Cloud Security Posture Management Manual (Google Cloud Platform)

Go to > Cyber Incident Monitoring

Requirements

Set Up Cloud Account Access

Note: To set up CSPM for a GCP project, you need admin privileges for the project.

## Manual Authentication for GCP

To authenticate manually and monitor a GCP organization, you must:

1. Create a new GCP service account
2. Assign it the necessary roles (organization/project level)
3. Generate credentials
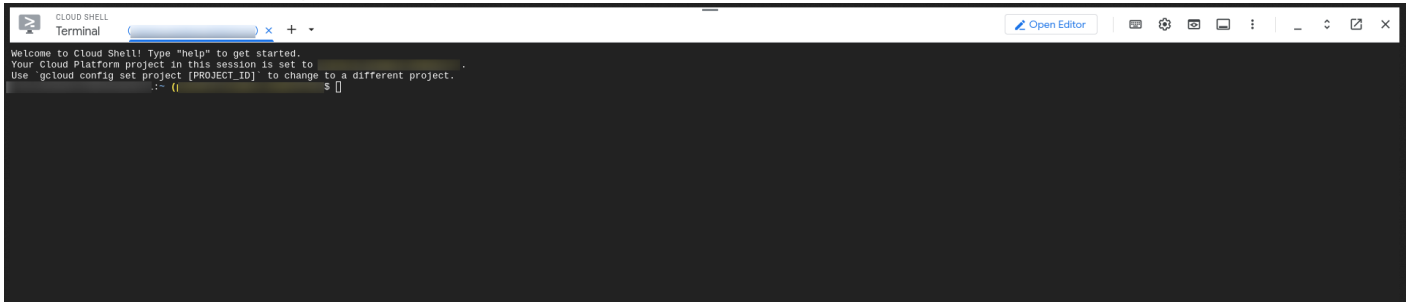4. Provide those credentials to the CSPM integration

Steps to Set Up CSPM on GCP

1. Go to Google Cloud Console.

In the top-right corner, click on the **Cloud Shell** Icon
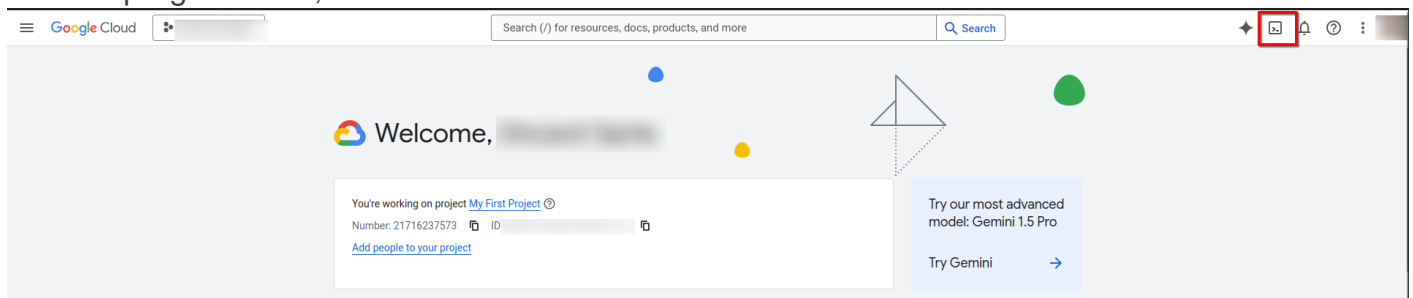
You should be seeing the image below

2. Set Your Active Project

Run this command to select the GCP project where you want to create the service account:

gcloud config set project **<PROJECT_ID>**

3. Create a new service account:

gcloud iam service-accounts create **<SA_NAME>** \
   --description="Elastic agent service account for CSPM" \
   --display-name="Elastic agent service account for CSPM" \
   --project=**<PROJECT_ID>**

4. Assign Required IAM Roles

Replace **<ORG_ID>** and **<PROJECT_ID>** in the commands below:

- **Assign the necessary roles to the service account at Organization Level:**

  gcloud organizations add-iam-policy-binding **<ORG_ID>** \
  --member=serviceAccount:**<SA_NAME>**@**<PROJECT_ID>**.iam.gserviceaccount.com \
  --role=roles/cloudasset.viewer
  gcloud organizations add-iam-policy-binding **<ORG_ID>** \
  --member=serviceAccount:**<SA_NAME>**@**<PROJECT_ID>**.iam.gserviceaccount.com \
  --role=roles/browser

- **Assign the necessary roles to the service account at Project Level:**

  gcloud projects add-iam-policy-binding **<PROJECT_ID>** \
  --member=serviceAccount:**<SA_NAME>**@**<PROJECT_ID>**.iam.gserviceaccount.com \
  --role=roles/cloudasset.viewer

```
gcloud projects add-iam-policy-binding <PROJECT_ID> \
--member=serviceAccount:<SA_NAME>@<PROJECT_ID>.iam.gserviceaccount.com \
--role=roles/browser
```

Note: *The Cloud Asset Viewer role grants read access to cloud asset metadata. The Browser role grants read access to the project hierarchy.*

5. Download the credentials JSON (first, replace <KEY_FILE> with the location where you want to save it):

```
gcloud iam service-accounts keys create <KEY_FILE> \
   --iam-account=<SA_NAME>@<PROJECT_ID>.iam.gserviceaccount.com
```

6. Provide CyTech the following values:

- Project ID (the project where you want to provision the compute instance that will run CSPM)
- Credentials JSON values

If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.

Revision #9
Created 12 February 2025 10:37:35 by Vincent Sarte
Updated 14 February 2025 02:30:45 by Vincent Sarte