Permission Mining in GCP

Colin Estep
Netskope Threat Labs

Agenda

- IAM Exposure
- IAM in GCP
- A Real Example from GCP
- Permission Mining Solution
- Results and Remediation

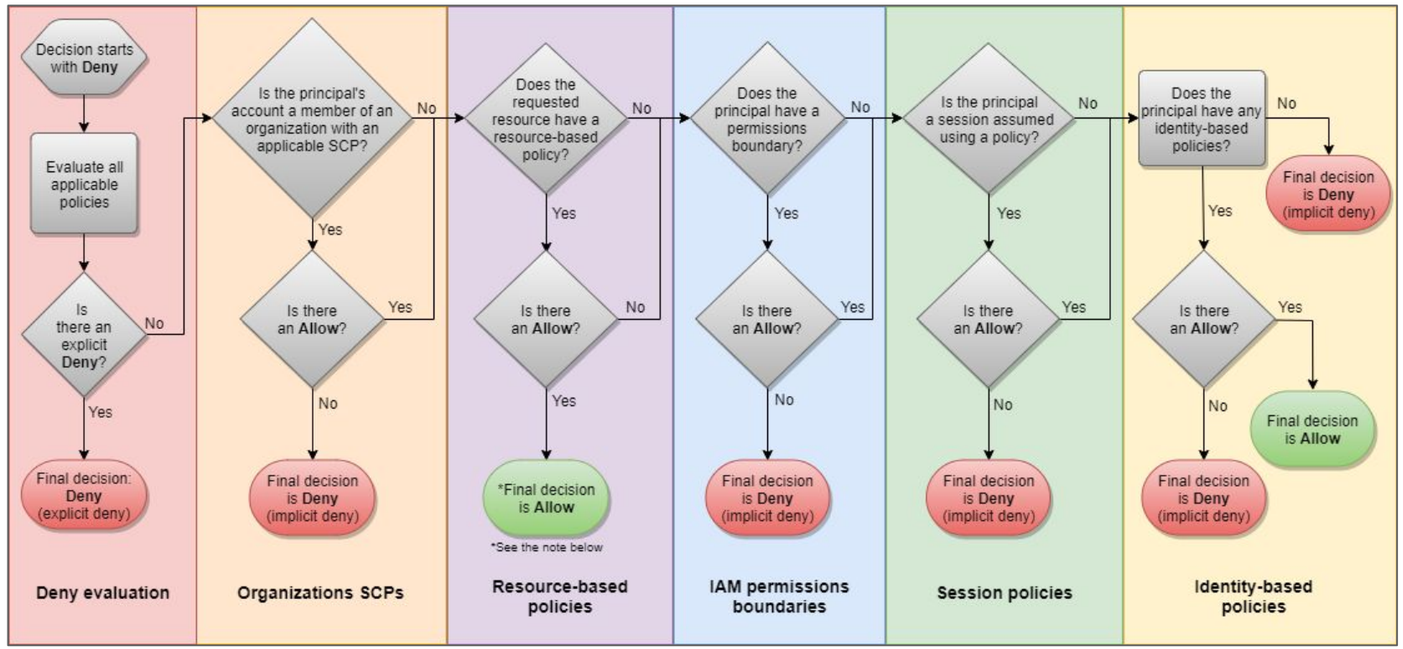
IAM Exposure

IAM Exposure

- What can your users do?
- Could a compromised credential result in administrator access?
- CodeSpaces was put out of business

Why is IAM challenging?

- Too many privileges may be given in a time crunch
- Confusion about the capability of granted permissions
- It is difficult to audit indirect permissions at scale



IAM in GCP

Identities in GCP

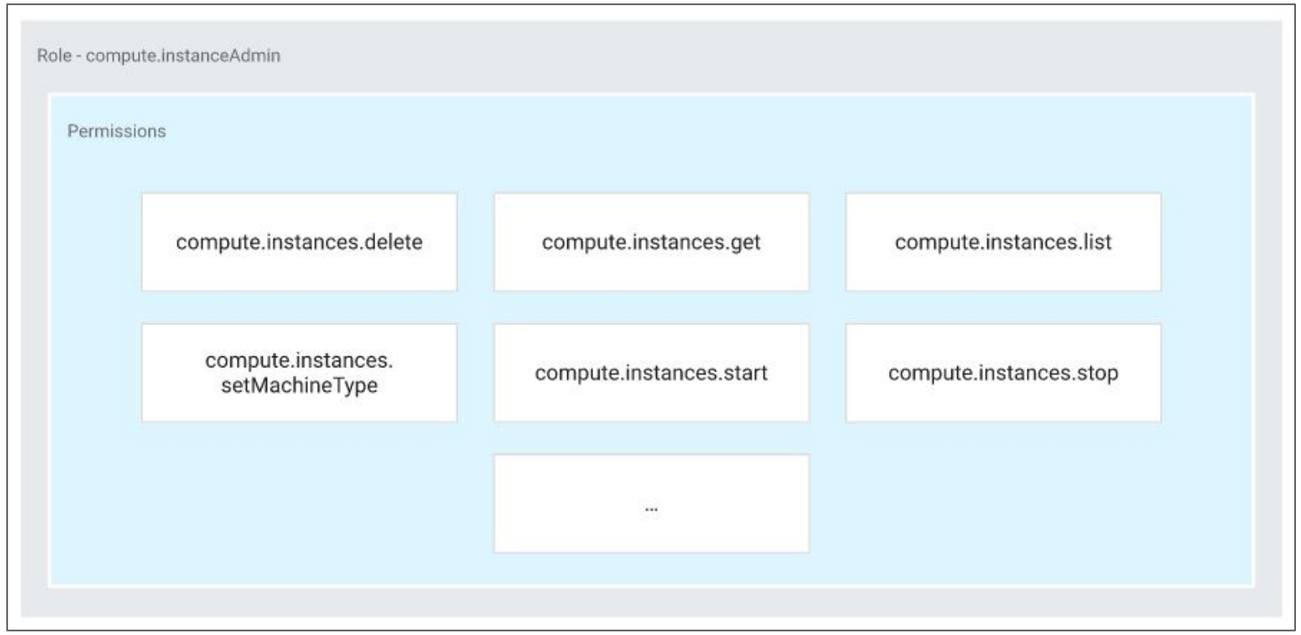
There are 4 different types of identities in GCP, which are called Members:

- User
- Group
- Domain
- Service Account

All of these are assigned permissions in the same way

GCP Terminology

- **Permission**: Allows a specific API call
- **Role**: A collection of permissions



GCP Terminology

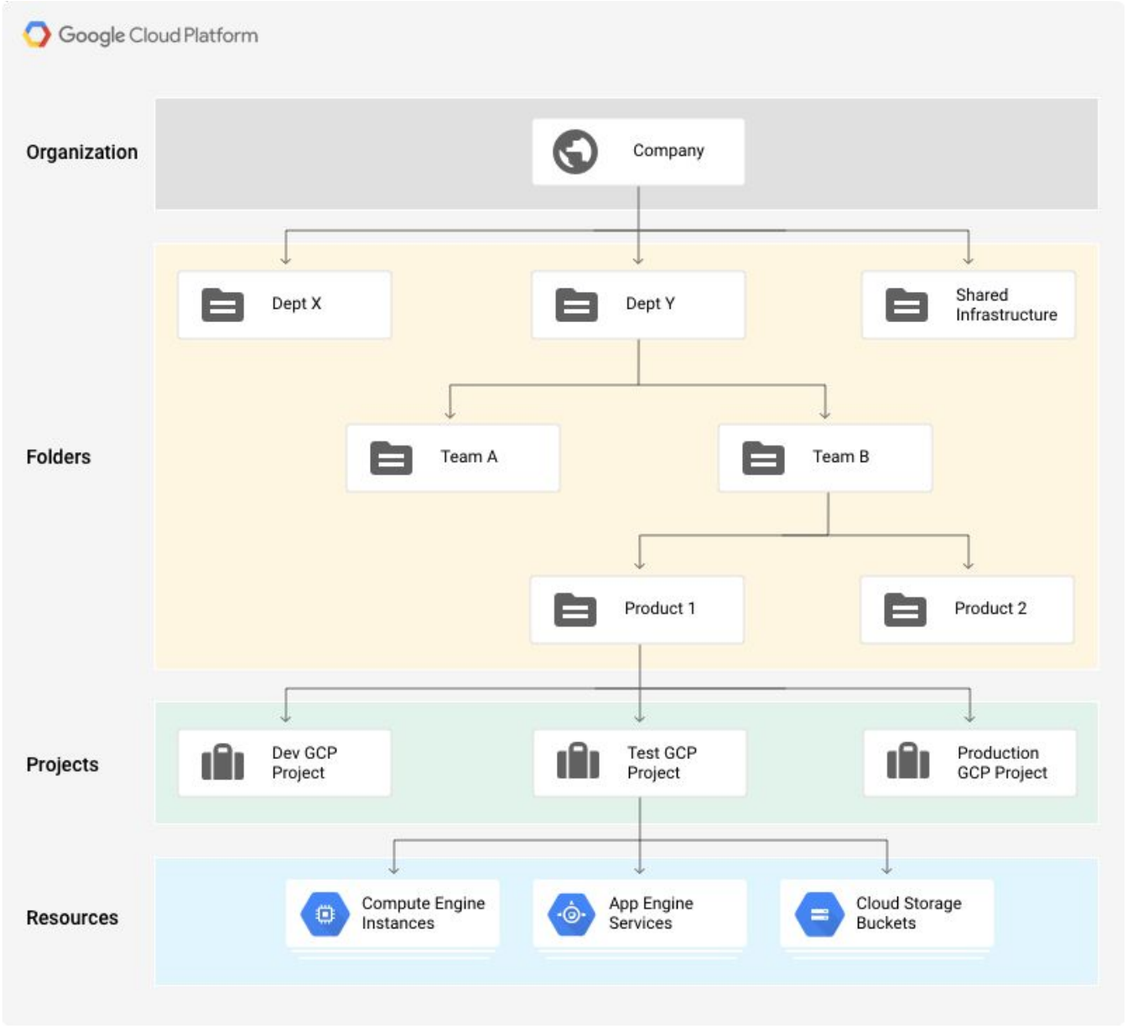
- **Binding**: When a role is assigned to a member

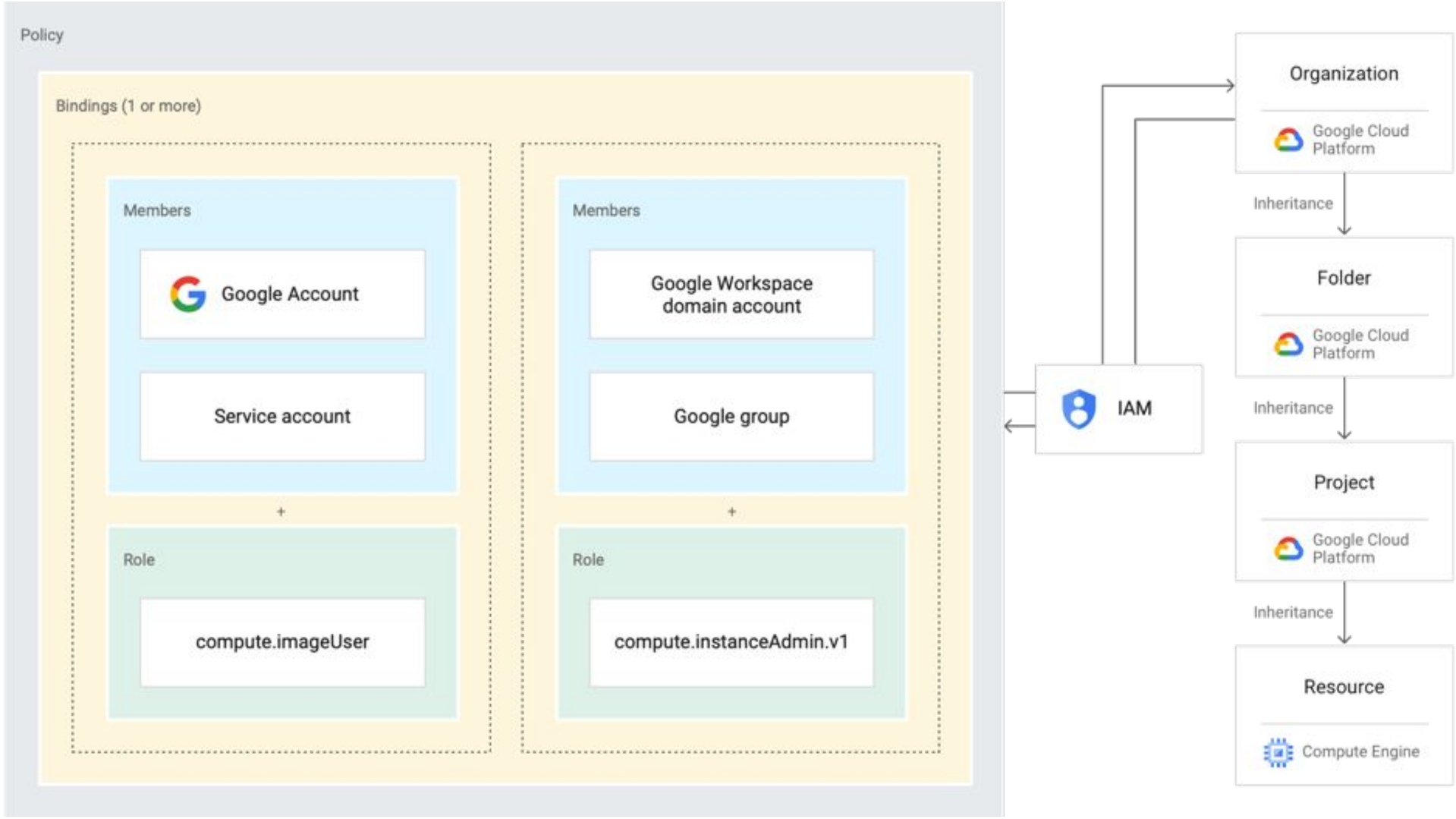
- **Policies**: A collection of bindings

The different types of Roles:

- Basic - not recommended
- Predefined
- Custom

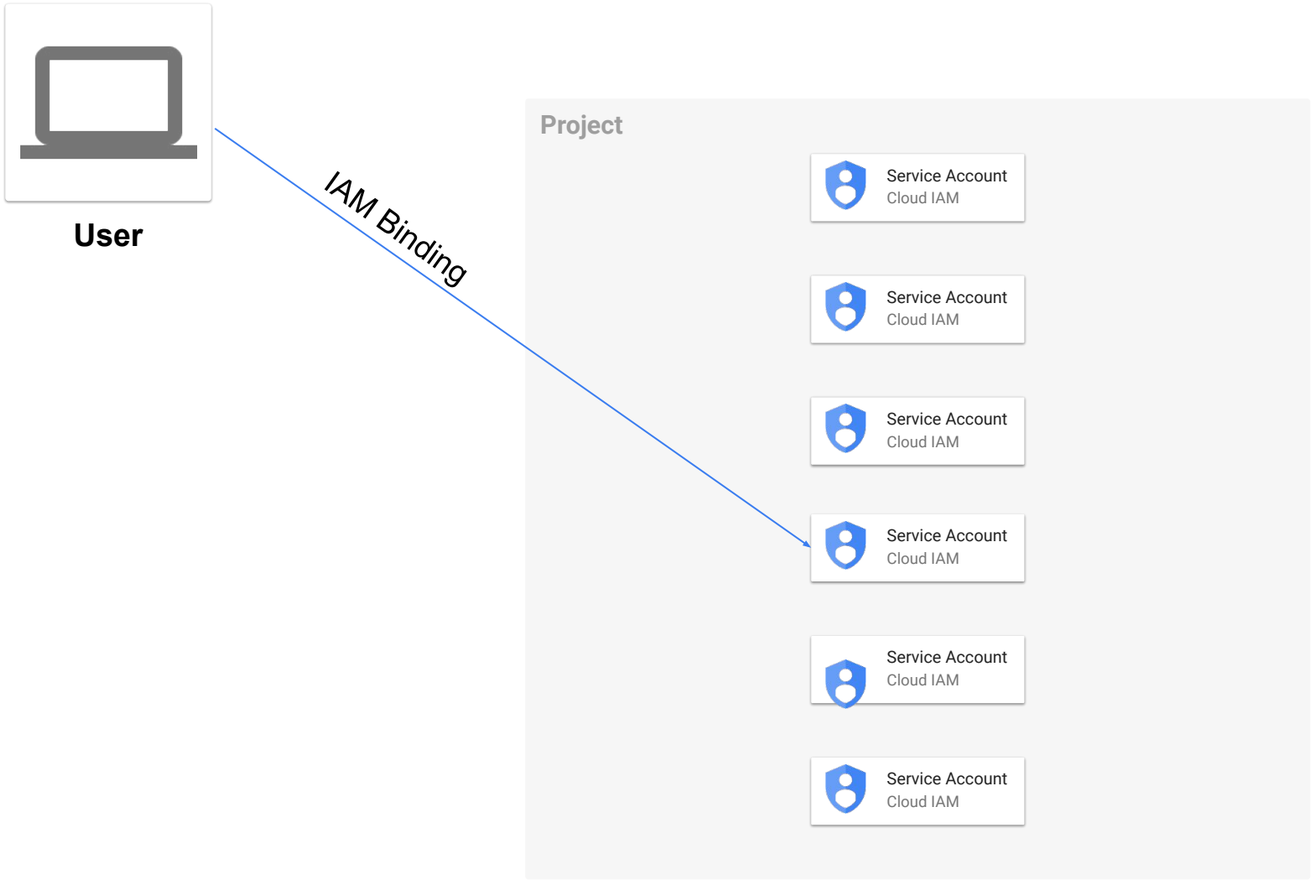
GCP Hierarchy



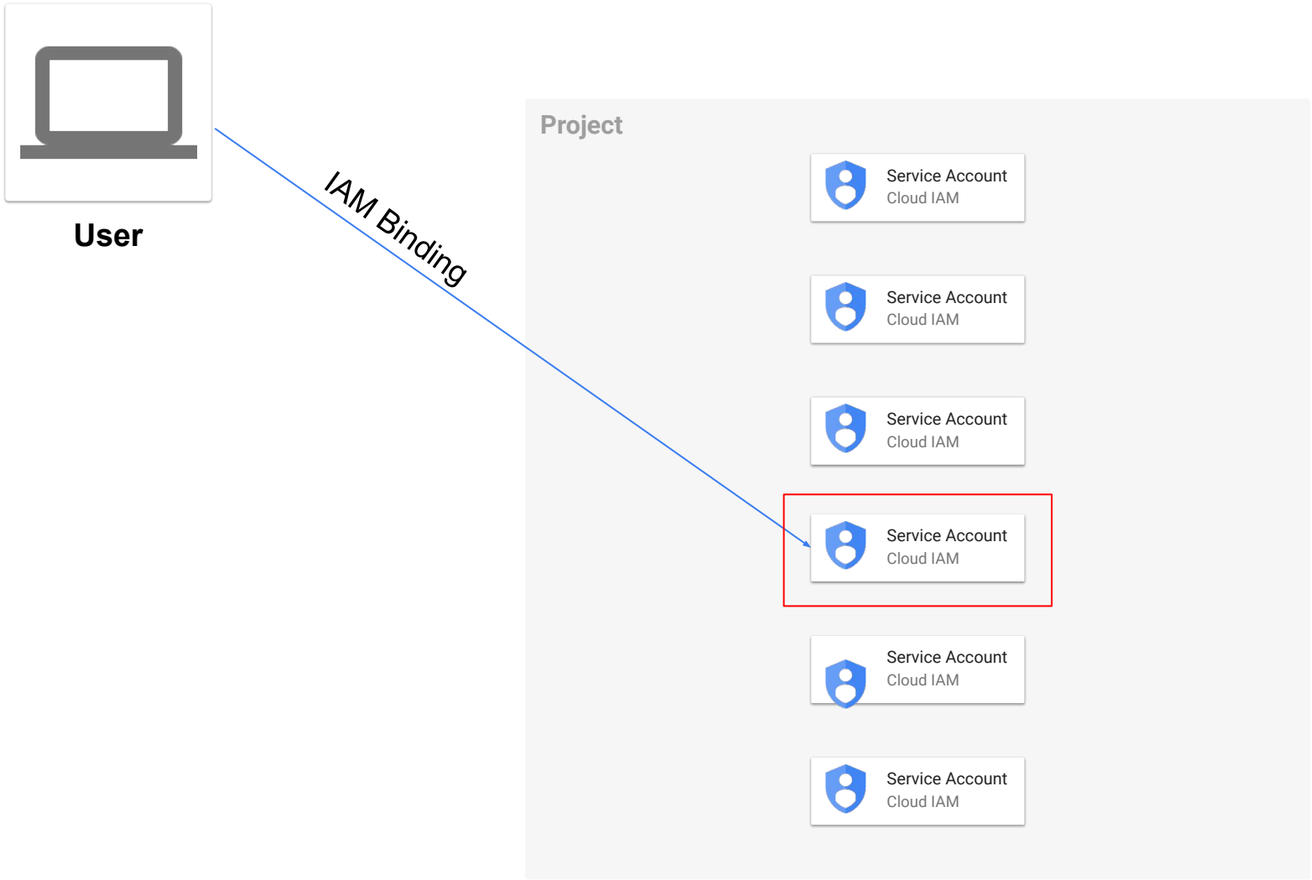

Policy
Bindings (1 or more)
Members
Google Account
Service account
+
Role
compute.imageUser
Members
Google Workspace domain account
Google group
+
Role
compute.instanceAdmin.v1
IAM
Organization
Google Cloud Platform
Inheritance
Folder
Google Cloud Platform
Inheritance
Project
Google Cloud Platform
Inheritance
Resource
Compute Engine

Service Accounts: Identities and Resources

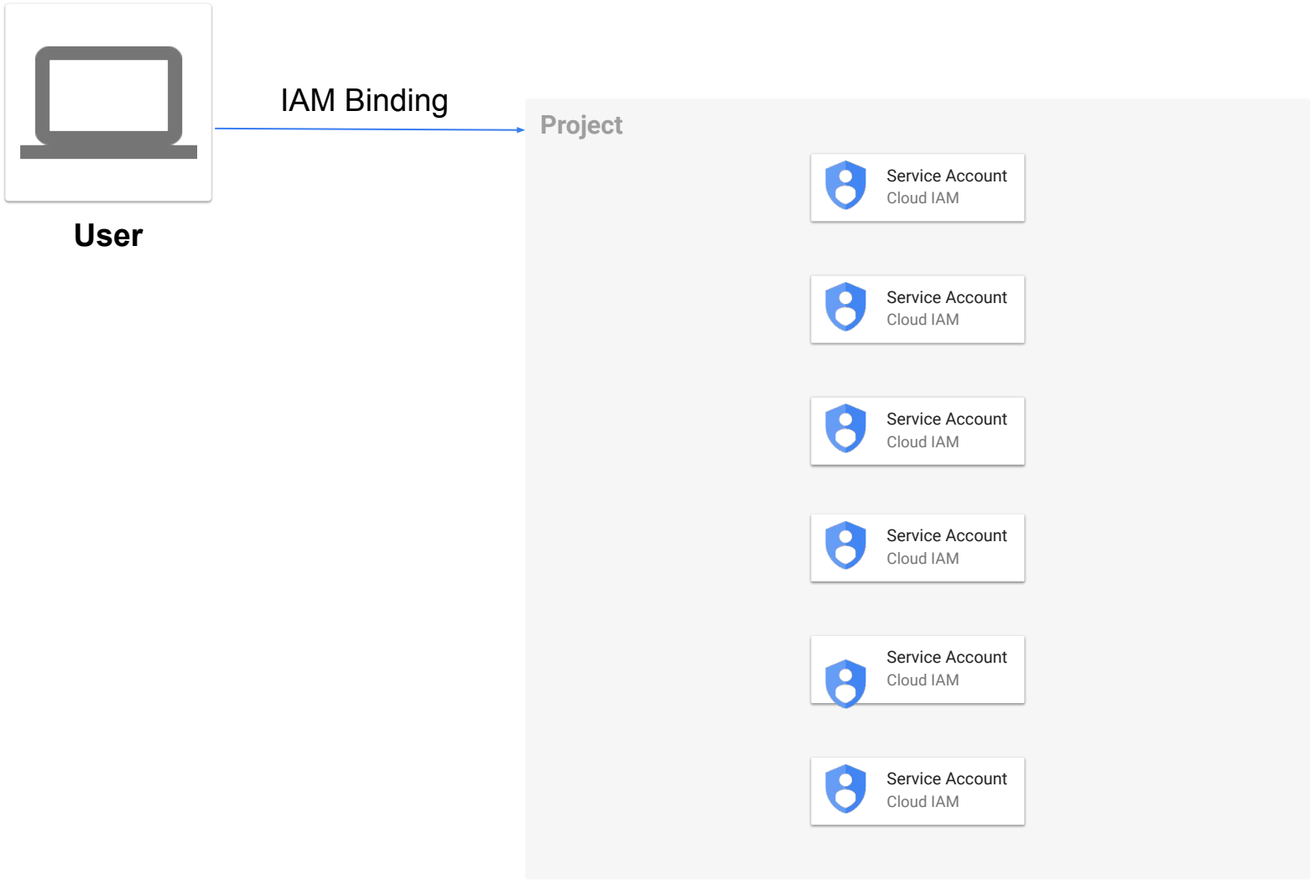
Binding at a Service Account



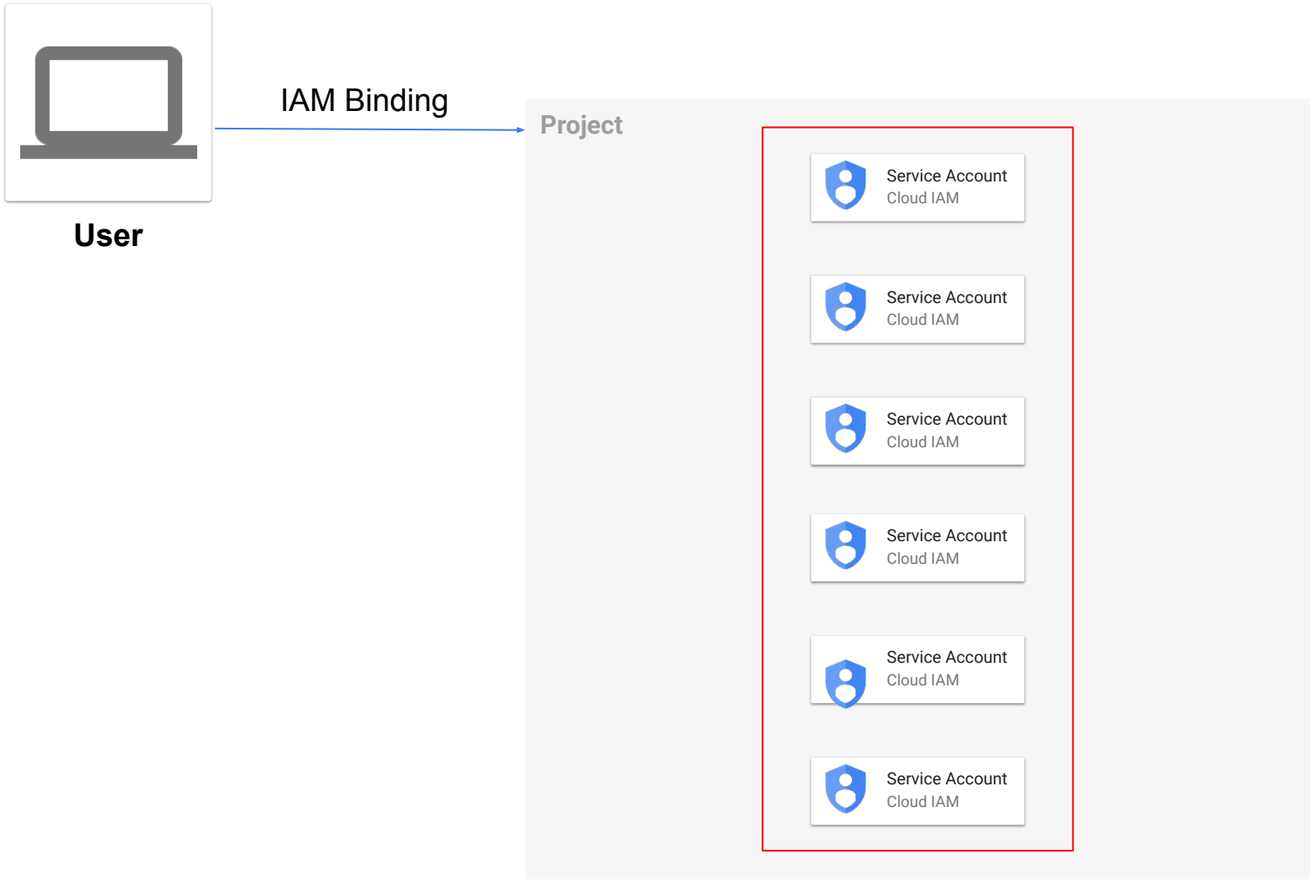
Binding at a Service Account



Binding at a Project



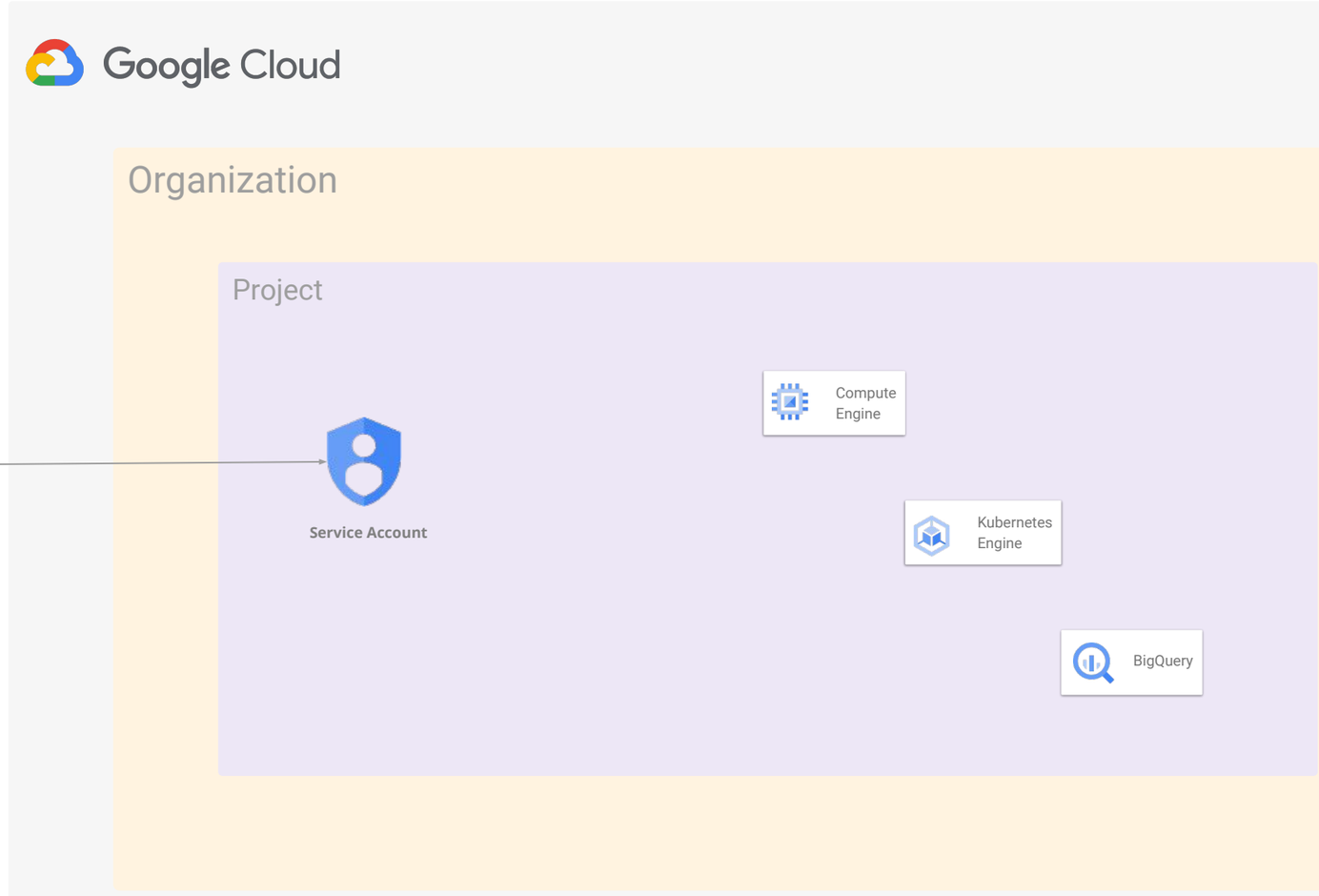
Binding at a Project



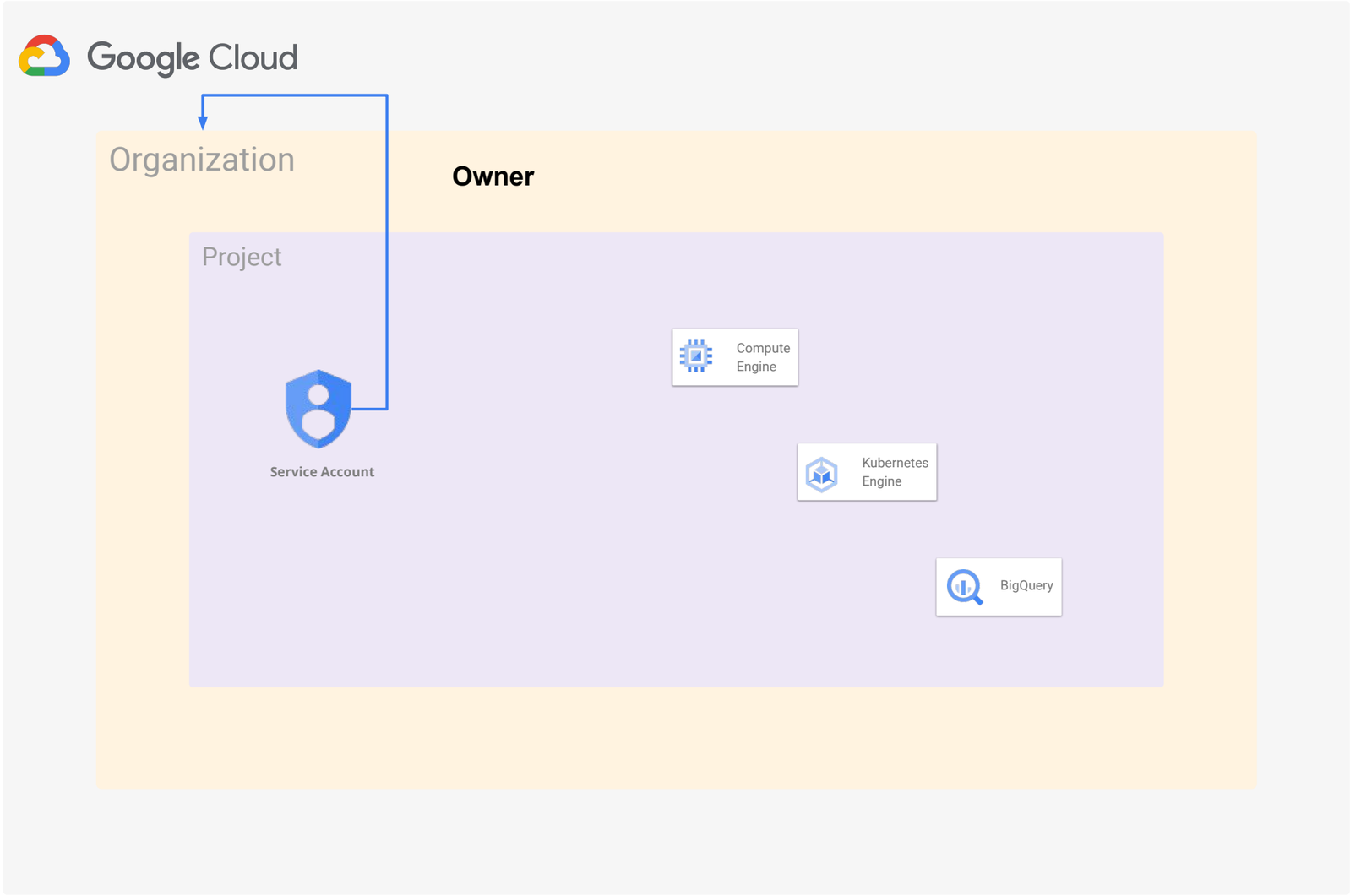
Real Example in GCP


Google Cloud
Organization
Project
Compute Engine
Kubernetes Engine
BigQuery

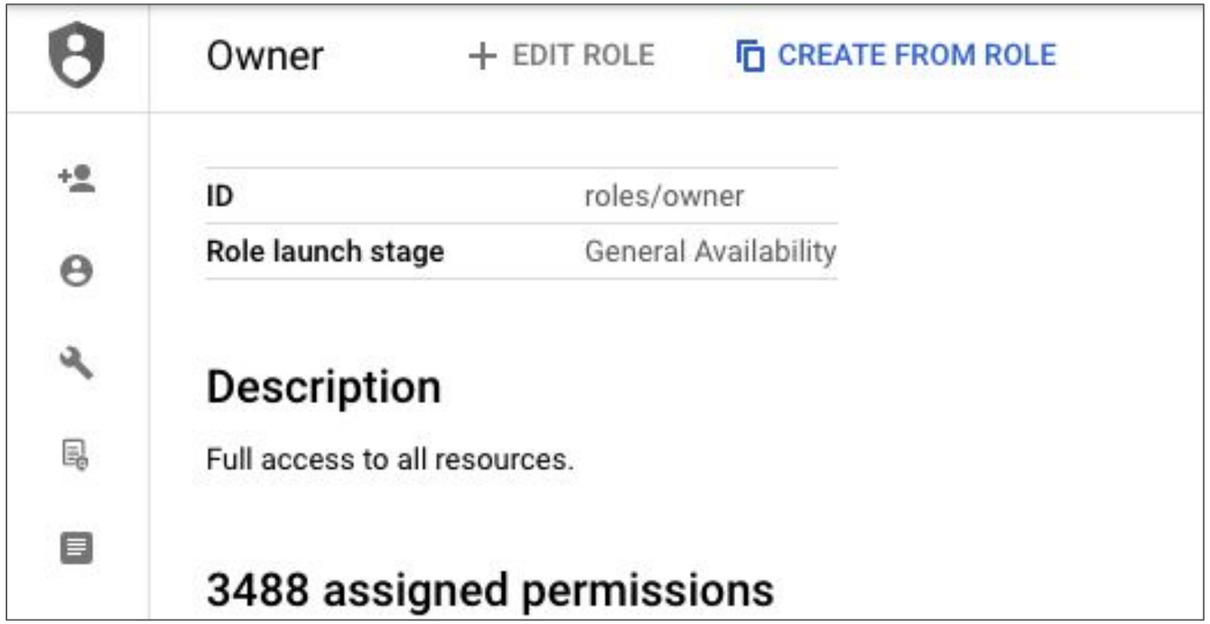
Service Account Created

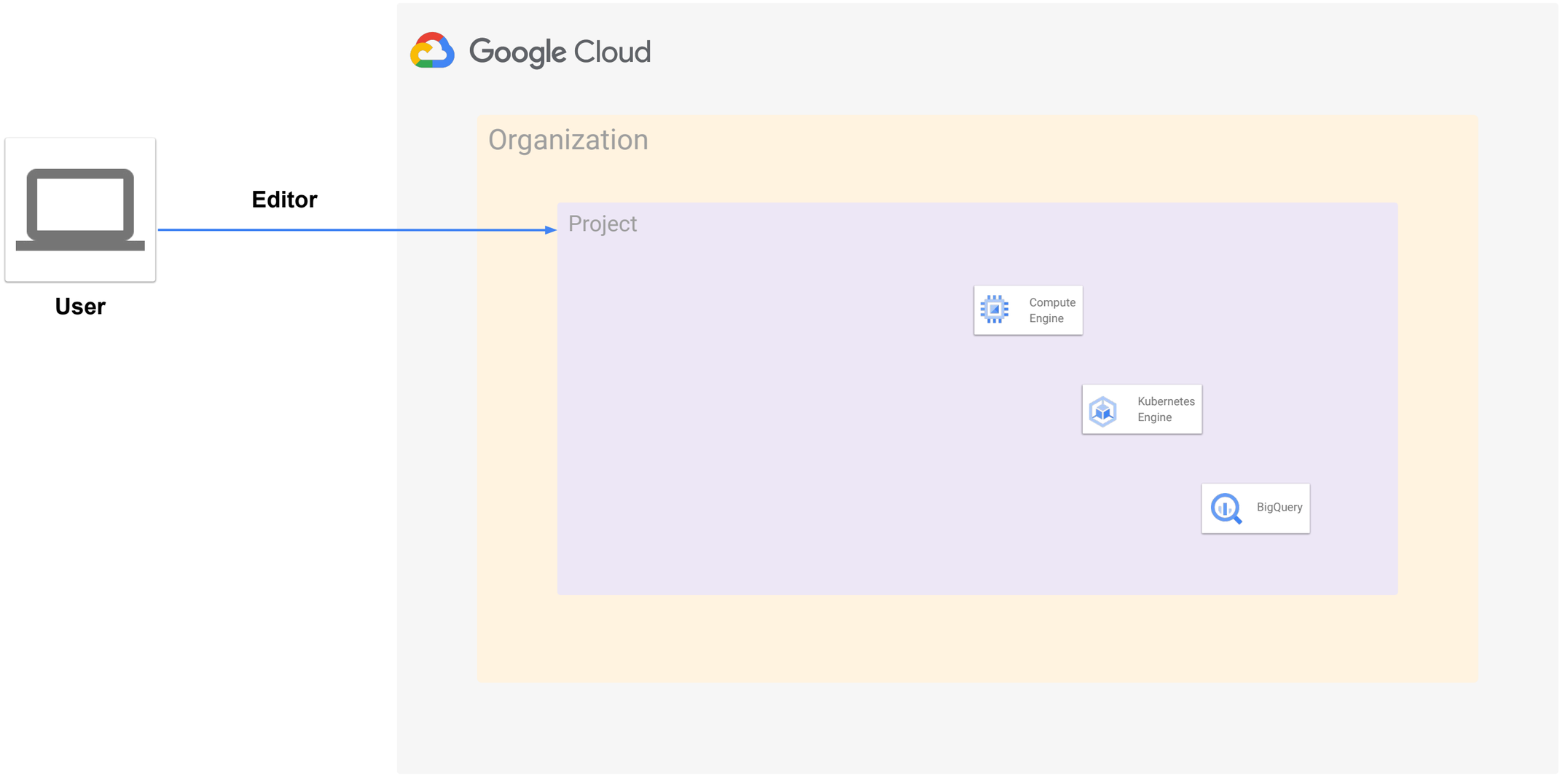


"Owner"
Permission Granted

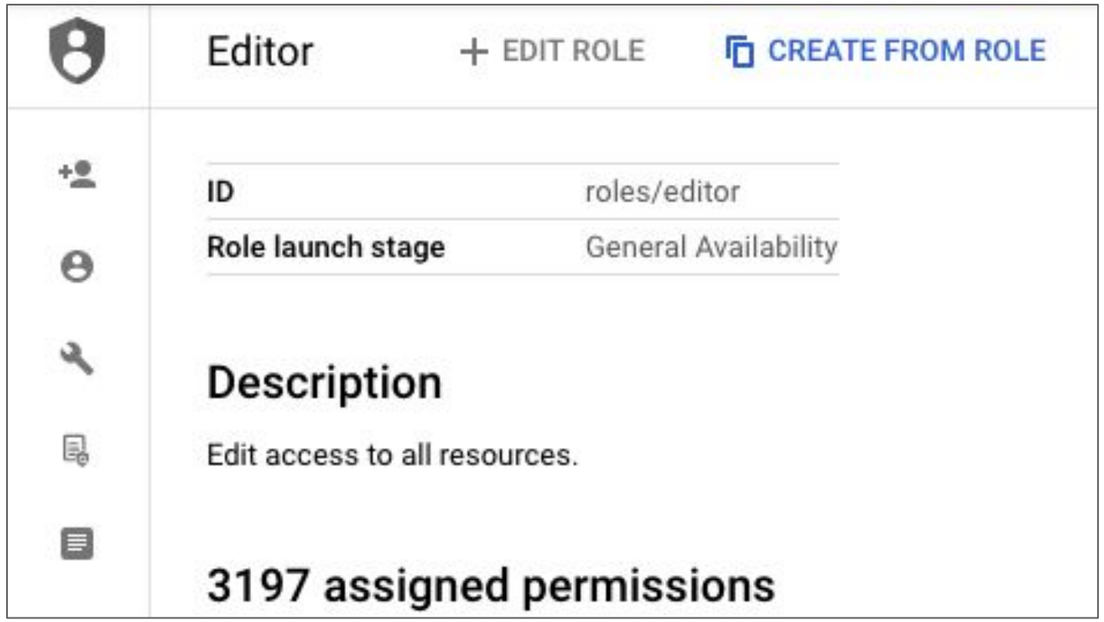


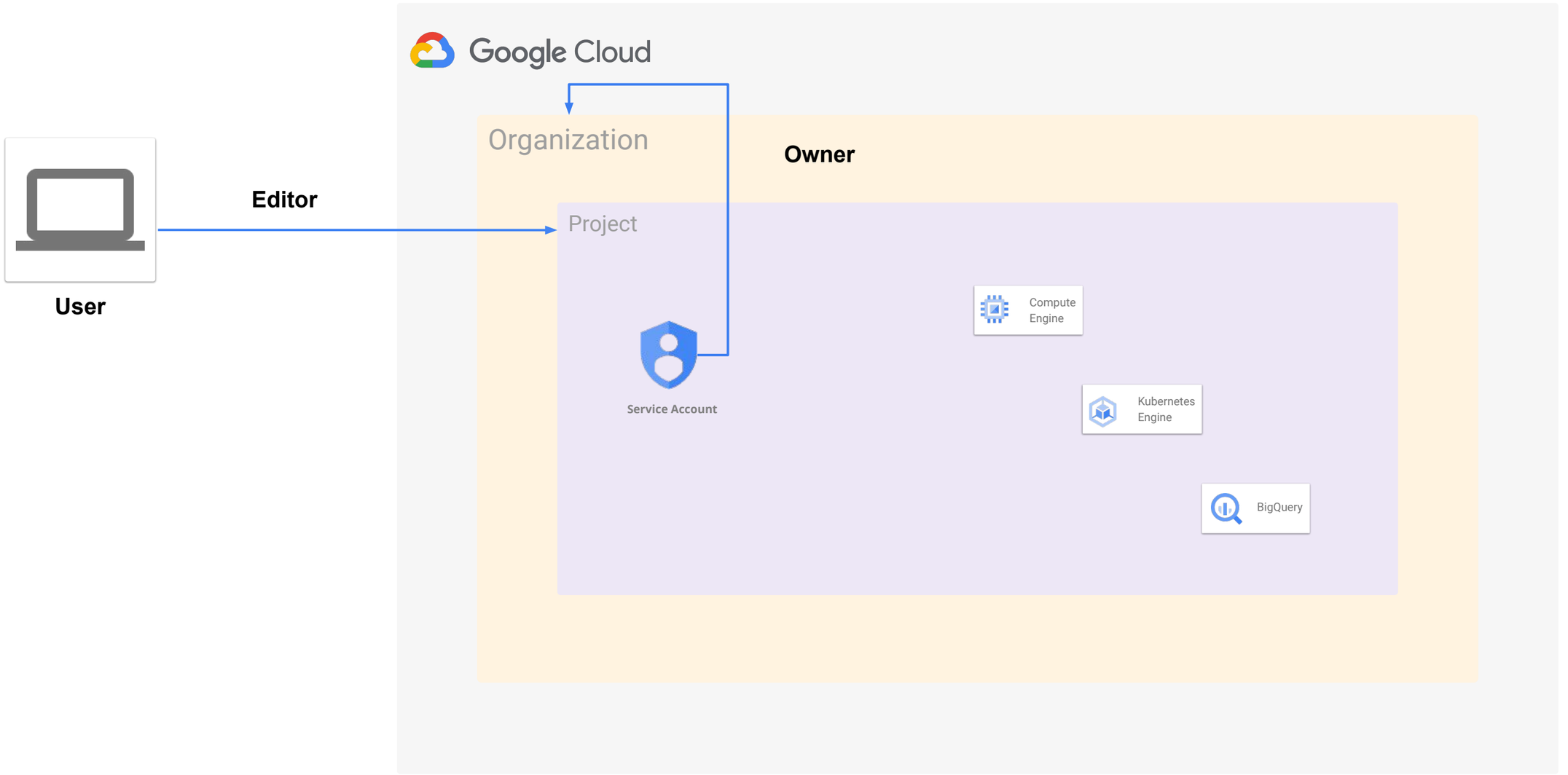
Owner

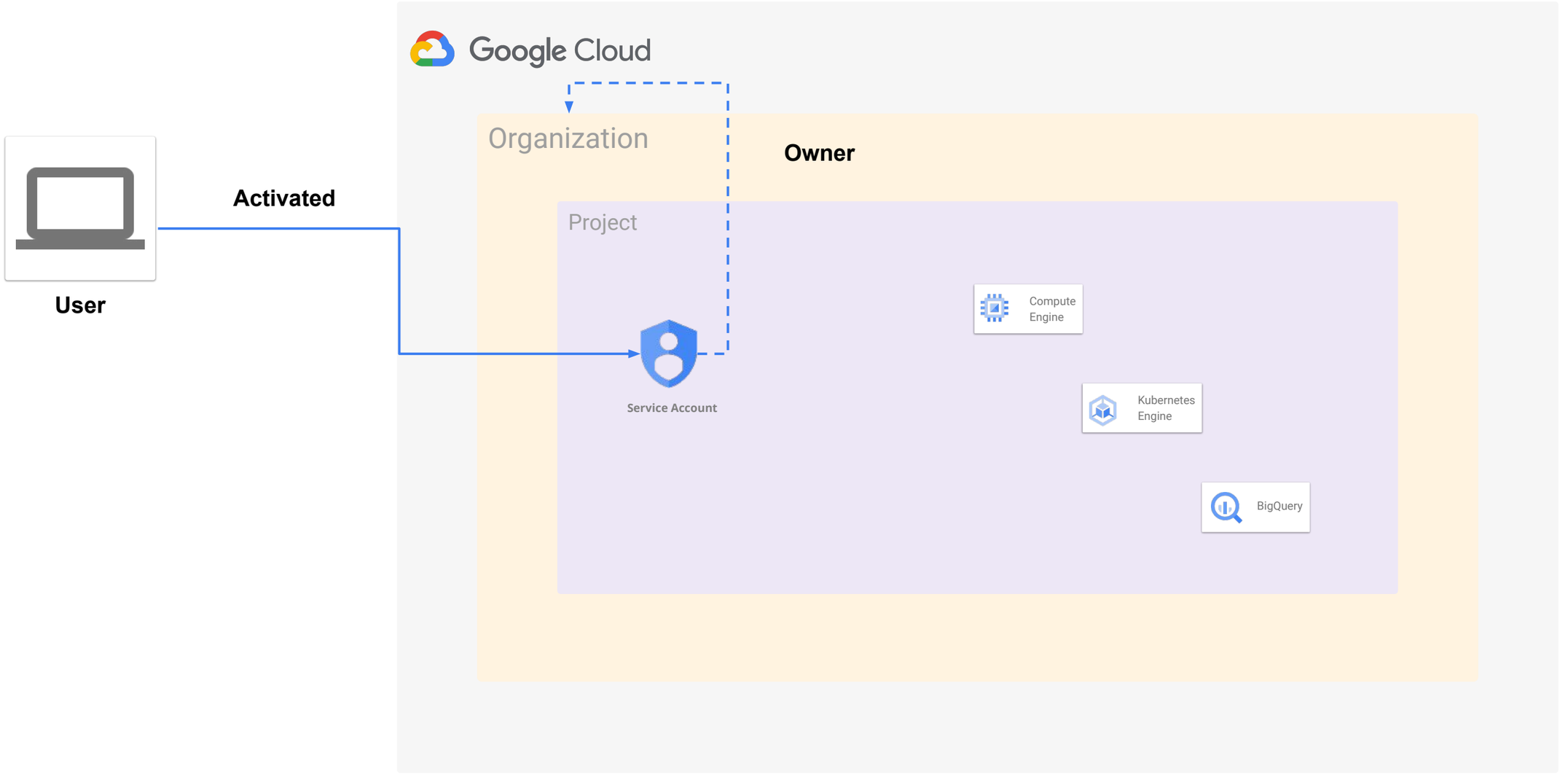

Owner
+ EDIT ROLE
CREATE FROM ROLE
ID
roles/owner
Role launch stage
General Availability
Description
Full access to all resources.
3488 assigned permissions


Google Cloud
Organization
Project
Editor
User
Compute Engine
Kubernetes Engine
BigQuery

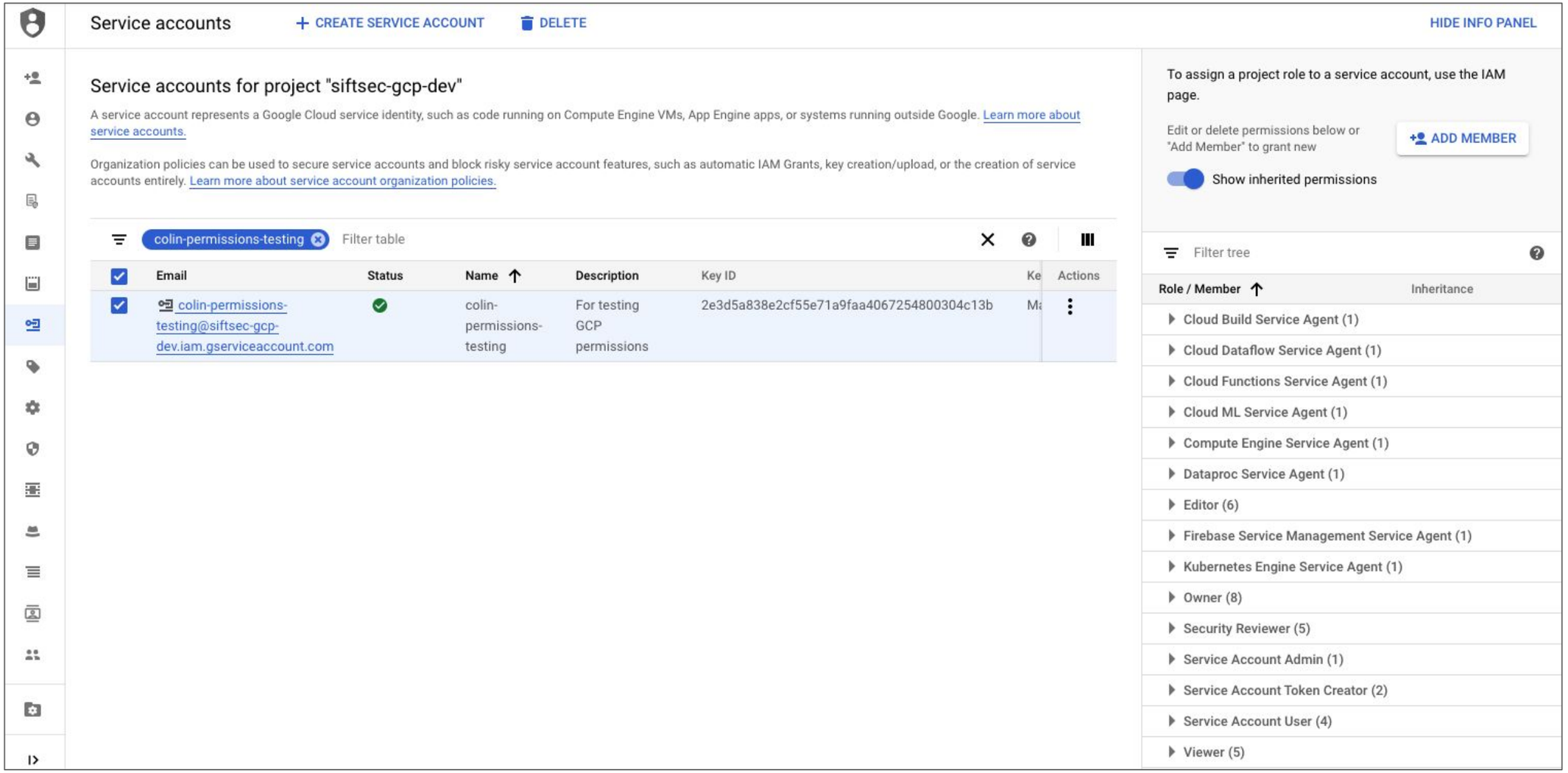
Editor


Editor
+ EDIT ROLE
CREATE FROM ROLE
ID
roles/editor
Role launch stage
General Availability
Description
Edit access to all resources.
3197 assigned permissions


Google Cloud
Organization
Owner
Editor
Project
User
Service Account
Compute Engine
Kubernetes Engine
BigQuery


Google Cloud
Organization
Owner
Project
Activated
User
Service Account
Compute Engine
Kubernetes Engine
BigQuery

Why is this a problem?

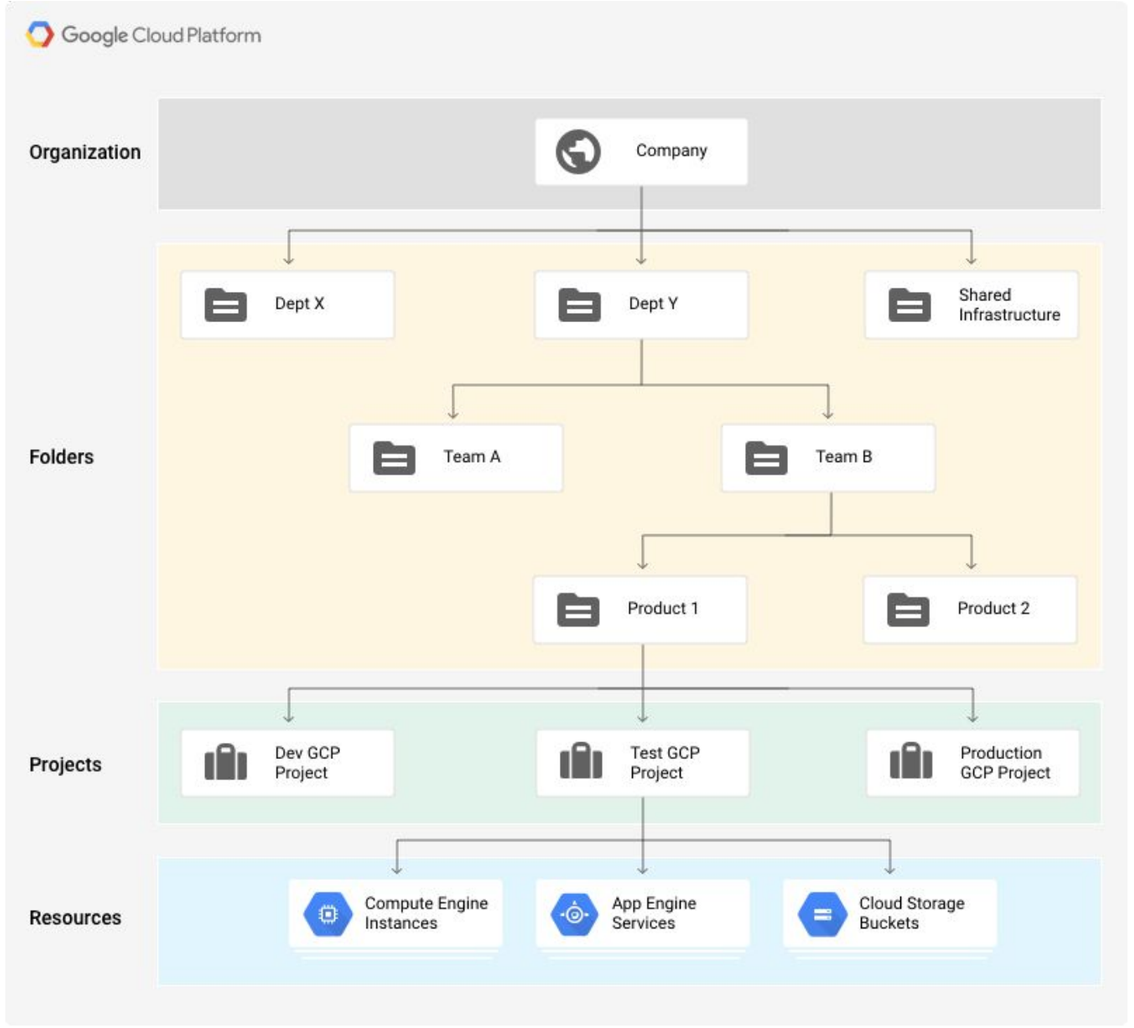

Service accounts
+ CREATE SERVICE ACCOUNT
DELETE
HIDE INFO PANEL
Service accounts for project "siftsec-gcp-dev"
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.
colin-permissions-testing
Filter table
Email
Status
Name
Description
Key ID
Actions
colin-permissions-testing@siftsec-gcp-dev.iam.gserviceaccount.com
colin-permissions-testing
For testing GCP permissions
2e3d5a838e2cf55e71a9faa4067254800304c13b
To assign a project role to a service account, use the IAM page.
Edit or delete permissions below or "Add Member" to grant new
ADD MEMBER
Show inherited permissions
Filter tree
Role / Member
Inheritance
Cloud Build Service Agent (1)
Cloud Dataflow Service Agent (1)
Cloud Functions Service Agent (1)
Cloud ML Service Agent (1)
Compute Engine Service Agent (1)
Dataproc Service Agent (1)
Editor (6)
Firebase Service Management Service Agent (1)
Kubernetes Engine Service Agent (1)
Owner (8)
Security Reviewer (5)
Service Account Admin (1)
Service Account Token Creator (2)
Service Account User (4)
Viewer (5)

Permission Mining Solution

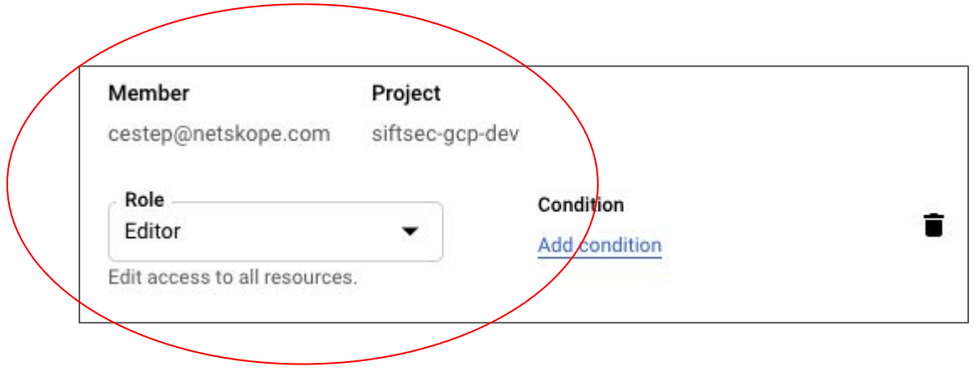
What does it do?

- Can continually monitor the environment
- Uses a graph to find privilege escalation potential
- Provides a report containing direct and indirect permissions
- Users can monitor and mitigate risk

Hierarchy Inventory

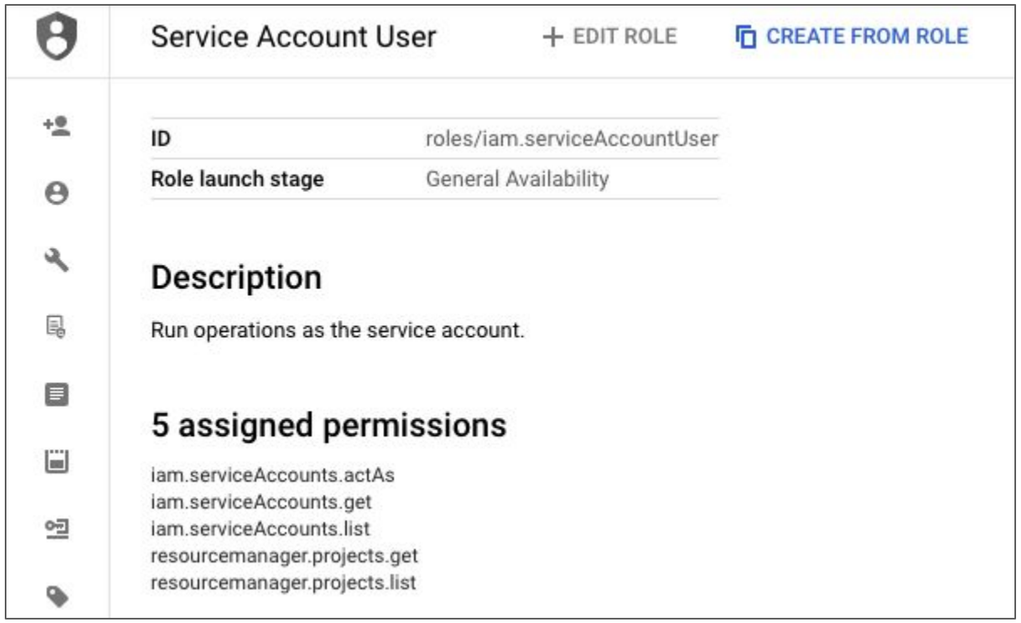


Compile Direct Bindings

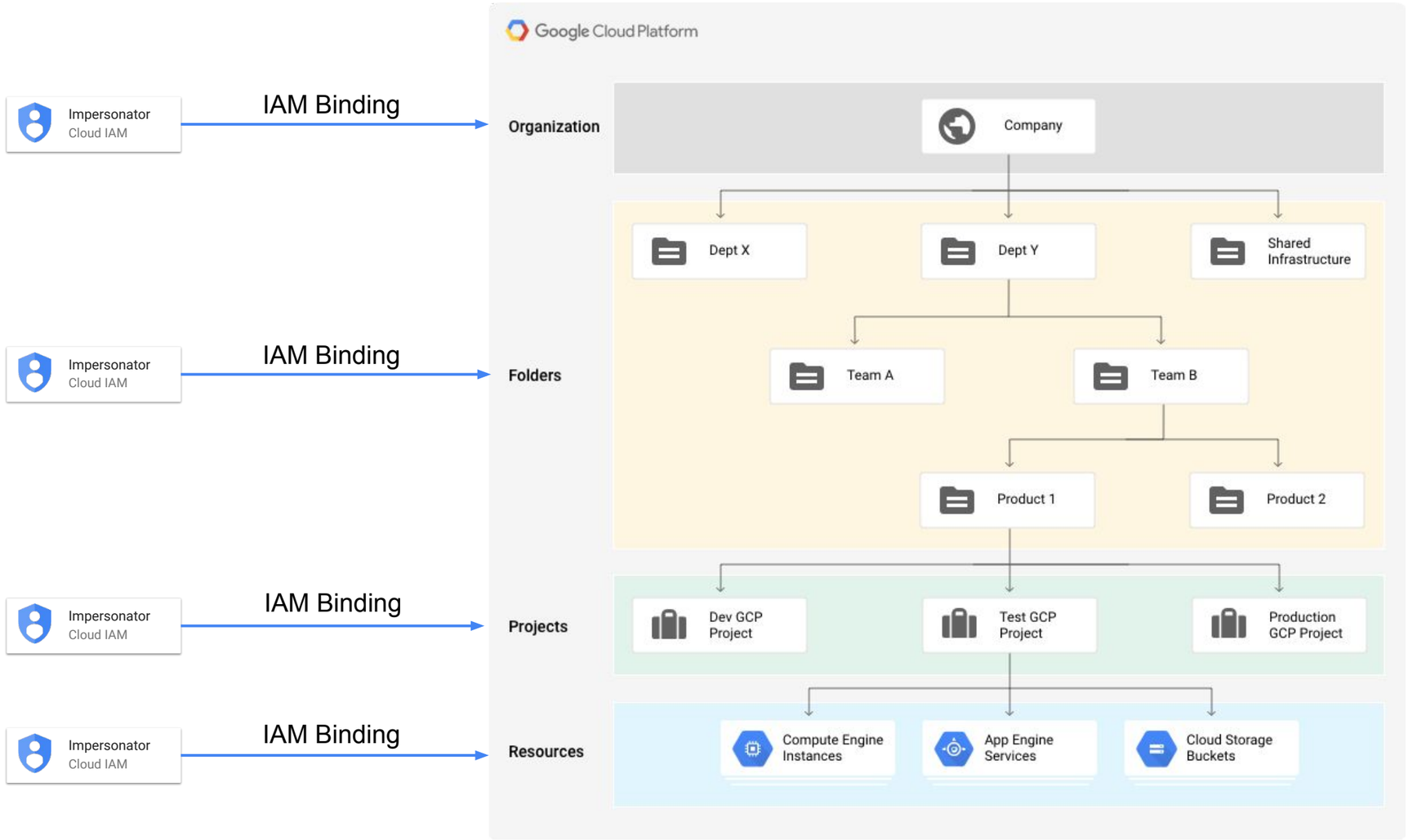


Find Impersonators

- Owner
- Editor
- Service Account Token Creator
- Service Account Key Admin
- Service Account User



Graph Construction



Find Potential Privilege Escalation

- Traverse the graph for each member
- Find the Service Accounts in scope
- Compile all of the permissions assigned to Service Accounts
- Apply the extended bindings to the member

Our Results

Member Report

Report for cestep

Direct Bindings

Project bindings

'siftsec-gcp-dev': ['roles/editor']

Extended Bindings

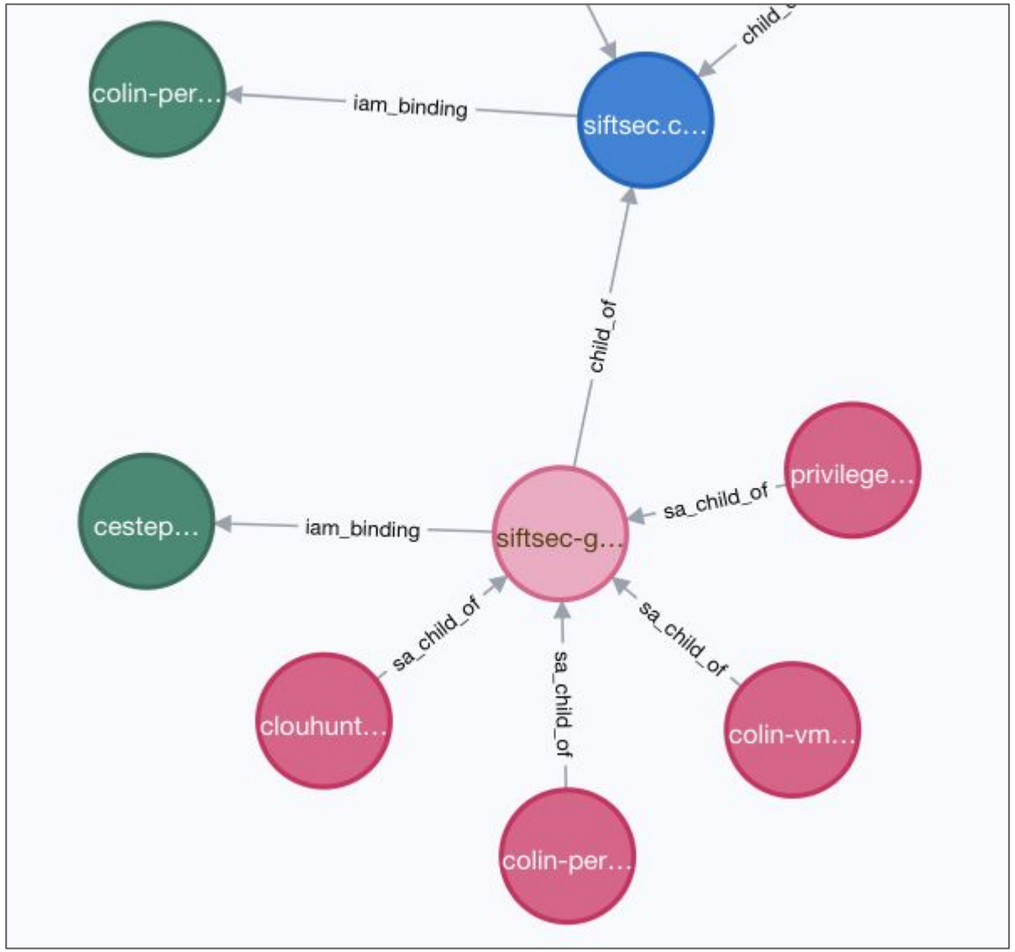
Organization bindings

'siftsec.com': ['roles/iam.securityReviewer', 'roles/owner', 'roles/pubsub.editor', 'roles/browser']

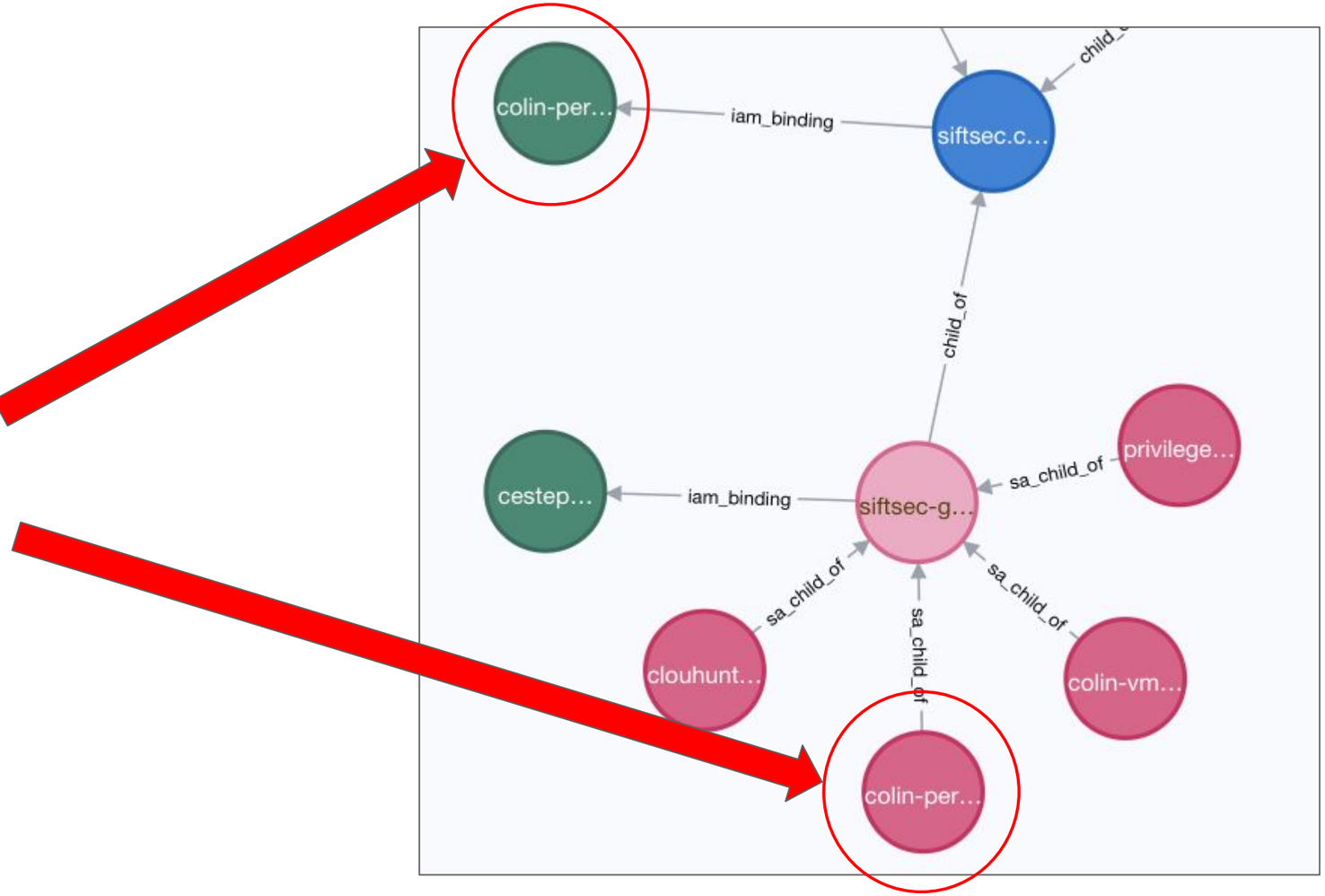
Graph Layout

Legend:

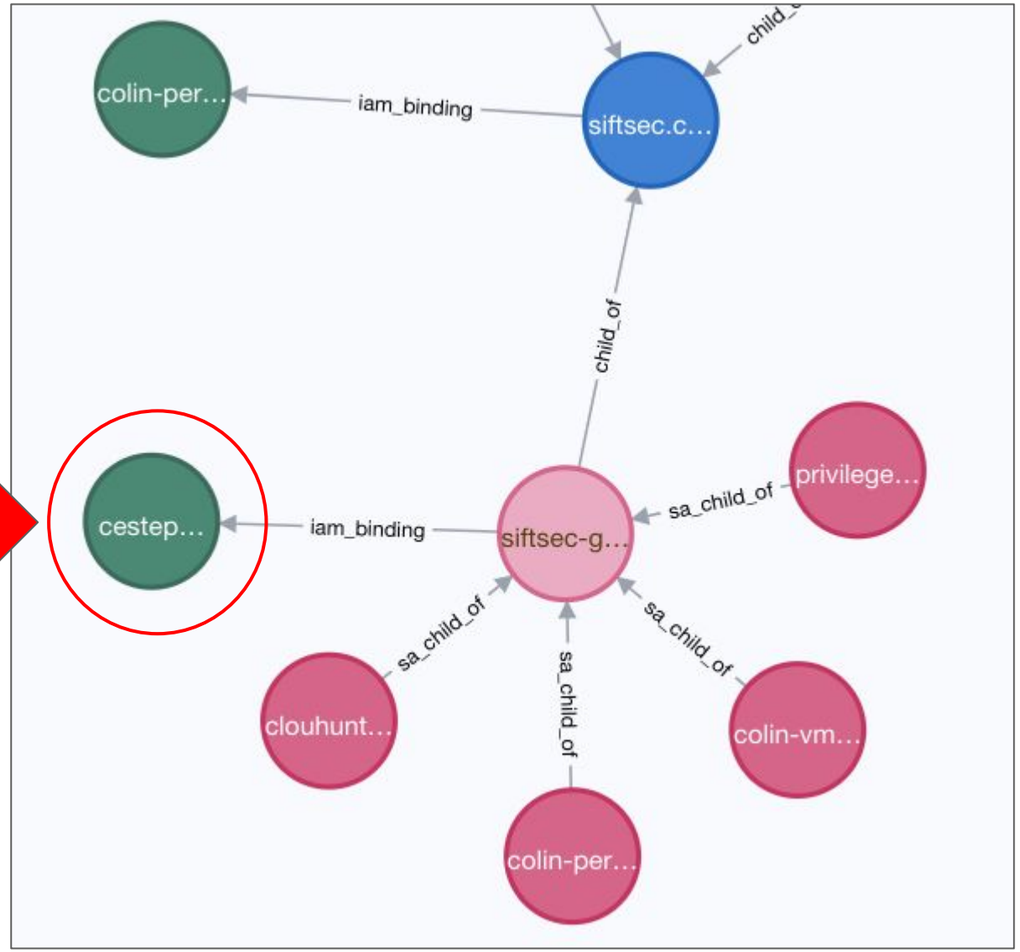
- Blue => Organization
- Green => Member
- Light Pink => Project
- Dark Pink => Service Account

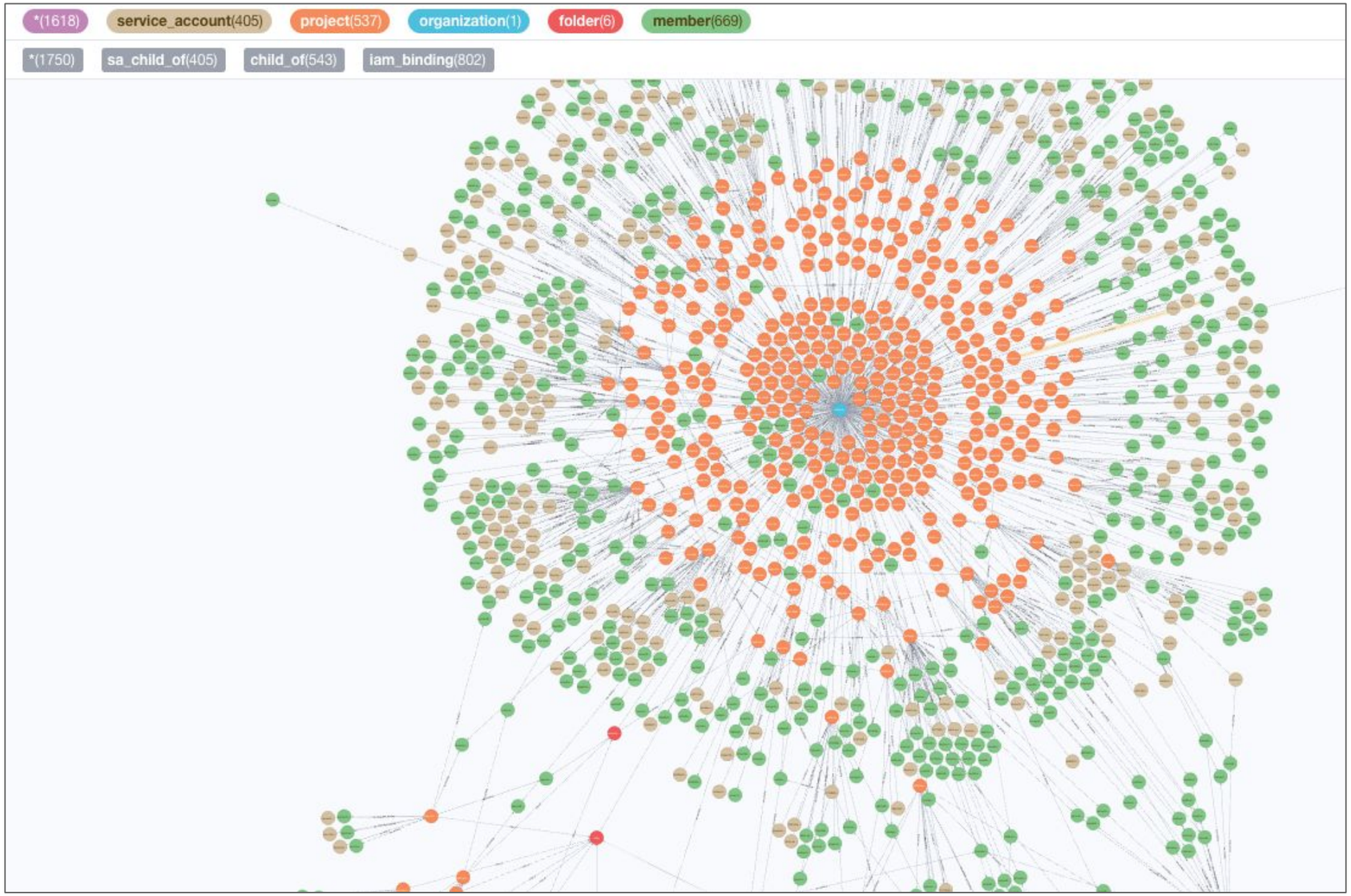


Service Account



Impersonator




*(1618)
service_account(405)
project(537)
organization(1)
folder(6)
member(669)
*(1750)
sa_child_of(405)
child_of(543)
iam_binding(802)

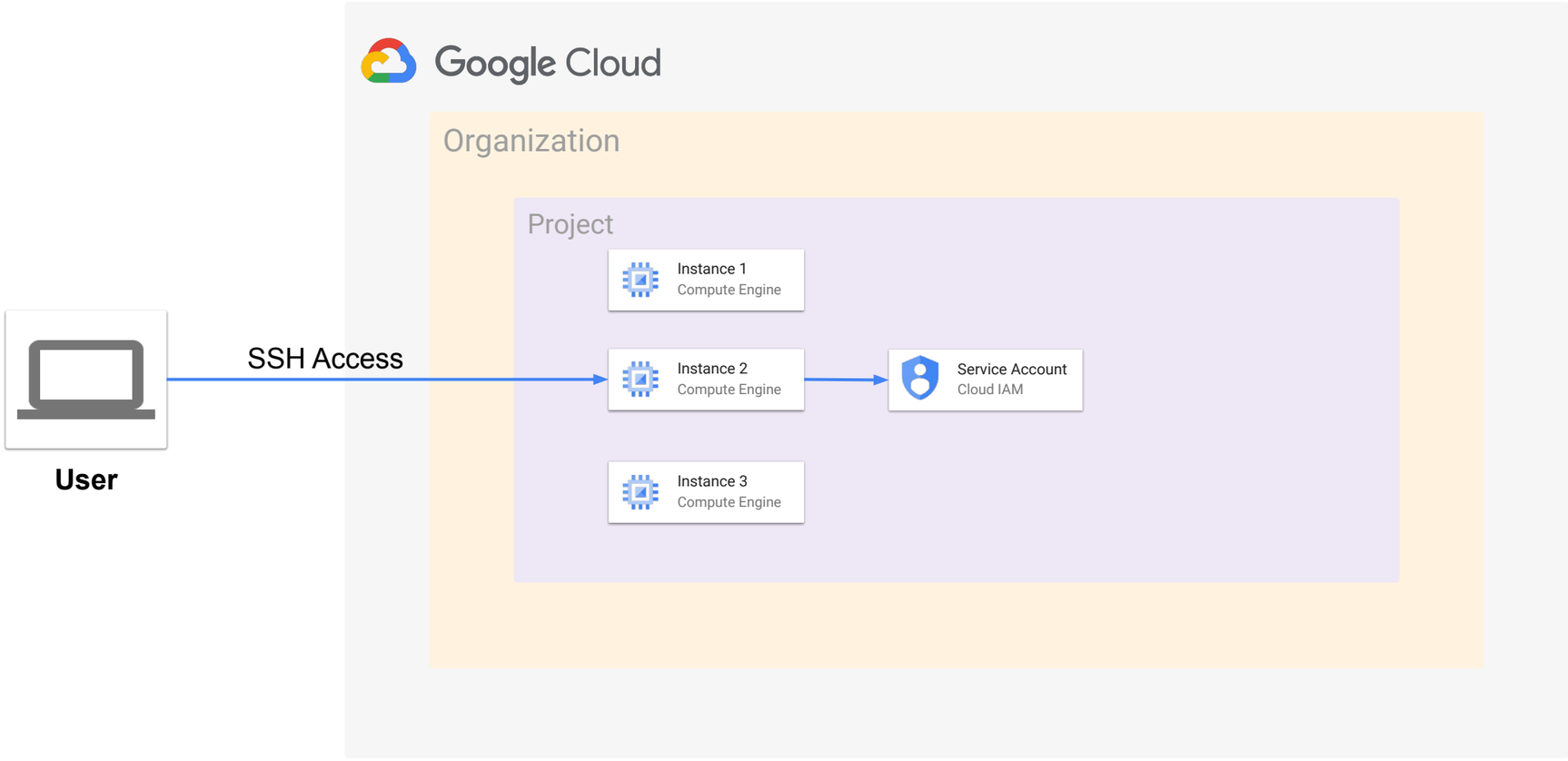
Remediation

- Bringing service account bindings down the hierarchy
- Changing out basic roles for more granular roles
- Removing bindings that are not needed

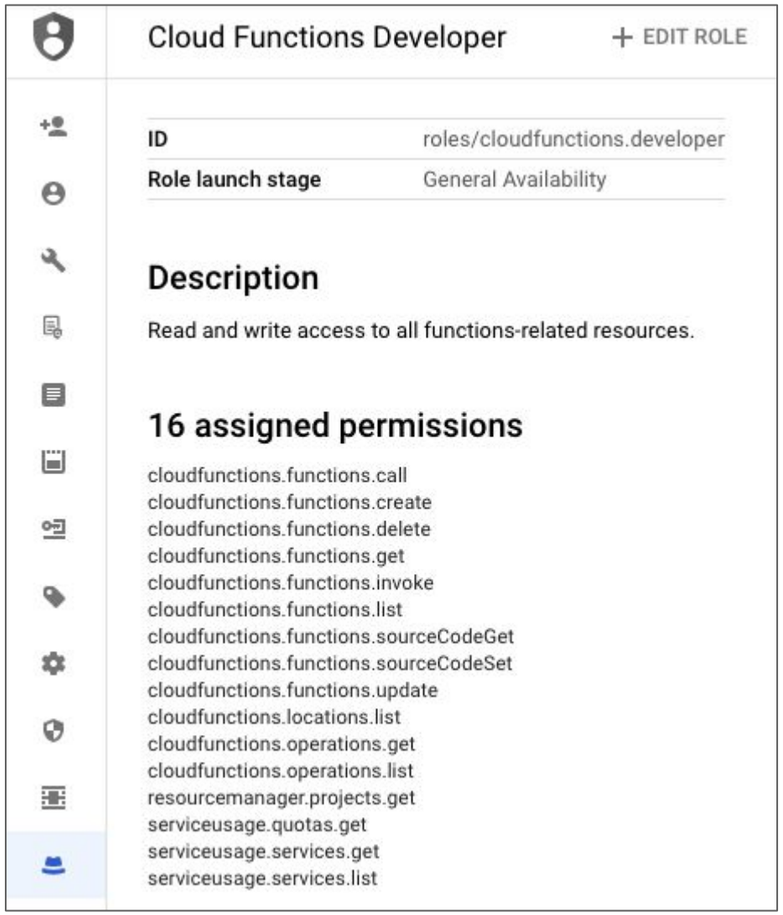
We want to proactively reduce risk in the environment without waiting for a compromise.

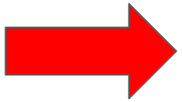
Future Enhancements

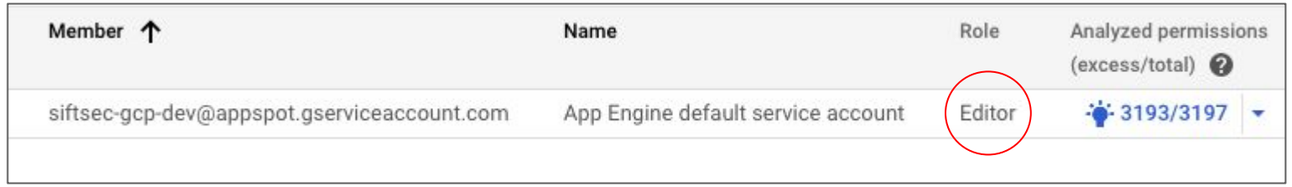
Compute Engine



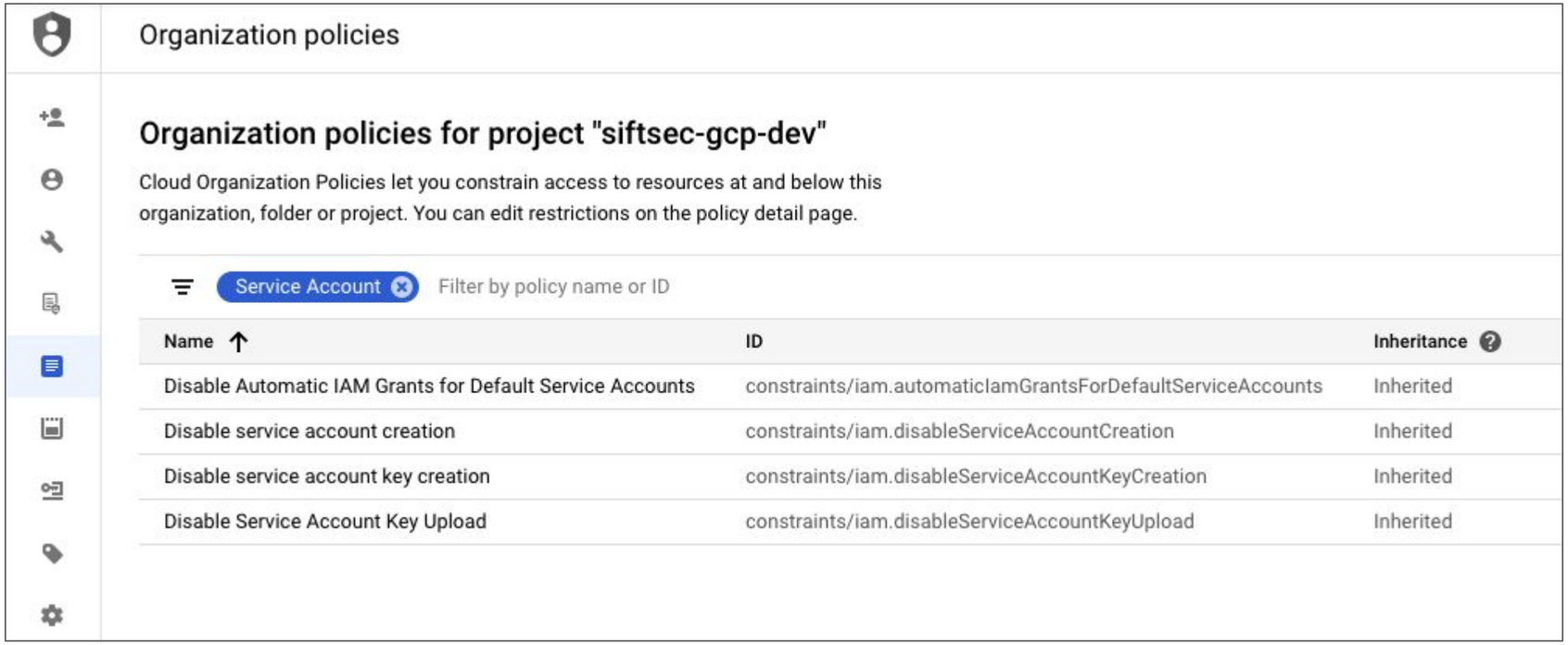
Cloud Functions







Organization Policies



Thank you!

Colin Estep

@colinestep

https://www.linkedin.com/in/colinestep/

Project URL:

github.com/netskopeoss/iaas_permission_mining