B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.

C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.

D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Correct Answer: C

https://cloud.google.com/identity/solutions/automate-user- provisioning#cloud_identity_automated_provisioning

"Cloud Identity has a catalog of automated provisioning connectors, which act as a bridge between Cloud Identity and third-party cloud apps."

PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps
PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Study Guide