GitHub repository

Infrastructure Provisioning Project

Default VPC Network 10.1.0.0/16

Firewall

Google Managed SaaS ConfigSync

Cloud Source Repositories mirror

GitHub mirrors

Merge

code review

Pull Request

Branch

vulnerability scan

Commit

Managed Project

logs/events

Managed Project

Project A production

logs/events

Security Command Center

Production Folder

logs/events

Project A experimentation

Experimentation Folder

Google Cloud

DMIA Infrastructure Provisioning

This architecture uses a single priviledged account to provision infrastructure.

This allows DMIA staff to operate with lower priviledged accounts while offering a self-service model to users via GitHub Pull Requests.

This account is used to create:

- A GCP project inside our experimentation/production folders
- A budget for the project
- An initial set of IAM users who can access the project

Each project comes with it's own VPC network and firewall rules. Expermentation and production folders enforce different policies.

All logs in all projects are aggregated in Security Command Center.

Minor changes will allow this service to provision resources in AWS and Azure as well as resources defined with Terraform.