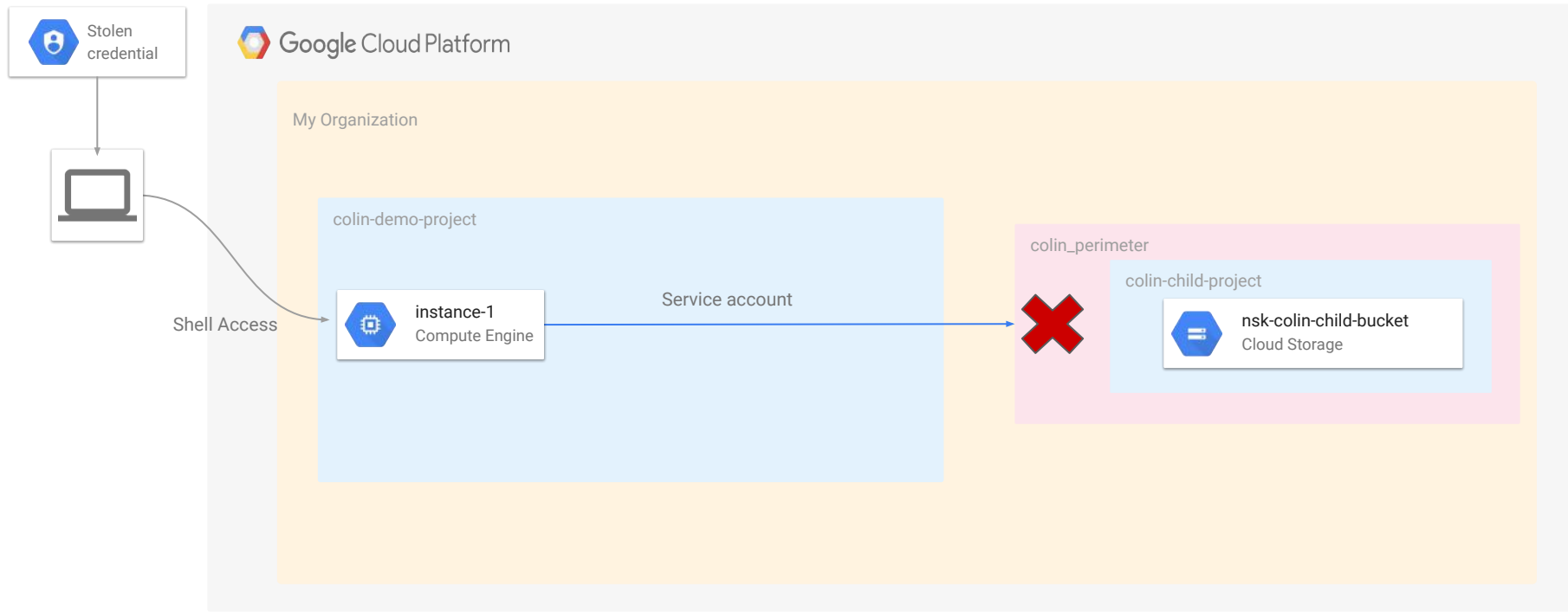


Exploiting IAM in GCP

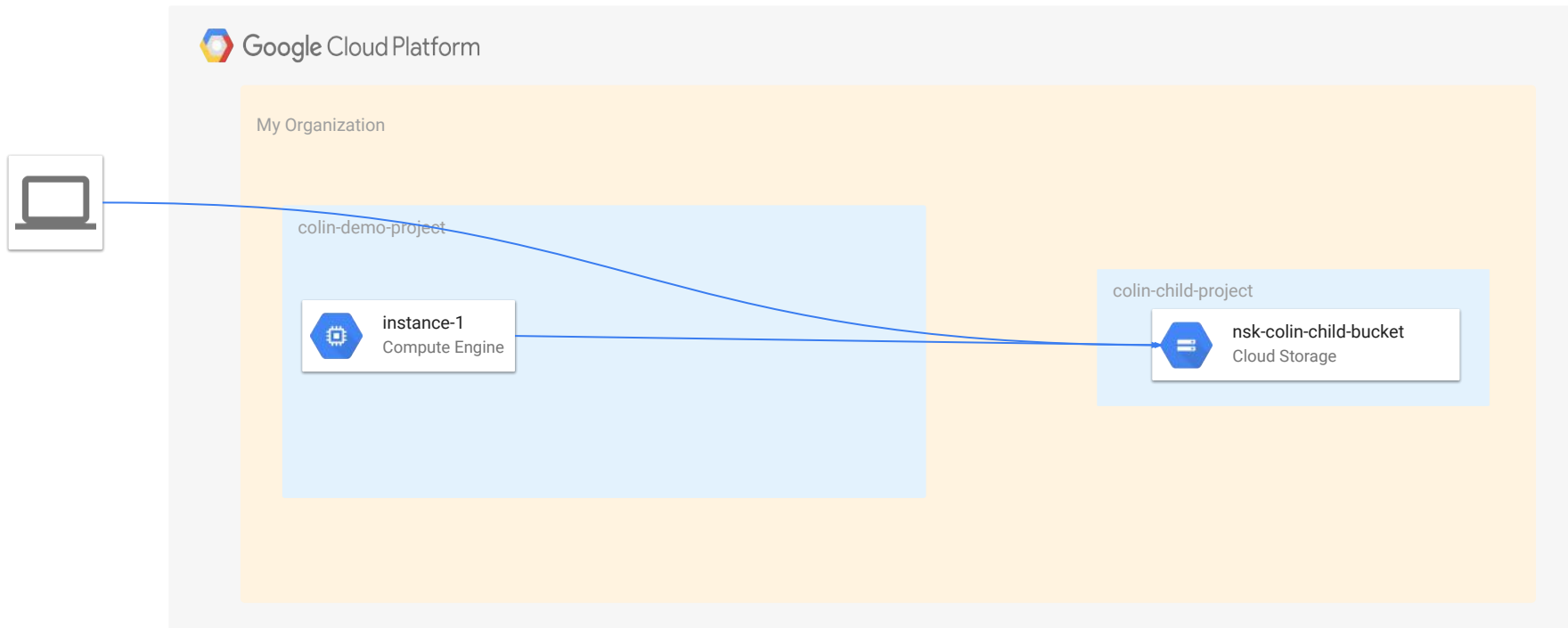
Who am I?

- Formerly Security @ Apple, Netflix
- Startup experience: built cloud security software
- Currently Research @ Netskope
- Focused on AWS, GCP

What's the Story...



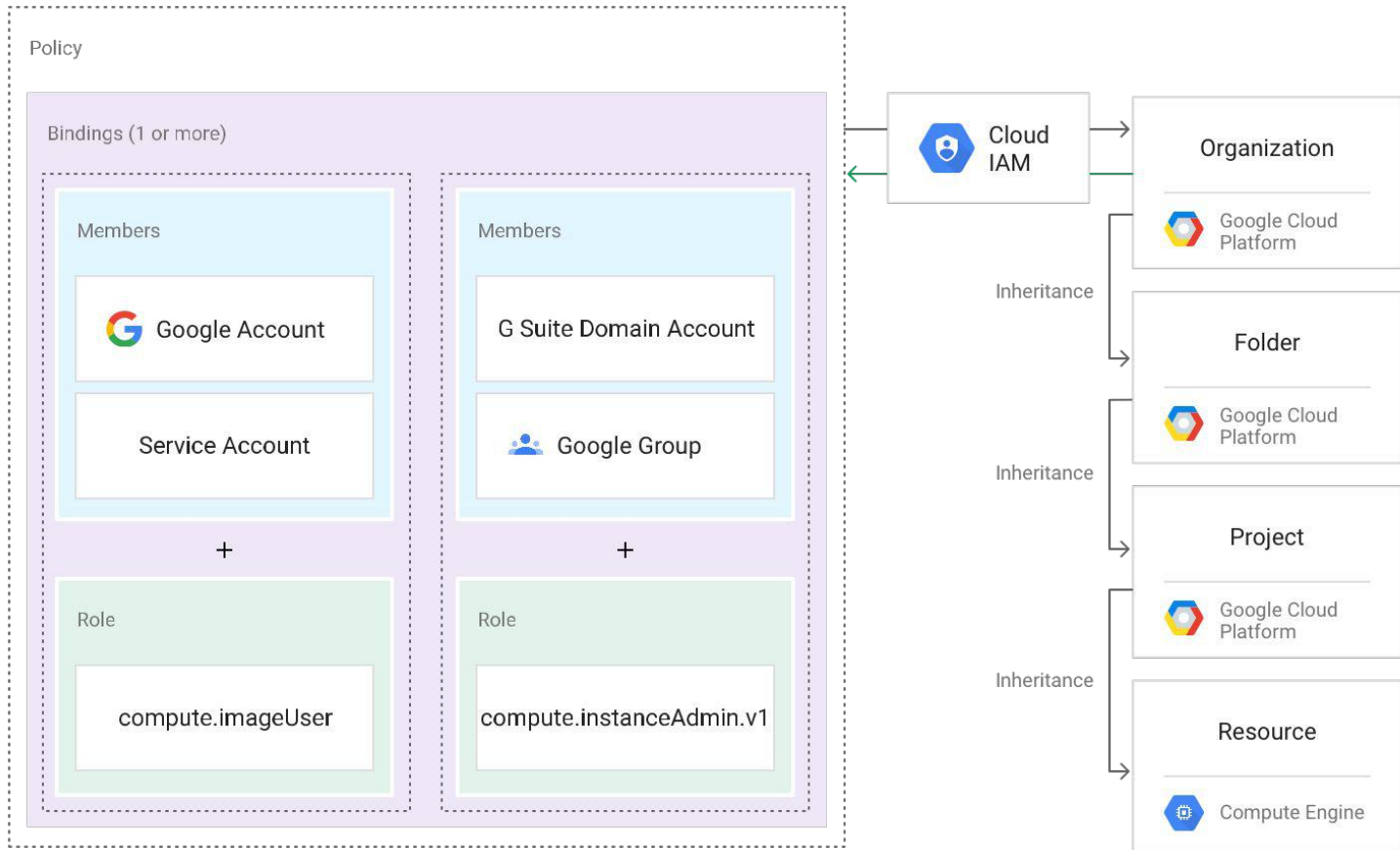
End Condition



Agenda

- IAM in GCP
- VPC Service Controls
- Service Account Deep Dive
- GCP Demo
- Q&A

IAM in GCP



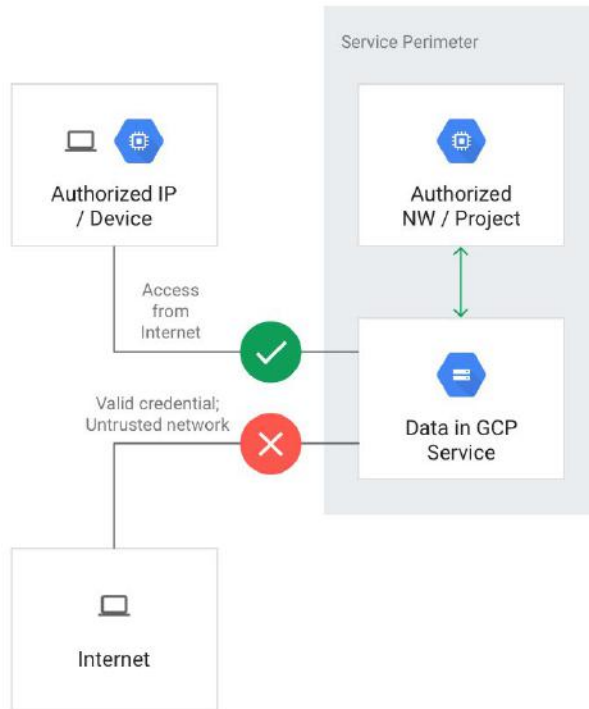
Types of Roles

- **Primitive Roles** - created by Google (not recommended)
 - Owner
 - Editor
 - Viewer
- **Predefined Roles** - created by Google
 - Compute Instance Admin
 - Storage Object Viewer
 - etc.
- **Custom Roles** - defined by users

VPC Service Controls

What are VPC Service Controls?

- Designed to mitigate Data Exfiltration risks
 - Create perimeters around your resources, such as Storage buckets
 - Control the movement of data past the boundaries of your perimeter
 - Set conditions to allow data flow outside of the perimeter
- Independent of IAM policies
 - IAM allow access would still be blocked based on the service control perimeter













Access Context Manager

- Another service that works in tandem with VPC service controls
- Allows admins to define the rules for access using certain criteria
 - Device type and operating system
 - IP address
 - User identity

An Example

Protecting: nsk-colin-child-bucket



← Edit VPC Service Perimeter





colin_perimeter

Must begin with a letter. Use only alphanumerics and underscores.

Perimeter Type

- ☒ Regular perimeter (default)
Regular service perimeters protect services on the projects it contains.
- ☐ Perimeter bridge
Perimeter bridges allow access between other regular service perimeters.

Projects to protect ?


Project Name ↑	Id	
 colin-child-project	colin-child-project	
 colin-folder-project	colin-folder-project	

ADD PROJECTS

Services to protect ?

Specify which services are protected by the perimeter. Only GCP Services that support perimeter controls can be added. To reduce the risk of your data being exfiltrated, we recommend that you restrict all storage services in the services list.

Service Name ↑


Google Cloud Storage API

ADD SERVICES

Ingress Policy: Access Levels (optional) ?

Access levels apply only to requests for protected resources coming from outside the service perimeter. Access levels cannot be used to permit protected resources or VMs to access data and services outside the perimeter.

Choose Access Level

NetskopeVPN

I>

Combining the Controls

- Google says: IAM + VPC Service Controls = Defense in Depth
- IAM can be misconfigured, but the Service Controls protect you
- Everyone should be monitoring changes to these controls
 - What if someone changes the access level rule to allow all traffic from multiple countries?
 - What if somebody removes a service control perimeter?

Service Account Deep Dive

What is a Service Account?

- Identity for applications to authenticate
- Designed for non-human use
- Uses RSA keys instead of passwords
- Can't access the web console
- Also considered resources – can apply bindings to them

More about Service Accounts

- A service account must be created in a Project
- IAM bindings can be granted at any level
 - Elevated Bindings = bindings at the Folder, Organization
- Google creates some service accounts automatically
 - Default account for Compute Engine, App Engine, etc.
 - Accounts they will use for internal processing

Default Service Account - Compute Engine

Google advises against it:

1. Create a new service account rather than using the Compute Engine default service account.
2. Grant IAM roles to that service account for only the resources that it needs.
3. Configure the instance to run as that service account.
4. Grant the instance the `https://www.googleapis.com/auth/cloud-platform` scope to allow full access to all Google Cloud APIs, so that the IAM permissions of the instance are completely determined by the IAM roles of the service account.

Compute Engine Service Account Role

Contains a primitive role:

- Project Editor

Project Editor Permissions (1894 in total)

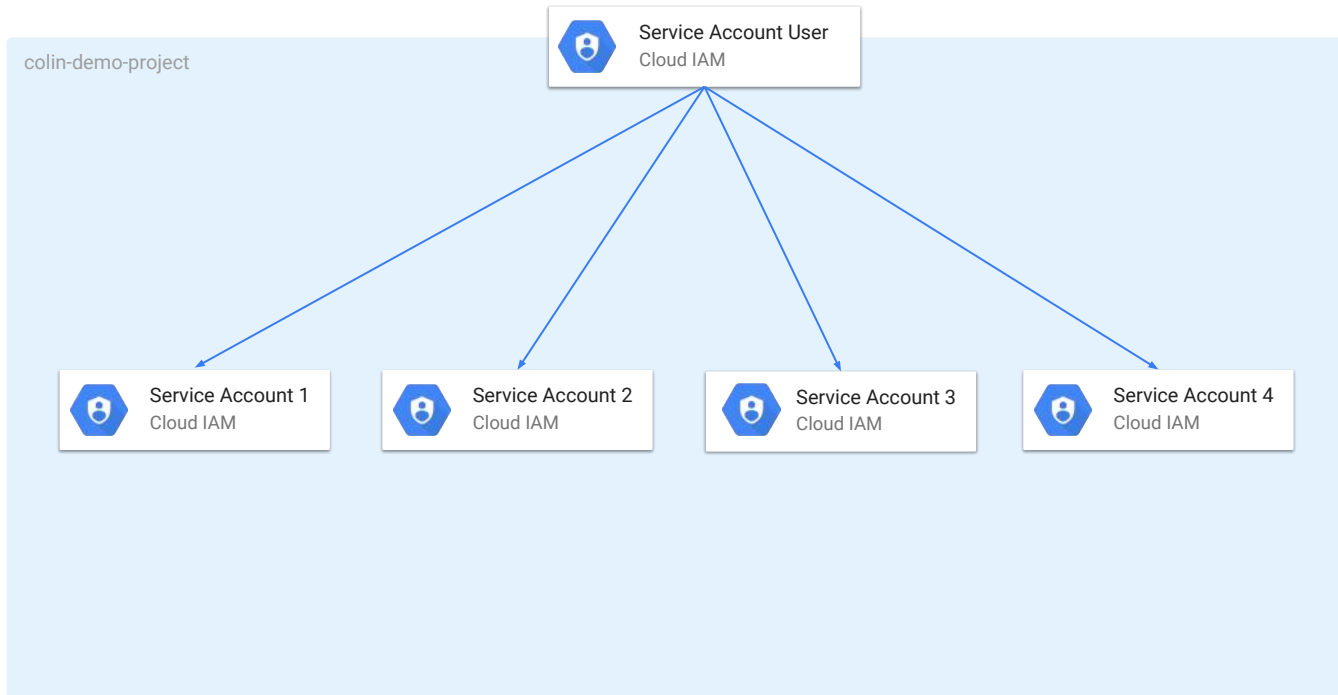
VPC Service Controls

```
accesscontextmanager.accessLevels.create
accesscontextmanager.accessLevels.delete
accesscontextmanager.accessLevels.get
accesscontextmanager.accessLevels.list
accesscontextmanager.accessLevels.update
accesscontextmanager.accessPolicies.create
accesscontextmanager.accessPolicies.delete
accesscontextmanager.accessPolicies.get
accesscontextmanager.accessPolicies.getIamPolicy
accesscontextmanager.accessPolicies.list
accesscontextmanager.accessPolicies.update
accesscontextmanager.accessZones.create
accesscontextmanager.accessZones.delete
accesscontextmanager.accessZones.get
accesscontextmanager.accessZones.list
accesscontextmanager.accessZones.update
accesscontextmanager.policies.create
accesscontextmanager.policies.delete
accesscontextmanager.policies.get
accesscontextmanager.policies.getIamPolicy
accesscontextmanager.policies.list
accesscontextmanager.policies.update
accesscontextmanager.servicePerimeters.create
accesscontextmanager.servicePerimeters.delete
accesscontextmanager.servicePerimeters.get
accesscontextmanager.servicePerimeters.list
accesscontextmanager.servicePerimeters.update
```

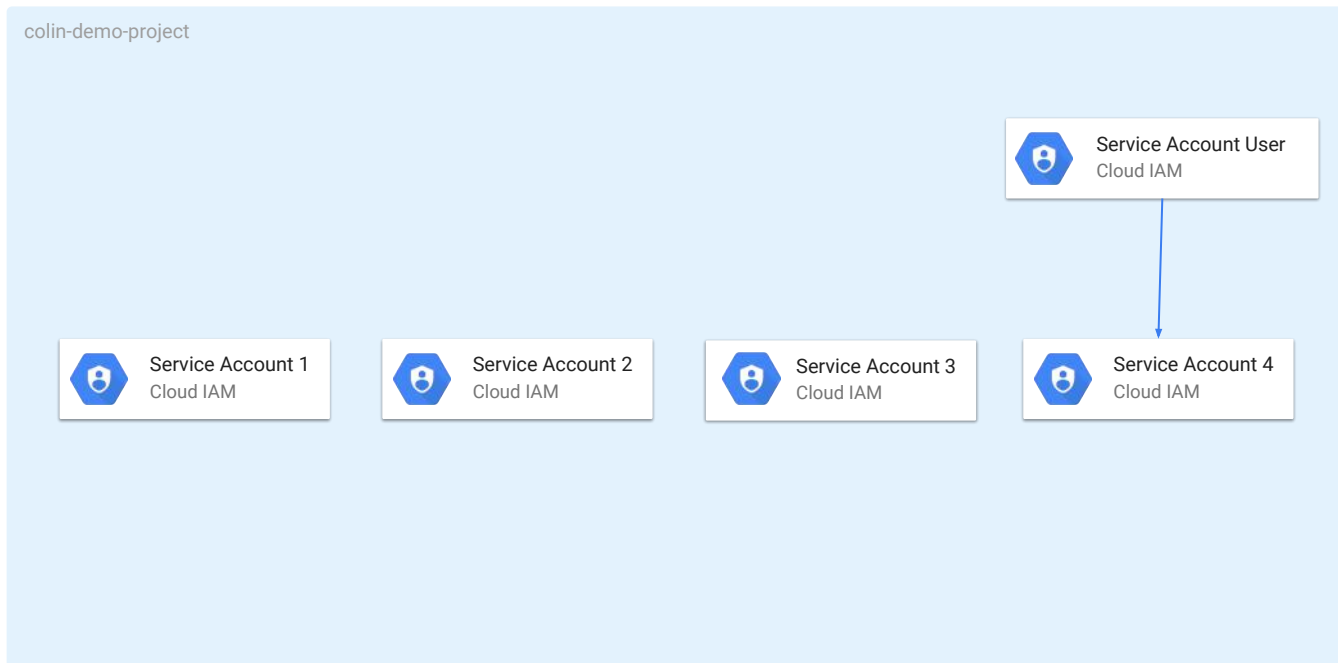
Service Account Impersonation

```
iam.serviceAccountKeys.create
iam.serviceAccountKeys.delete
iam.serviceAccountKeys.get
iam.serviceAccountKeys.list
iam.serviceAccounts.actAs
iam.serviceAccounts.create
iam.serviceAccounts.delete
iam.serviceAccounts.get
iam.serviceAccounts.getIamPolicy
iam.serviceAccounts.list
iam.serviceAccounts.update
```

Binding at the Project level



Binding at the Service Account Level



Permissions for Impersonating a Service Account

- **Generating Service Account Keys**

- iam.serviceAccountKeys.create
- iam.serviceAccountKeys.get

- **Impersonation only**

- iam.serviceAccounts.actAs

Why Service Account Impersonation?

- Privilege Escalation
- It's easy to lose track:
 - a. VMs could have service accounts
 - b. SSH keys could be applied project-wide
 - c. User can now operate as the service account from a VM
- Obfuscates your activity in GCP

Access Scopes for Virtual Machines

- Legacy Method for applying permissions
- Must be set when using a service account
- Restricts API access for the service account
- Set on a per-instance basis

Service account ?

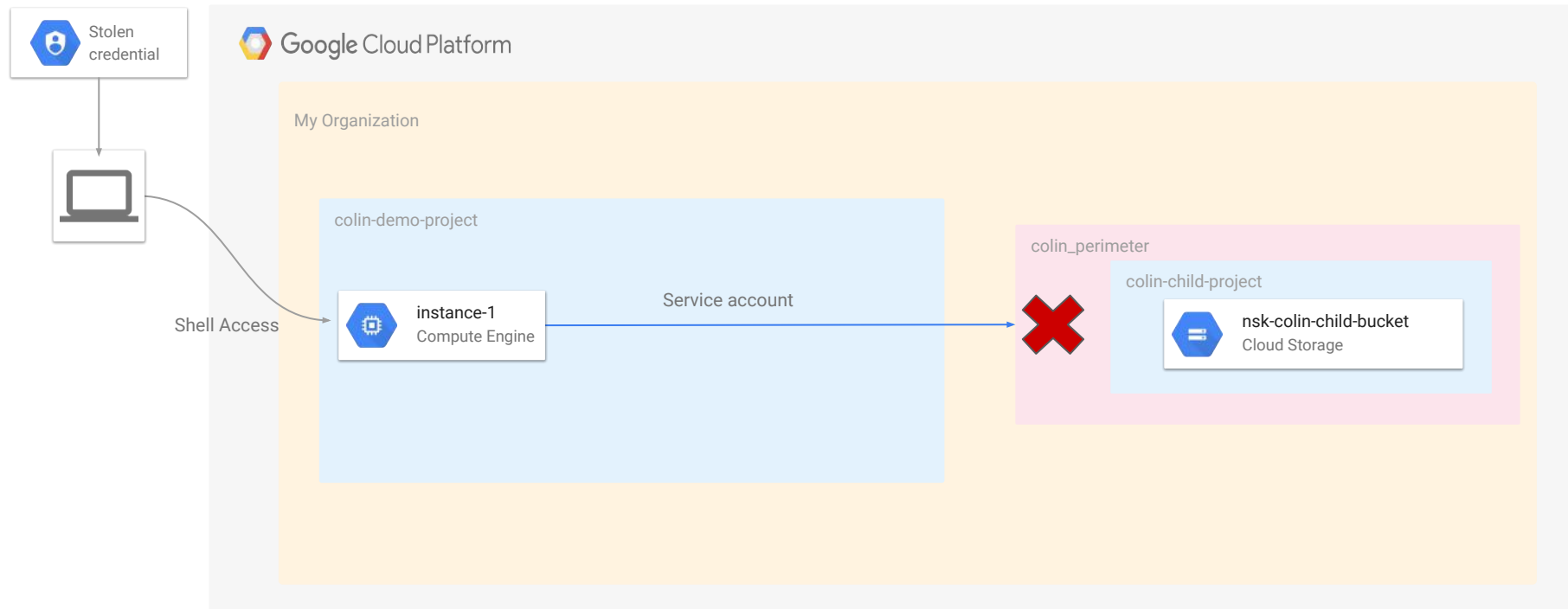
Compute Engine default service account ▼

Access scopes ?

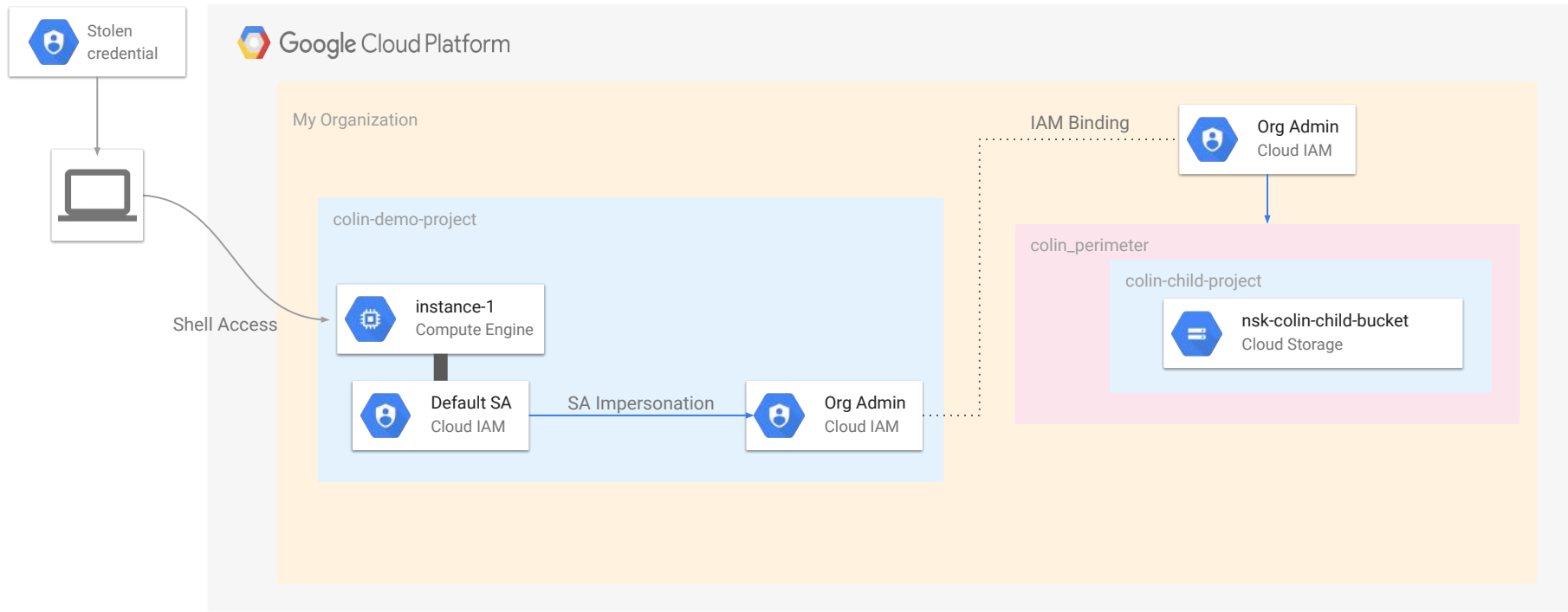
- ☐ Allow default access
- ☒ Allow full access to all Cloud APIs
- ☐ Set access for each API

GCP Demo

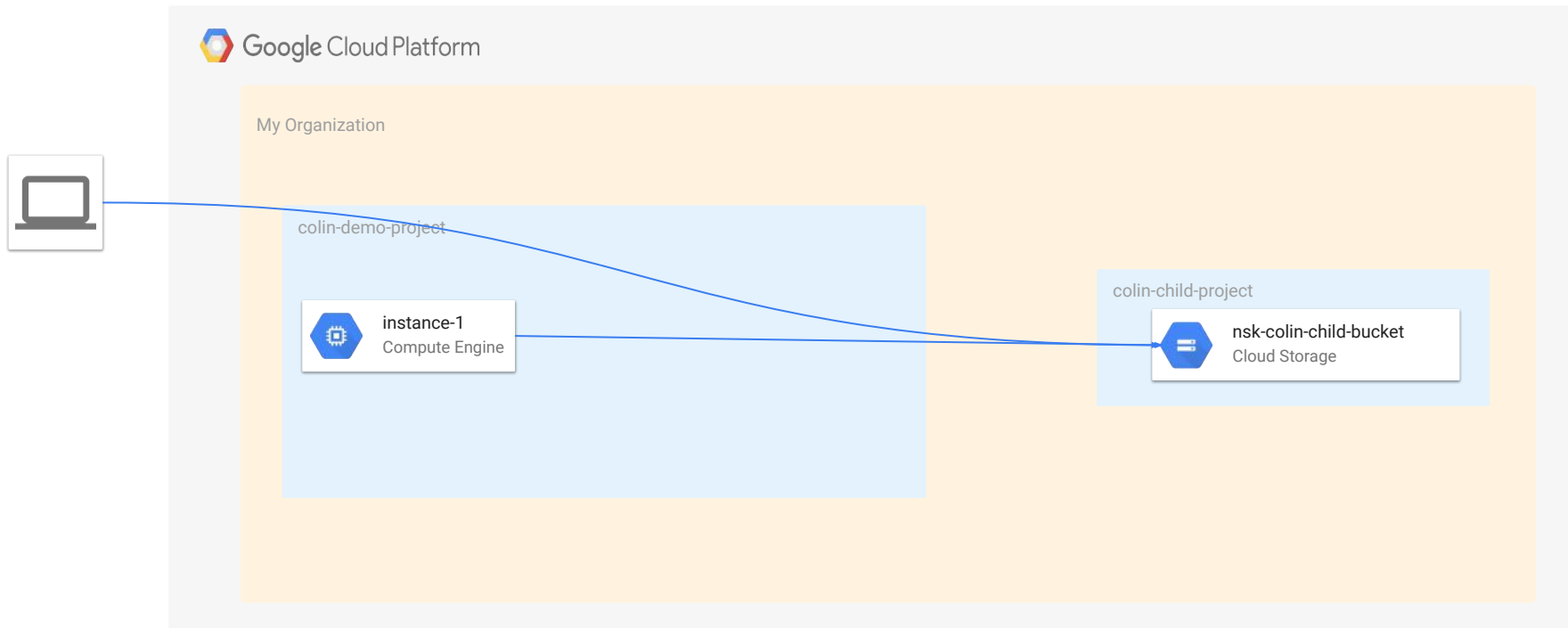
Our Scenario again...



IAM Flow



End Condition



Demo

Key Takeaways

- Keep Service Accounts with **elevated bindings** in their own Project(s)
 - Keep public workloads out of the Project
 - Keep the Project under lock and key
 - Service accounts in the same Project may be able to see each other
- Bind permissions to specific Service Accounts whenever possible
- Don't use Default Service Accounts
- Avoid using Primitive Roles



Thank you!

Colin Estep

Netskope Threat Research

<https://www.netskope.com/blog>