Cyscale

Google Cloud Security Cheat Sheet

Enhance your cloud security using these essential commands to safeguard your VMs, databases, buckets, and many others. Using this cheatsheet, you can secure your Google Cloud resources in no time.

Storage

Enable uniform bucket-level access for Cloud Storage Buckets

```
gsutil uniformbucketlevelaccess set on gs://<bucketName/
```

Ensure Cloud Storage Bucket is not anonymously or publicly accessible

```
gsutil iam ch -d allAuthenticatedUsers -d allUsers
gs://<bucketName>
```

VMs

Enable Shielded VM for Compute Instances

Firstly, stop the instance:

```
gcloud compute instances stop <instanceName>
```

Then, enable Shielded VM:

```
gcloud compute instances update <instanceName>
--shielded-vtpm --shieldedvm-integrity-monitoring
```

Block Project-Wide SSH keys on Compute Instances

```
gcloud compute instances add-metadata --metadata
blockproject-ssh-keys=TRUE
```

SQL

Ensure the Cloud SQL database instances require all incoming connections to use SSL*

*ensure that your app uses the SSL/TLS certificate provided by the CloudSQL instance or connect to the database through Cloud SQL Auth Proxy

```
gcloud sql instances patch <instanceName> --require-ssl
```

Remove public IPs for cloud SQL instances and set a private IP

```
gcloud sql instances patch <instanceName>
--network=<VPCNetworkName> --noassign-ip
```

Others

Enable DNSSEC for Cloud DNS

```
gcloud dns managed-zones update <zoneName>
--dnssec-state on
```

Ensure KMS encryption keys are rotated within a period of 90 days

```
gcloud kms keys update <keyName> --keyring=<keyRing>
--location=<location> --nextrotation-time=<nextRotationTime>
--rotation-period=<rotationPeriod>
```

Configure an Essential Contact for your organization

```
gcloud essential-contacts create --email="<email>"
--notification-categories="<notificationCategories>"
--language="<language>" --<resourceType>="<resourceID>"
```

Enable Cloud Asset Inventory

```
gcloud services enable cloudasset.googleapis.com
```

Delete the default network for a Google Cloud project

```
gcloud compute networks delete default
```

Enable VPC Flow Logs for every subnet in a VPC network

```
gcloud compute networks subnets list --network <network>
--format="table(name)" | tail -n +2 | xargs -p -n 1 -I
'<subnet>' gcloud compute networks subnets update
'<subnet>' --enable-flow-logs --logging-aggregation-
interval=interval-5-sec --logging-flow-sampling=1
--logging-metadata=include-all
```

You can find these commands, and more, in Cyscale. The Cyscale Platform is a powerful cloud security solution that automates cloud misconfiguration checks, strengthens cloud security, and simplifies compliance tasks. By leveraging advanced contextual analysis and providing actionable insights, the platform empowers organizations to confidently embrace the cloud while ensuring a robust security posture. Streamline your cloud security management and gain peace of mind with Cyscale.