GCP

Google Cloud

Professional Cloud Security Engineer

Google Certified

Professional Security Engineer

Professional Security Engineer

- Pay attention for 5 minutes, before we dive in.
- Course is long, 12+ Hours of video
- Basic foundation for GCP is required
- Learn by Doing
- So with every exam objective, There is hand-on Lab – 50+

GCP certifications

https://cloud.google.com/certification/guides/cloud-security-engineer

Cloud Cost for this course

- $0 – for GCP account without domain
- Domain Purchase cost
- GCP Free trial
- $300 for next 3 months https://cloud.google.com/free
- Length: Two hours
- Registration fee: $200 (plus tax where applicable)
- Languages: English
- Exam format: Multiple choice and multiple select,

Udemy Tips

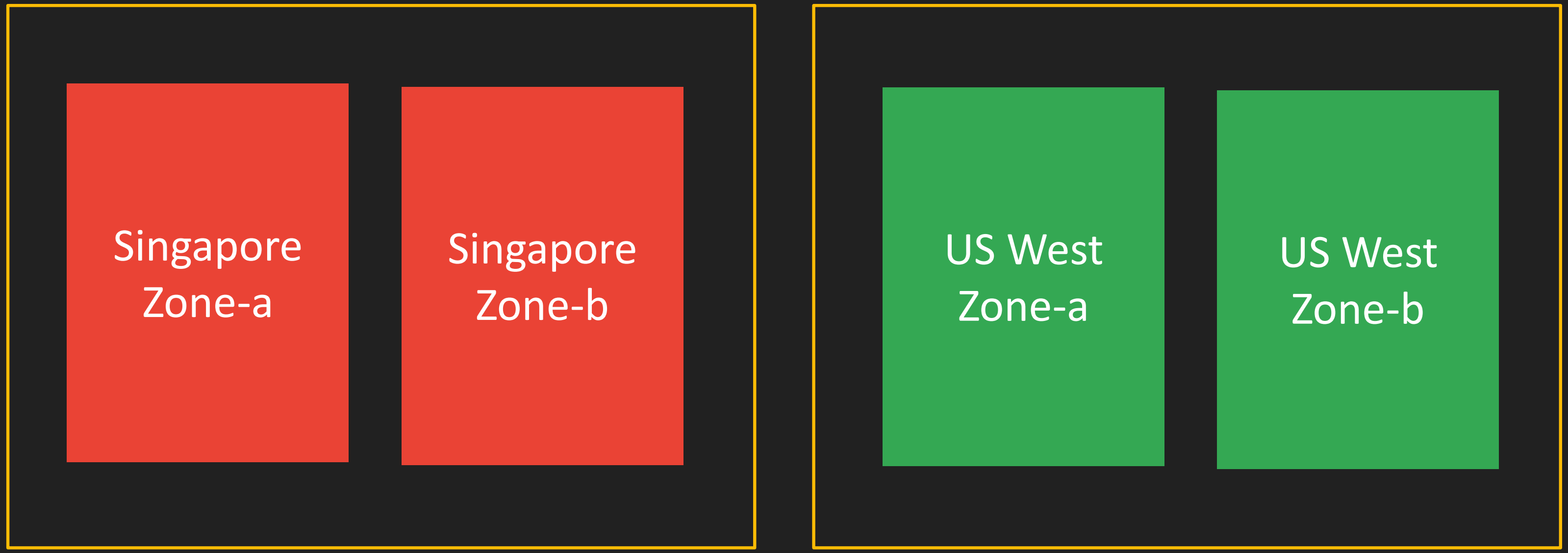
PSE Exam Guide

GCP Fundamental

GCP Regions & Zones

Why Zones & Regions

- Low latency
- Follow Government rules
- High availability
- Disaster recovery



Singapore Zone-a

Singapore Zone-b

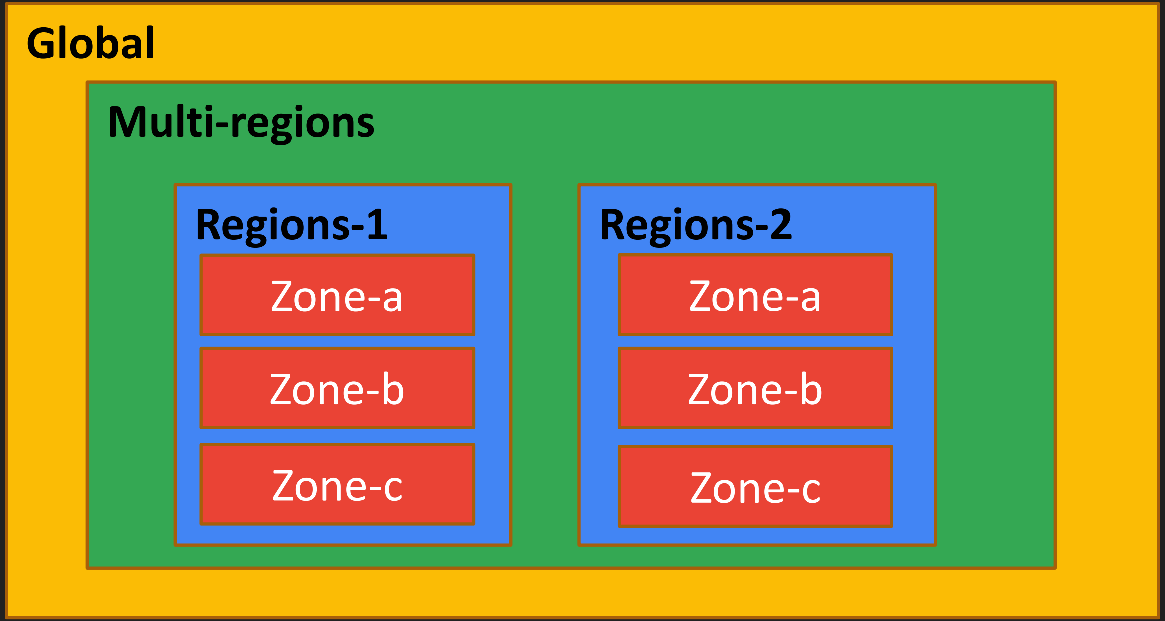
US West Zone-a

US West Zone-b

GCP (Zones & Region)

Fascinating Number: Google Is Now 40% Of The Internet (forbes.com)

- Zones – Independent data Center
- Region – Geographical area
- Multi-region : Collection of Geographical
- Global - Anywhere



Global Locations - Regions & Zones | Google Cloud

GCP Services

- GCP has 200+ services
- Security Engineer certification
  - Encryption
  - VPC
  - Hybrid Connectivity
  - Data Loss
  - SCC – Security Command Center

GCP Security at Google

BY ANKIT MISTRY

Security at Google

- What Google does to secure your app, data
- How Google does all these
- Security mechanism at different layers
- Shared responsibility model
- Tools GCP provide to secure your resources
- Regulatory compliance

Why trust on Google for Security

- Google has more than 7 app having billion plus users
- Security is main concern for Google
- Your app, data will be deployed in same infra where these amazing app is hosted.
- Google has hundreds of dedicated engineer working on security of their platform 24x7

How Google Secure Infra

- Hardware layer
  - Less than 1% of employee has physical access to data center
  - Google builds all hardware required for infrastructure
- IAM
  - Identity & access management
  - IAM centrally manage all Authorization
  - Who can do what on which resources

Contd

- User management
  - Google account authentication – Support for SAML
  - Enforce rule
    - Password length, 2 step verification
- Storage Data
  - Google By default encrypt all data with Google managed encryption key
  - CMEK, CSEK
- Data in Transit
  - Google encrypt all traffic which goes beyond physical boundary of Google.

Contd

- GCP offers IAP to secure your VM & App engine
- Built-in DOS attack prevention
- Data loss prevention
  - To Inspect
  - To Redact
  - To Transform
  - To re-identify PII Data

Contd

- VPC layer Security
  - Some Cloud native solutions
  - Subnet
  - Firewall rules
  - Ingress/Egress Traffic
  - Cloud Armor
- Operations
  - Logging, Monitoring, trace, Profiling

Contd

- Regulatory Compliance
  - Encryption, Hardware security, VPC Firewall is technical aspect of security
  - Compliance is another important face of Security.
  - Cloud providers need to follow different compliance standard.
  - Google does verification of Compliance after periodic interval.

Shared Responsibility Model

- Google Responsibility to secure cloud, app, data is one aspect
- As a cloud user, also responsible to secure individual resources
- Its shared responsibility between user & Google

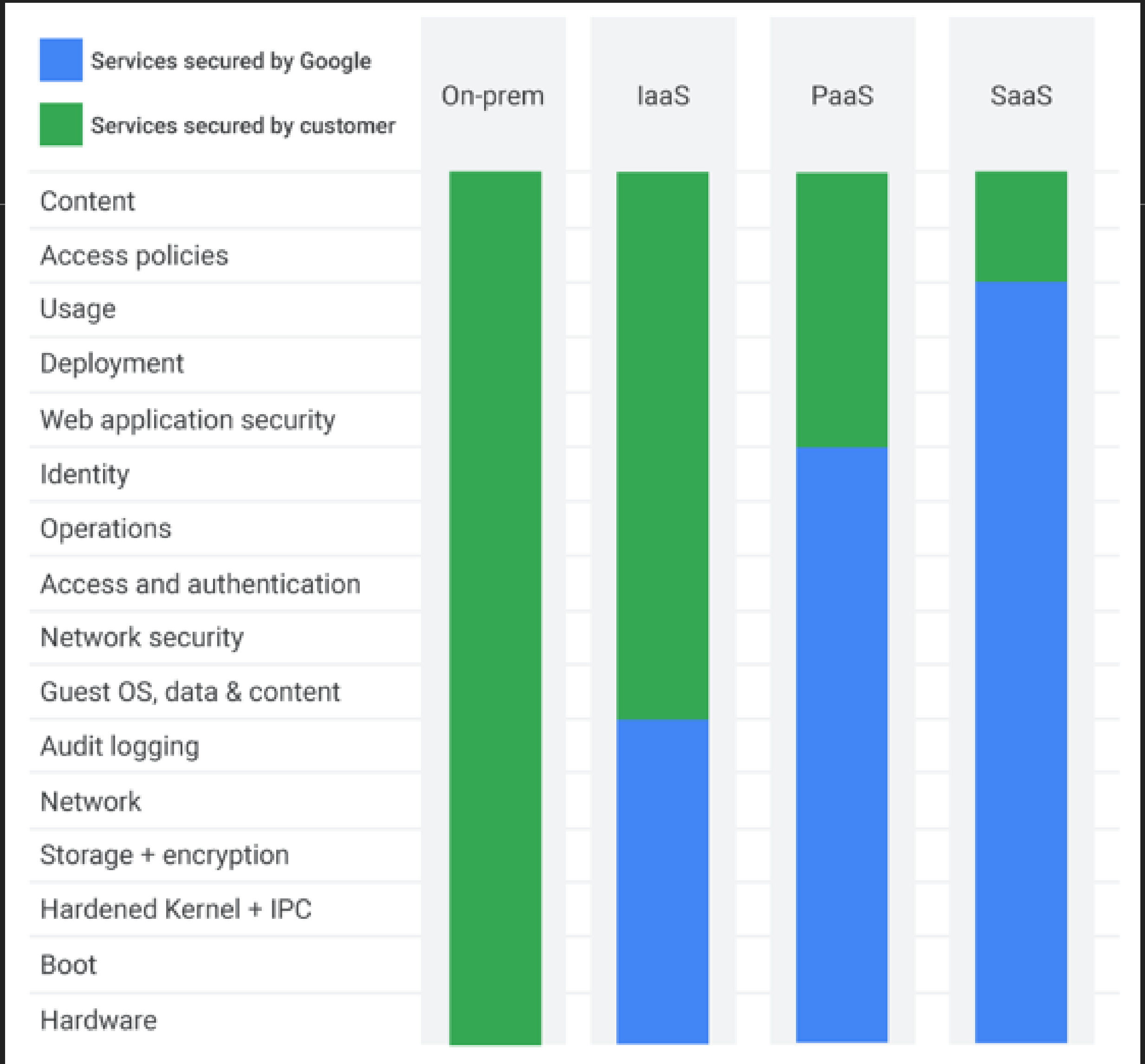


Figure 1: Responsibility chart

https://cloud.google.com/security/incident-response

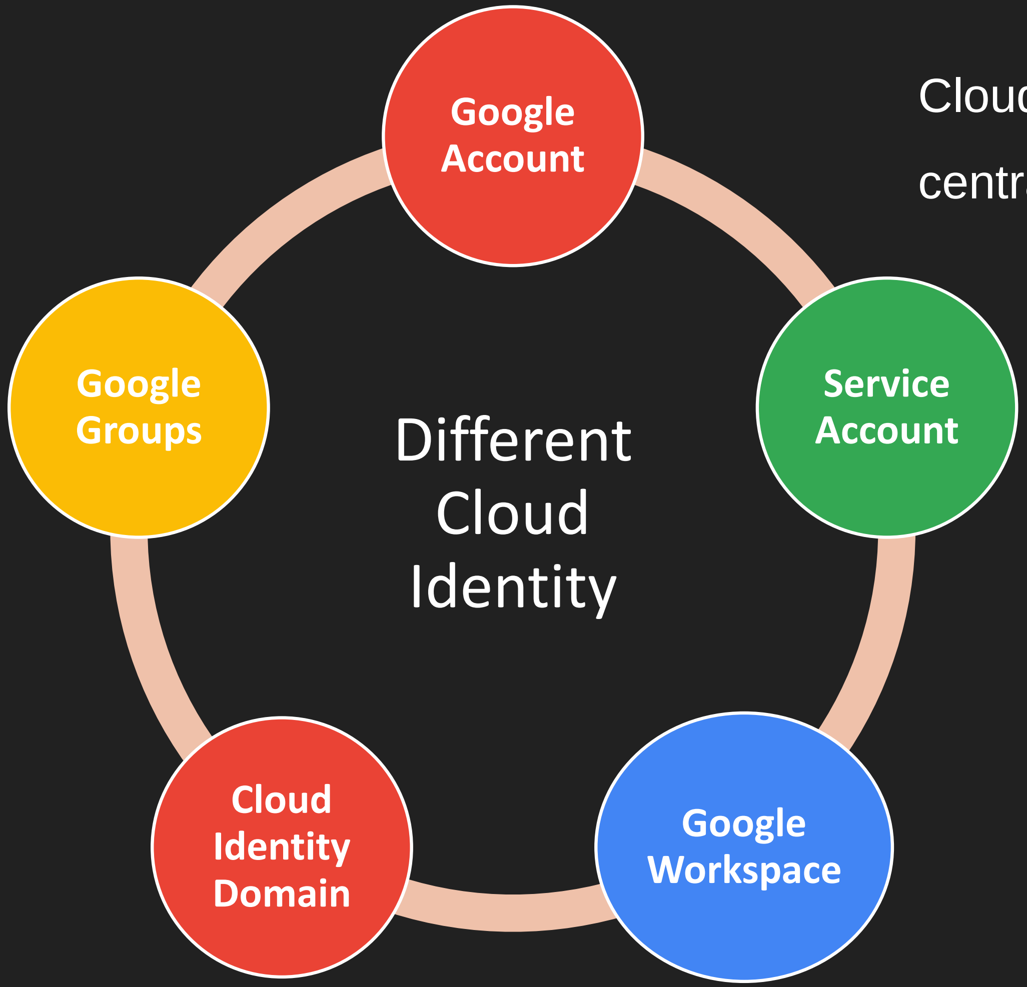
1.Configuring Access Within Cloud Solution Environment

BY ANKIT MISTRY

Module 1

- Cloud Identity Domain
- Google Admin Console
- Resource hierarchy
- IAM – Identity & access management

Cloud identity



Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.

Google Account

- With Any valid Email-ID
  - Gmail is common one.
- https://accounts.google.com/
- Good
  - when Learning GCP
  - Demonstrating some tutorial on GCP Console
- Issue :
  - Personal ID – Not Organization specific
  - If Employee left organization
- In GCP Console :
  - No Organization
  - You can not create Folders Hierarchy

Google Workspace

- Like Office 365
- Paid Subscription for all Office apps like :
  - Sheets, Slides, Docs & many more
- Verified Domain - *Example.com*
- Complete user management for employee in (*Example.com*)
- Subscription – per user per month/annual - 14 days Free Trial
- Admin management Console - https://admin.google.com

Google Cloud identity Domain

- Like Google Workspace without all apps
- Google Workspace = Paid Apps + Cloud identity Domain
- Verified Domain - *Example.com*
- Complete user management for employee in (*Example.com*)
- Subscription – Free/Paid
  - For Paid start with 14 Days Free Trial
- Admin management Console - https://admin.google.com

Create Cloud Identity Account (Hands-on)

BY ANKIT MISTRY

Verify Cloud Identity Domain (Hands-on)

BY ANKIT MISTRY

(Free trial)
GCP Account with Cloud Identity Domain

BY ANKIT MISTRY

(Free trial) GCP Account with Google Personal Account

BY ANKIT MISTRY

Explore Google Admin Console

BY ANKIT MISTRY

Add users (Hands-on)

BY ANKIT MISTRY

Create Groups(Hands-on)

BY ANKIT MISTRY

Password Policy & 2SV(Hands-on)

BY ANKIT MISTRY

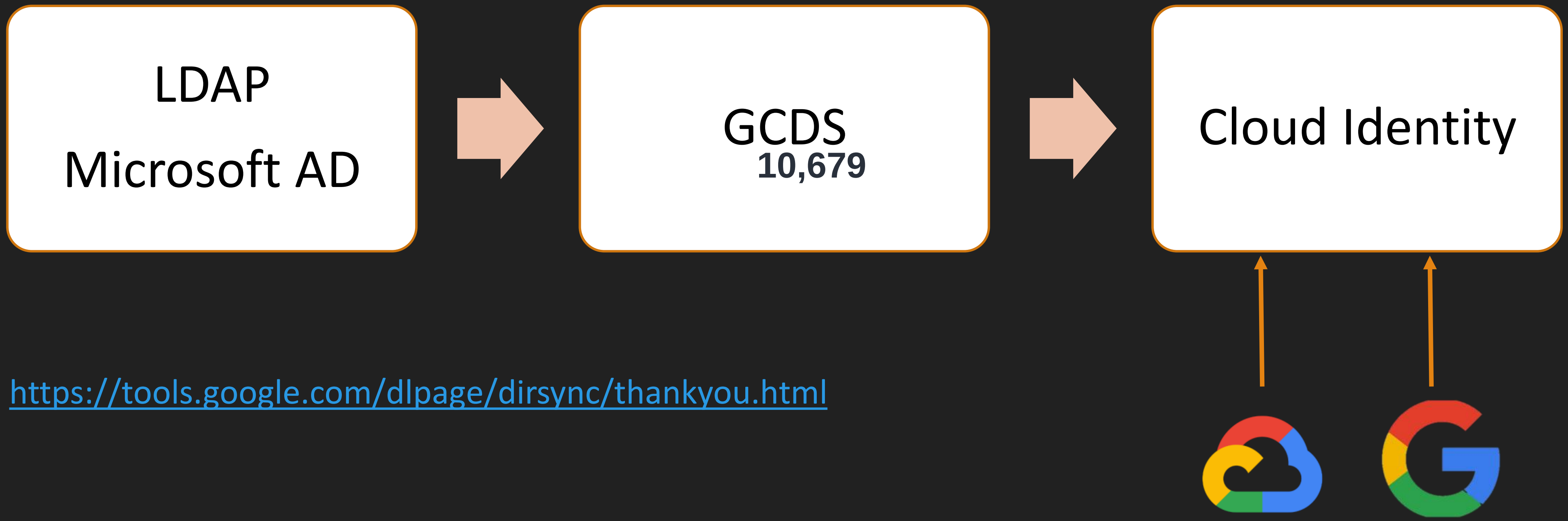
Google Cloud Directory Sync - GCDS

BY ANKIT MISTRY

GCDS

- Google Cloud Directory Sync (GCDS) helps you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server
- GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account
- You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.

GCDS



LDAP

Microsoft AD

GCDS

10,679

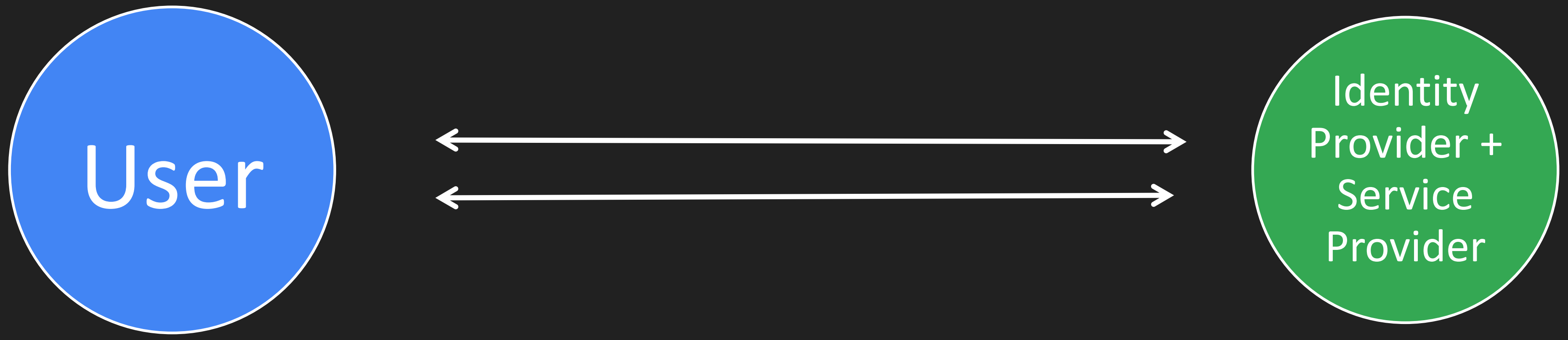
Cloud Identity

https://tools.google.com/dlpage/dirsync/thankyou.html

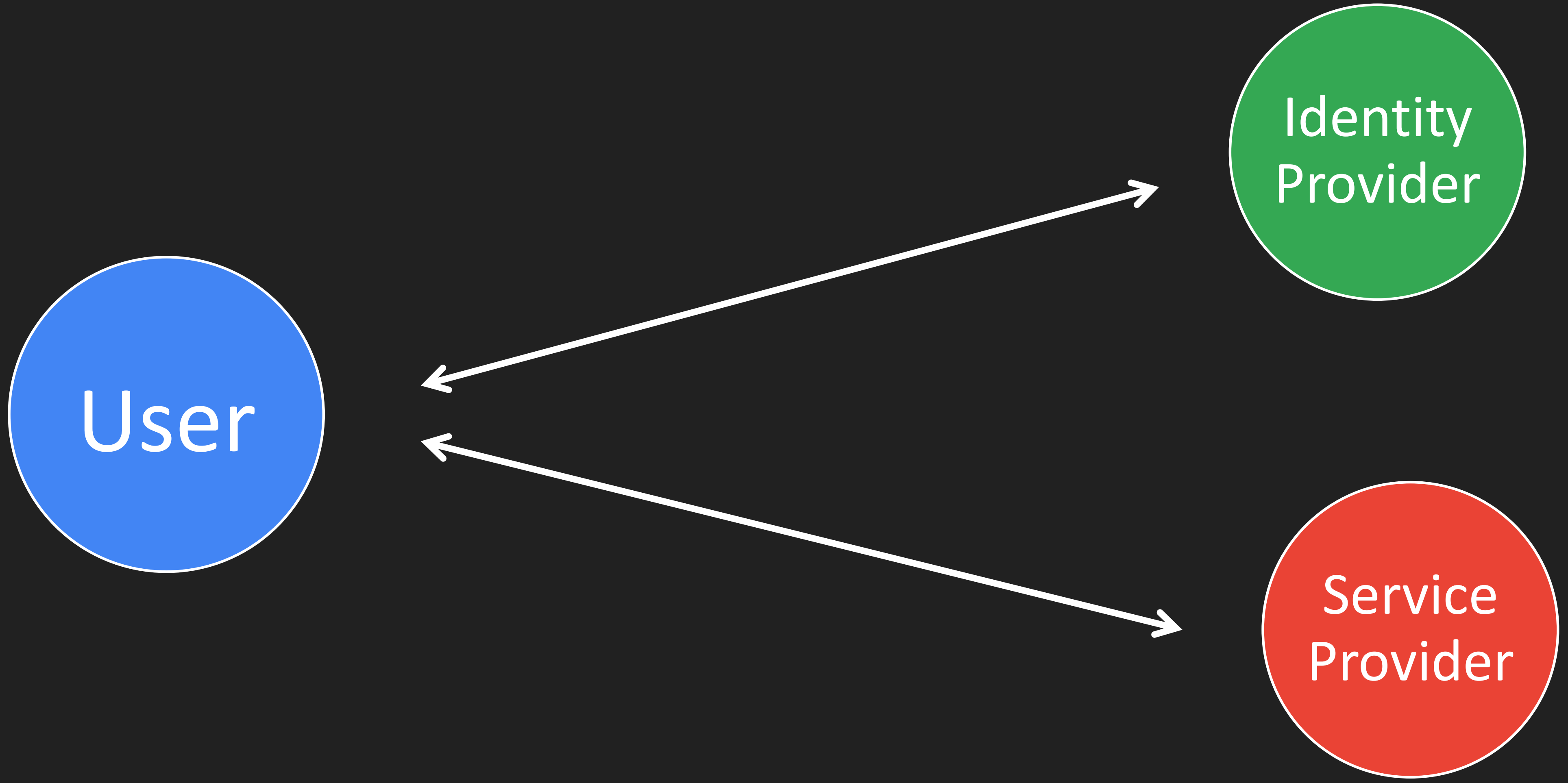
SAML

- Security Assertion Markup Language
- Google authentication
  - Credential stored at google server
  - password, user info, etc…
  - Google behaves like service provider + identity provider
- SAML – SSO based authentication
  - use our organization or some third party as identity provider
  - Google as service provider

Google Authentication



SSO

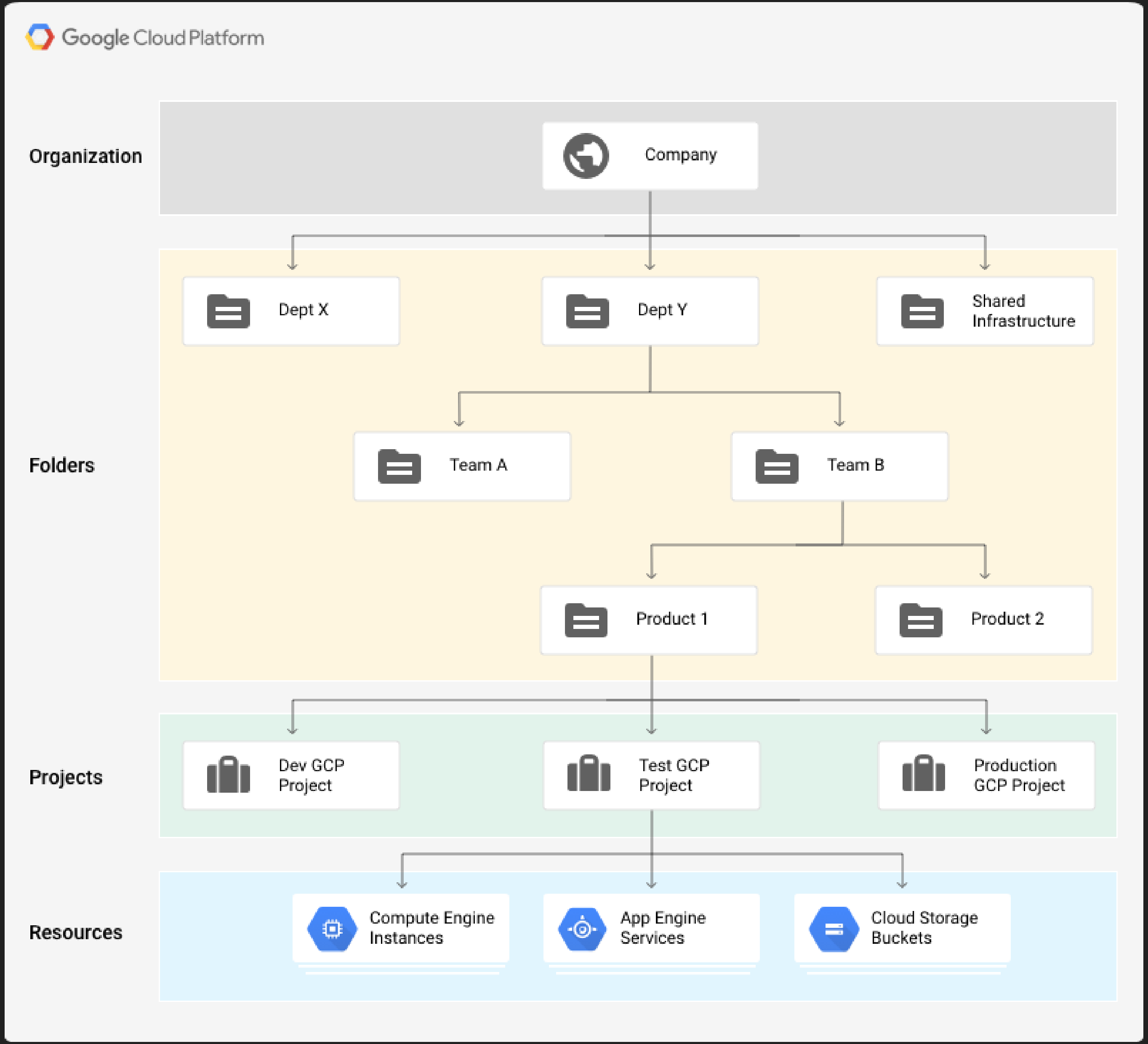


Configure SAML in Console

Let’s visit :

https://admin.google.com/

Resource Hierarchy in GCP



Google Cloud Platform

Organization

Company

Folders

Dept X

Dept Y

Shared Infrastructure

Team A

Team B

Product 1

Product 2

Projects

Dev GCP Project

Test GCP Project

Production GCP Project

Resources

Compute Engine Instances

App Engine Services

Cloud Storage Buckets

Organization policies

BY ANKIT MISTRY

3 Policy Use cases

- Disable service account creation
- Enforce uniform bucket-level access
- Skip default network creation

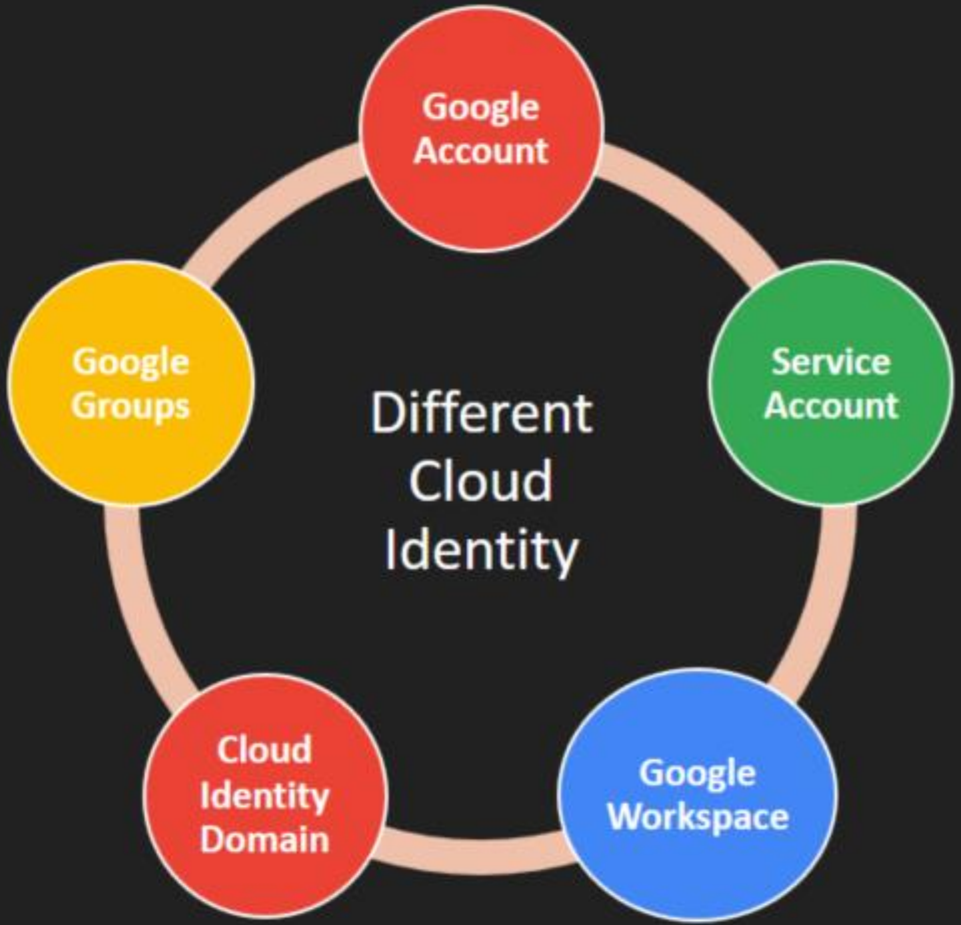
GCP : IAM

- IAM – Identity & Access management
- Fine-grained access control and visibility for centrally managing cloud resources.
- Who can do What on Which resources.
- Who - Identity - Member - Email
- What – Roles (Collection of Permissions)
- Which (Resources, Compute, Appengine, BigQuery)

X can Create VM in Compute Engine

Y **can** Delete, Create Bucket **in** Cloud Storage

Identity


Google Account
Service Account
Google Workspace
Cloud Identity Domain
Google Groups
Different Cloud Identity

Roles

Primitive

- Owner
- Editor
- Viewer

Pre-defined

- Role on single service
  - Compute Admin
  - Network viewer
  - Big query Job user

Custom Role

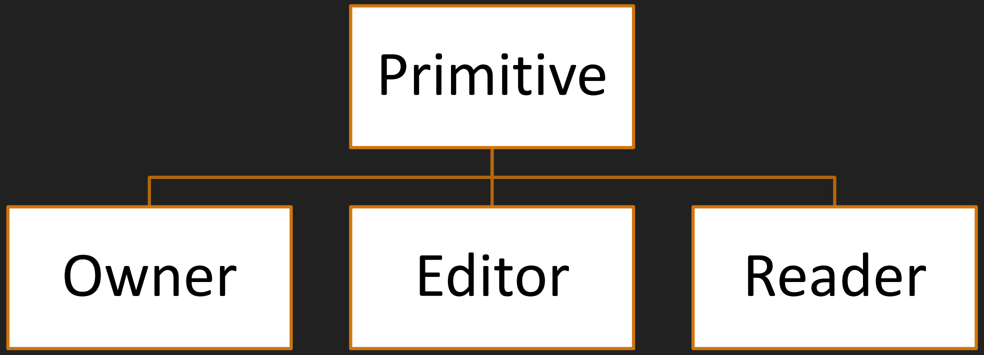
- Customized
- Can be created from Predefined role

Permission

- Roles = Collection of permission
- Structure of permission :
  - Service.ResourceType.Verb
- Example :
  - bigtable.tables.get
  - cloudfunctions.functions.list
  - storage.objects.delete
  - compute.disks.create

Primitive Roles

- Too much Broad access
- Not recommended
- Does not follow principal of least privilege
- Reader = Read only permission for all resource inside project
- Editor = Reader + Modification
- Owner = editor + manage user, groups, billing



Primitive

Owner

Editor

Reader

Pre-Defined Roles

- GCP defined Role
- Maintained by GCP
- For each product/services – Different sets of Roles defined
- Like :
  - Compute Admin
  - Network viewer
  - Big query Job user

Assign Roles to Identity

BY ANKIT MISTRY

Custom Roles

- Custom Defined
- Custom Roles can be defined by :

1. Combined Permission from multiple pre-define role
2. Remove Permission from pre-define role
3. Add Permission to pre-define role
4. Add list of permissions

Requirement for Custom Role

- For New Joinee , Create custom role from below requirement
  - can upload object inside bucket - create
  - can not delete object
  - can not create bucket

Assign Role at Org/Folder level

BY ANKIT MISTRY

Demo Steps

- User kapil

1. <u>Part – I</u>
    1. at Project level – Compute Admin
    2. at org level – Editor
2. <u>Part – II</u>
    1. Provide 2 role at same level

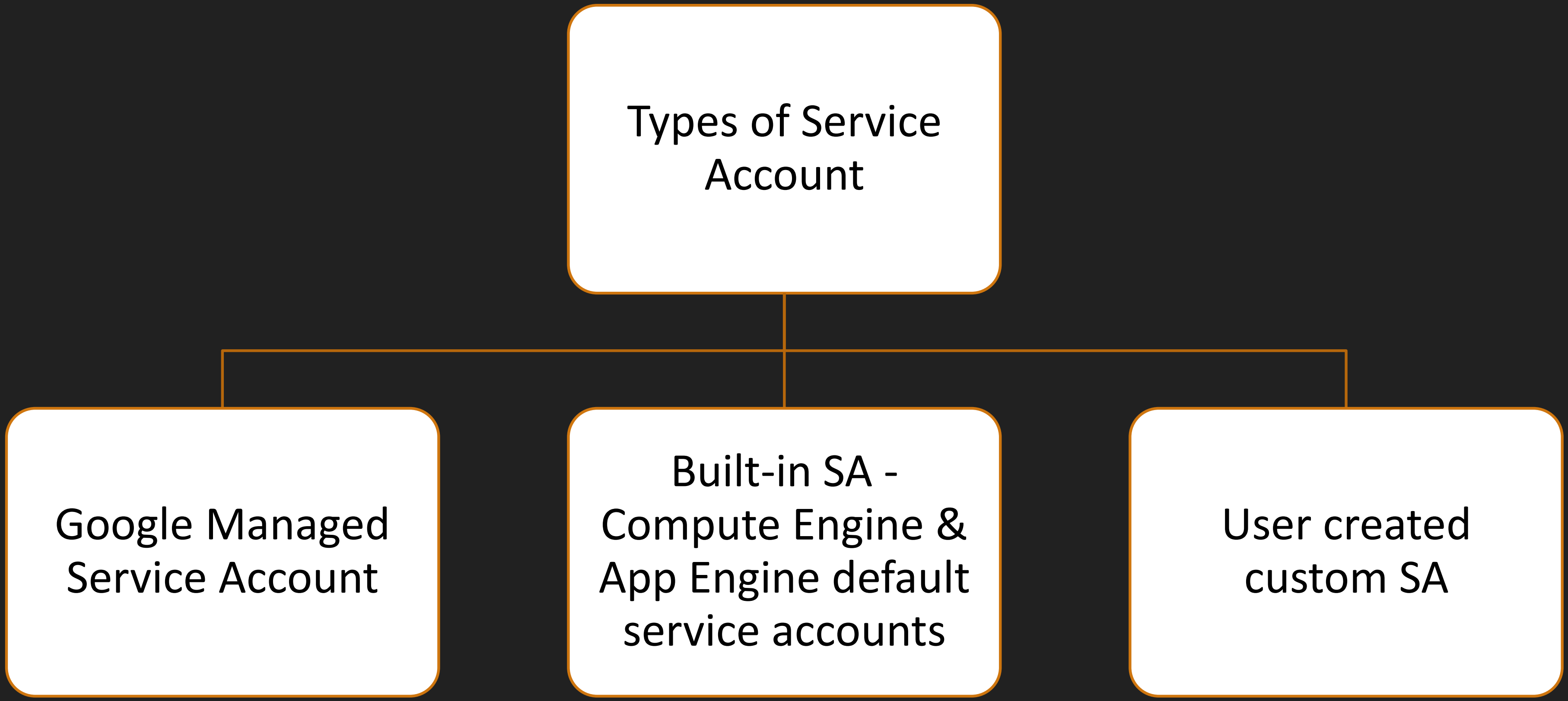
Service Account

BY ANKIT MISTRY

Service Account

- For non human – like for Apps, services
- Service Account is identity for Compute engine
- Service account keys for authentication
- Max 10 keys per Service Account
- Max 100 Service Account per project

Types Service Account



Types of Service Account

Google Managed Service Account

Built-in SA - Compute Engine & App Engine default service accounts

User created custom SA

[Hands-on] Create Service Account

BY ANKIT MISTRY

[Hands-on]
Service Account + Virtual Machine

BY ANKIT MISTRY

[Hands-on]
Cloud API access scopes
From Virtual Machine

BY ANKIT MISTRY

Access Scope

Legacy

- 3 Access Scopes
  - Allow default access
  - Allow full access to all Cloud APIs
  - Set access for each API
- Drawbacks – Machine must be stopped

Modern : IAM

- Assign role to Service account like Identity
- No Machine restart required

Service Account as Identity

- Service Account can be used as identity for Compute Engine, App Engine
- Service Account User role
  - User can use SA identity for Compute Engine, App Engine if user has
  - iam.serviceAccounts.actAs Permission
  - Service Account User role

Service Account as Resource

- User can use Service Account (Like Resource)
- User can do all things which role assigned to SA
- impersonate Service Account
- How to Do?
  - Provide user Service Account Token Creator role

Service Account RSA Private Key

- Like Google Account has Password
  - Service Account has keys
- Keys can be used for Authentication
- Generate Key from Cloud Console
- gcloud auth activate-service-account --key-file=rsa_private_keys.json

2.Configuring network security

BY ANKIT MISTRY

Module 2

- Network Resources
  - VPC, Firewall, Subnets, CIDR
- Share VPC & VPC Peering
- Cloud Interconnect – Partner interconnect
- Cloud VPN
- Cloud Load balancing

CIDR notation

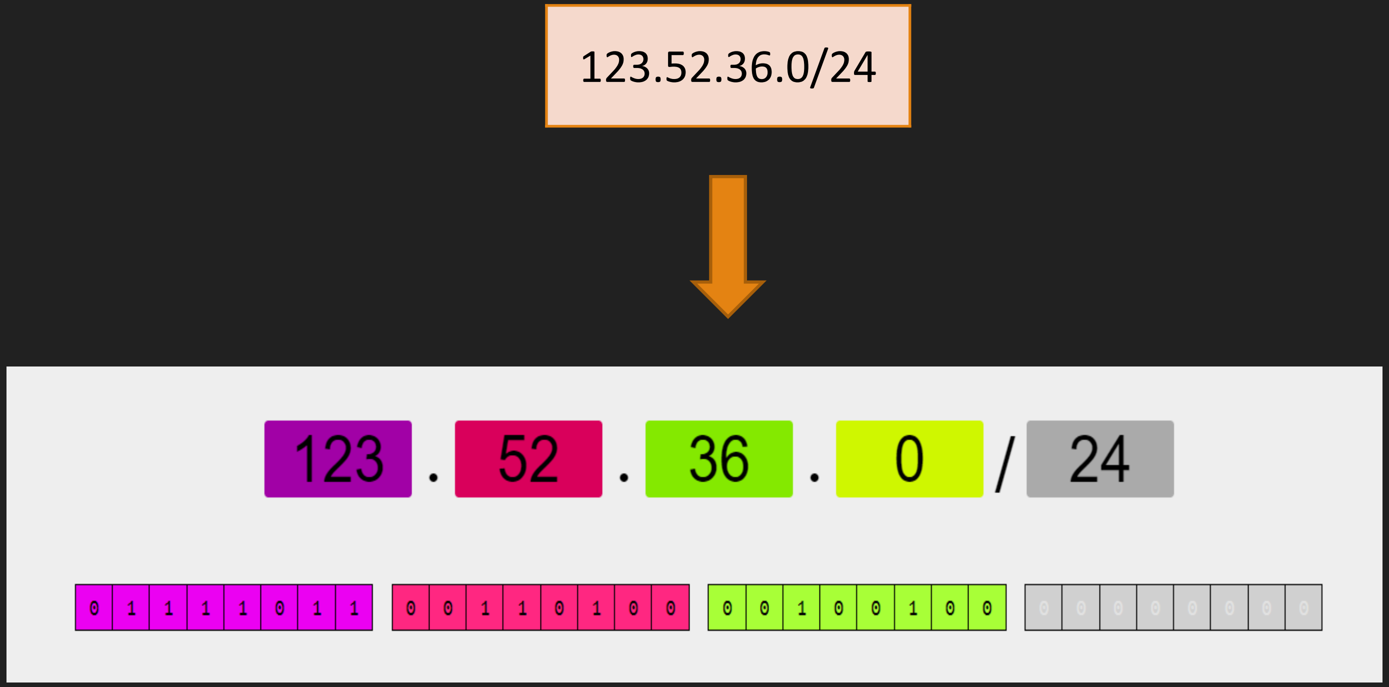
Classless Inter-Domain Routing

123.52.36.0
123.52.36.1
123.52.36.2
123.52.36.3
123.52.36.4
123.52.36.5
123.52.36.6
123.52.36.7
123.52.36.8
123.52.36.9
123.52.36.10
123.52.36.11

→ 123.52.36.0 / 24

123.52.36.0/24

CIDR notation



123.52.36.0/24

123 . 52 . 36 . 0 / 24

0 1 1 1 1 0 1 1 | 0 0 1 1 0 1 0 0 | 0 0 1 0 0 1 0 0 | 0 0 0 0 0 0 0 0

123.52.36.0
123.52.36.1
123.52.36.2
123.52.36.3
123.52.36.4
||
||
||
||
||
123.52.36.254
123.52.36.255

CIDR Notation

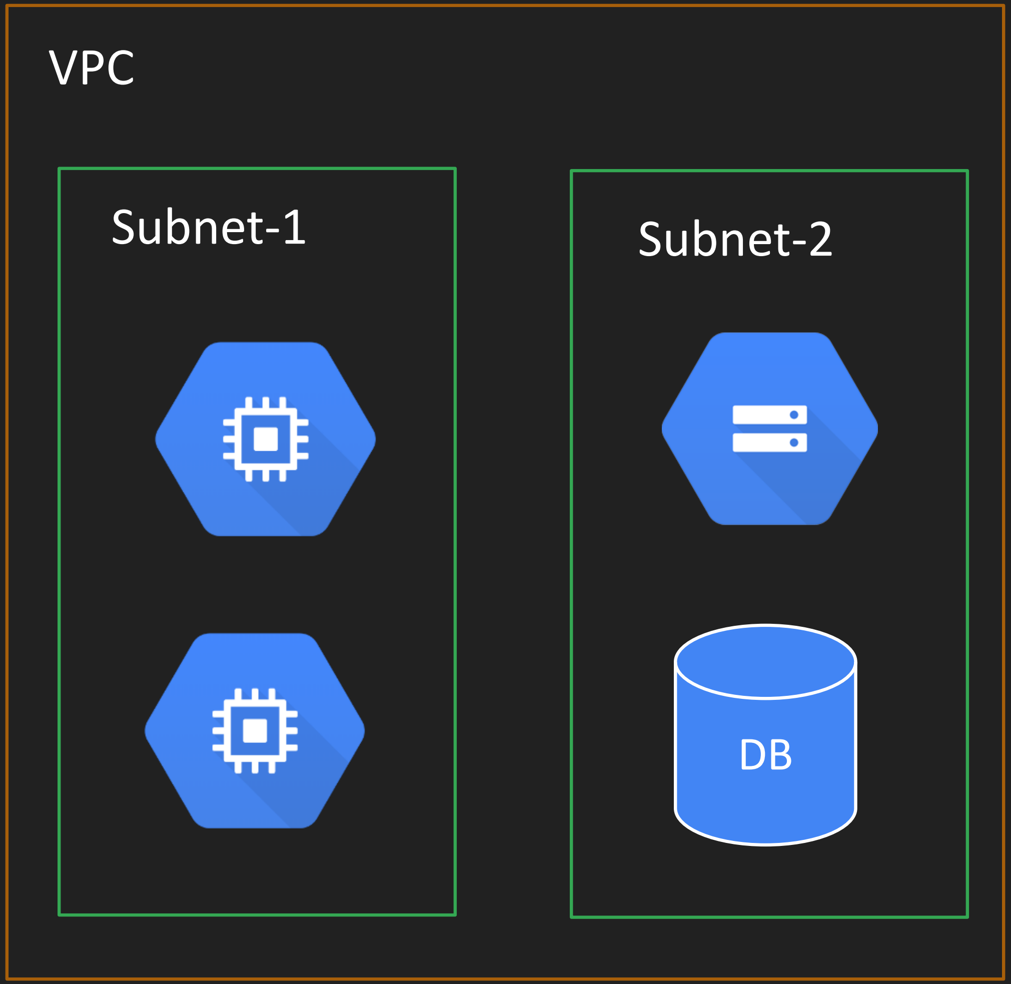
123.52.36.0/28	28 bits are fixed	4 bits are variable	Total IP address – 2^4 = 16
123.52.36.0/31	31 bits are fixed	1 bit is variable	Total IP address – 2^1 = 2
0.0.0.0/32	32 bits are fixed	0 bits are variable	Total IP address – 2^0 = 1
0.0.0.0/0	0 bits are fixed	32 bits are variable	Total IP address – 2^{32} = 4,294,967,296

VPC - Subnetworks

- No Network -> No Cloud
- Virtual version of a physical network
- Networks are part of projects
- It’s Global resources
- Placeholder to keep all your resources
- Max 5 networks per project
- No IP Assigned

- Network contain subnets
- Subnets are used for segregate resources
- Subnets has IP ranges
  - Expressed as CIDR notation
- VPC must have minimum one subnet
- Subnet belongs to one single region in GCP

VPC – Subnetworks



Types of VPC

Default

- Created when compute engine API enabled
- Every project has default VPC
- There is one subnet per regions

Auto

- With Auto mode, Default VPC can be created
- Fixed subnetwork ranges per region
- Can expand from /20 to /16
- Default firewall can be added easily.

Custom

- No Subnet automatically created
- Subnet creation manual
- Custom IP range allocation
- No necessary to create subnet in each region

[Hands-on] Default VPC

BY ANKIT MISTRY

[Hands-on]
Auto Mode VPC

BY ANKIT MISTRY

[Hands-on] Custom Mode VPC

BY ANKIT MISTRY

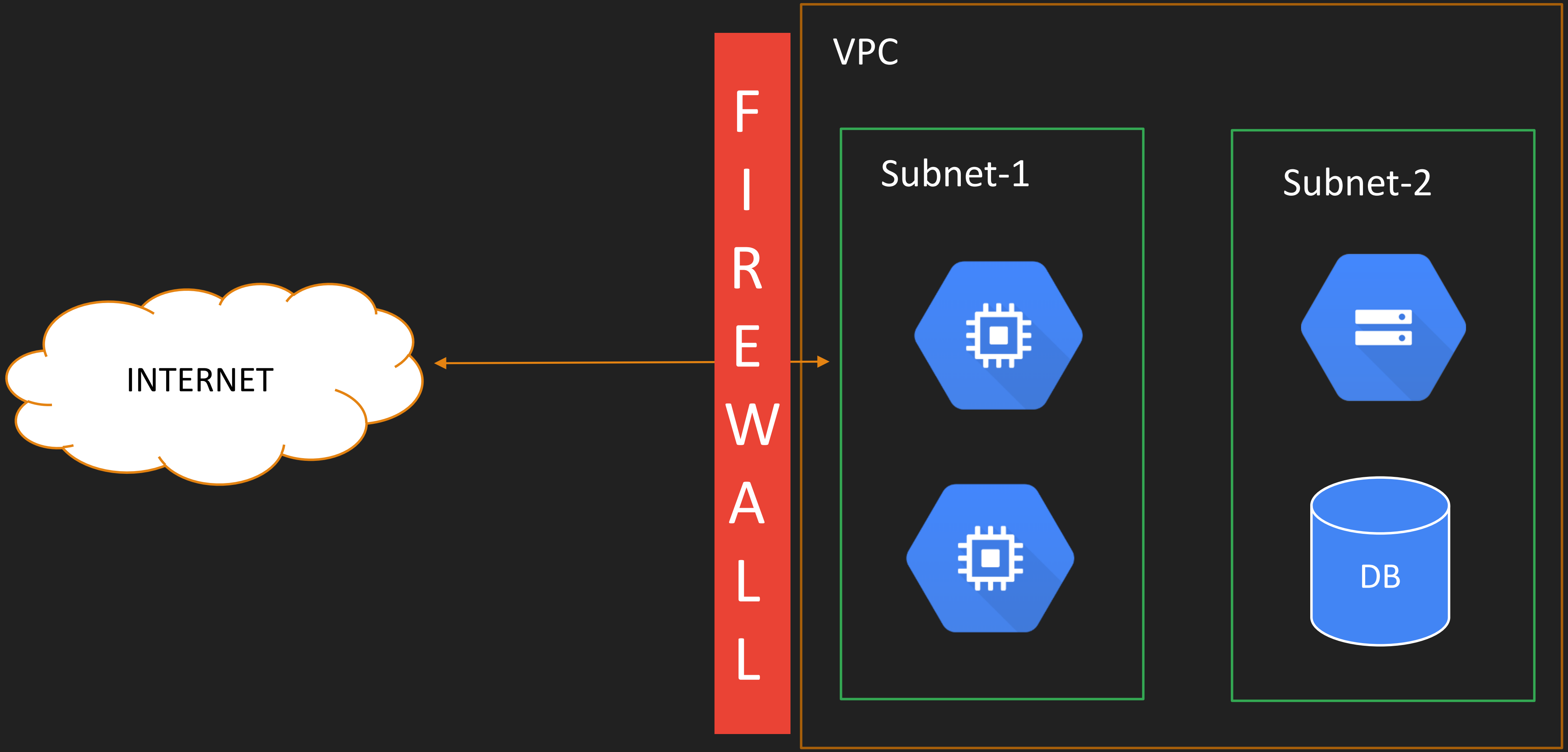
[Hands-on] Custom Mode VPC

BY ANKIT MISTRY

[Hands-on]
Create VM with all 3 VPC

BY ANKIT MISTRY

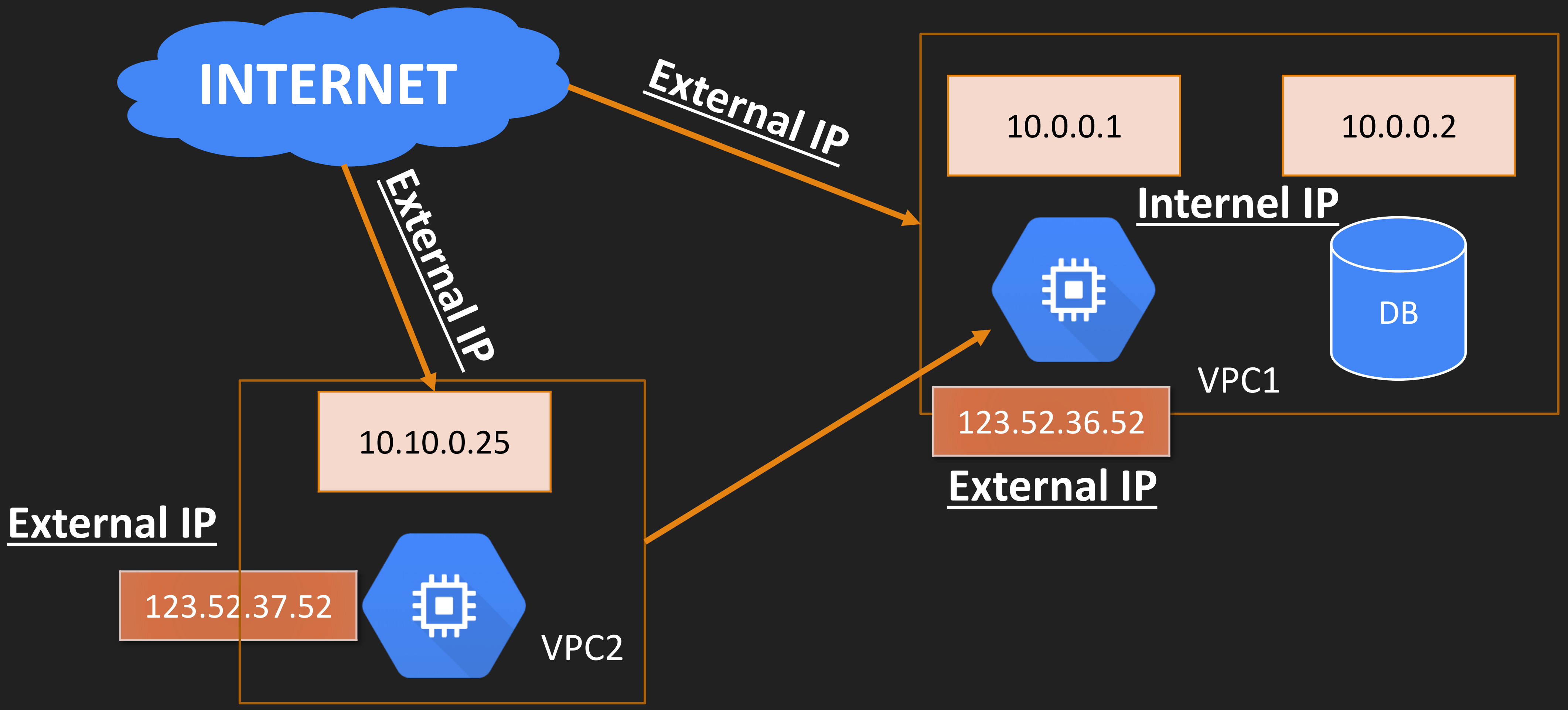
Firewall



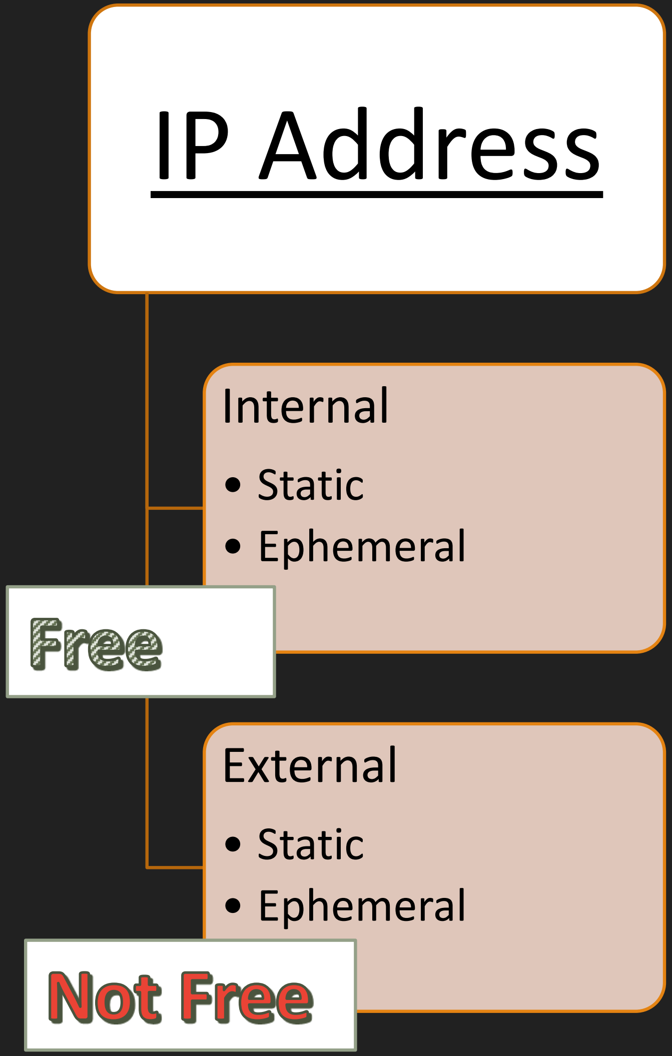
Firewall rules

- Trust nothing by default
- Some default rule :
  - Allow all outgoing traffic - egress
  - Deny all incoming traffic - ingress
- Rule has priority number : (0-65535)
  - Lower the number higher priority
- Common port/protocol
  - 22 – SSH, 3389 - RDP
  - ICMP – ping
  - 80 - HTTP/HTTPS

Internal IP – External IP



Static vs ephemeral IP



IP Address

Internal

- Static
- Ephemeral

Free

External

- Static
- Ephemeral

Not Free

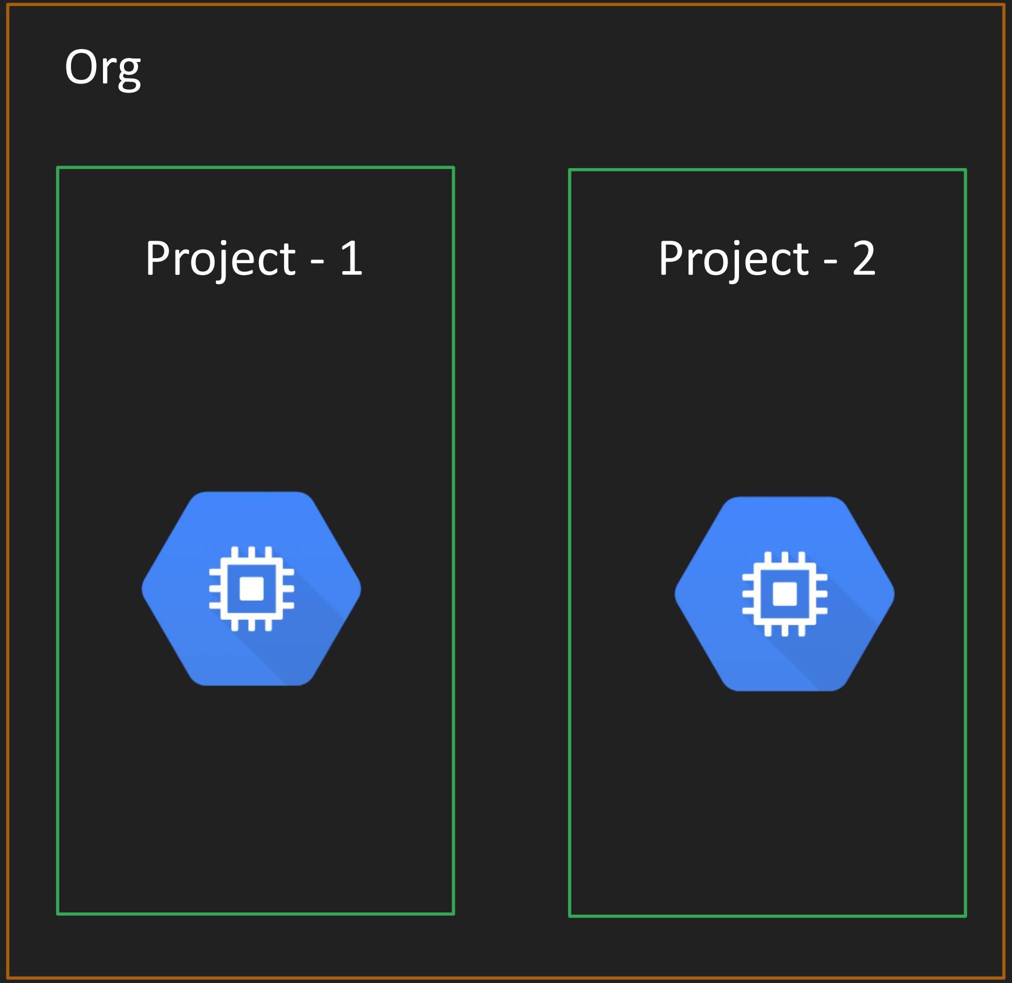
- Ephemeral IP
  - Short Lived
  - Changes after VM restarts
- Static IP
  - Constant – Can be exposed to outside
  - High cost when not in use

[Hands-on]
Expand Subnet IP ranges

BY ANKIT MISTRY

Shared VPC

- Host Project - Shared VPC
- Multiple Service Project
- Central management of VPC
- Large organization use shared VPC
- Max Host project – 100
- Max Service Project – up to 100
- Shared VPC is only available for projects within an organization node only



[Hands-on]
Shared VPC Demo

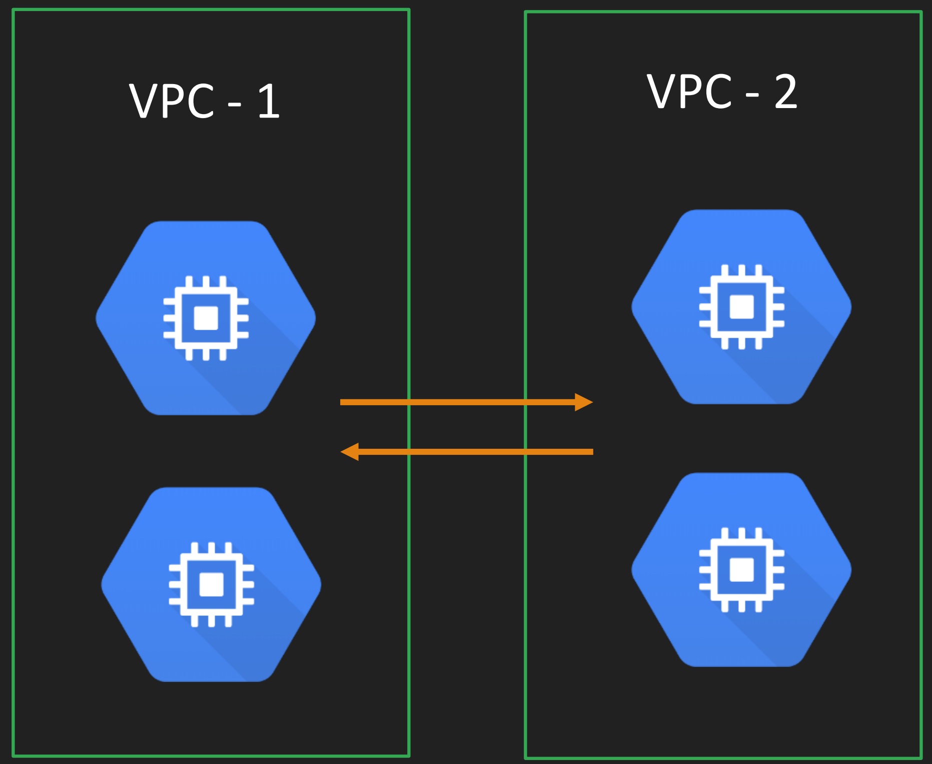
BY ANKIT MISTRY

[Hands-on] Shared VPC Demo

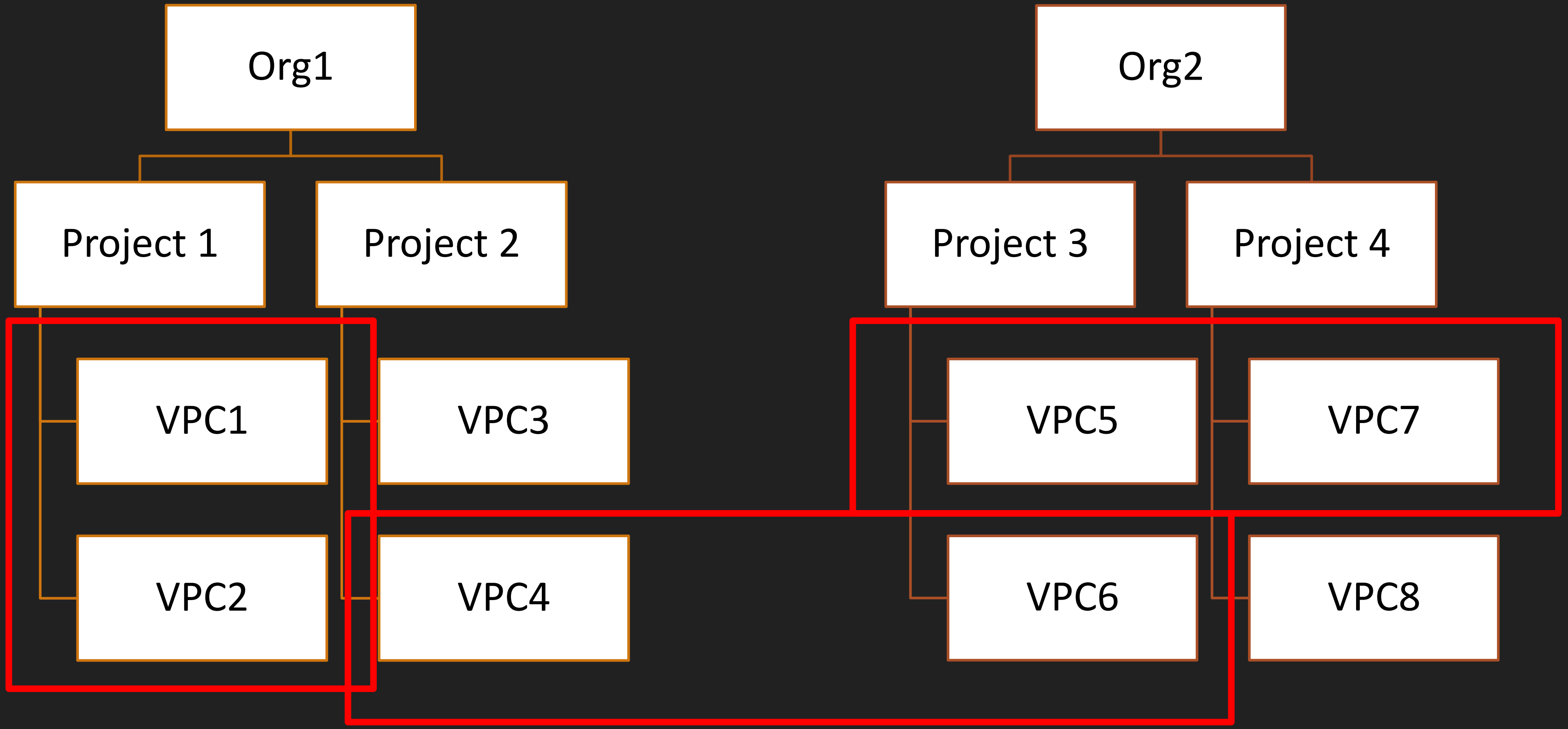
- HostProject
  - my-vpc
- ServiceP1
- ServiceP2
- Share my-vpc from HostProject to Service Project

VPC peering

- No central management
- VPC Managed by individual project team & control all ingress egress traffic
- Use case
  - Project 1 (Ecommerce App) wants to communicate to Project 2 (ML Services App) for Some services like Sentiment Analysis



VPC peering

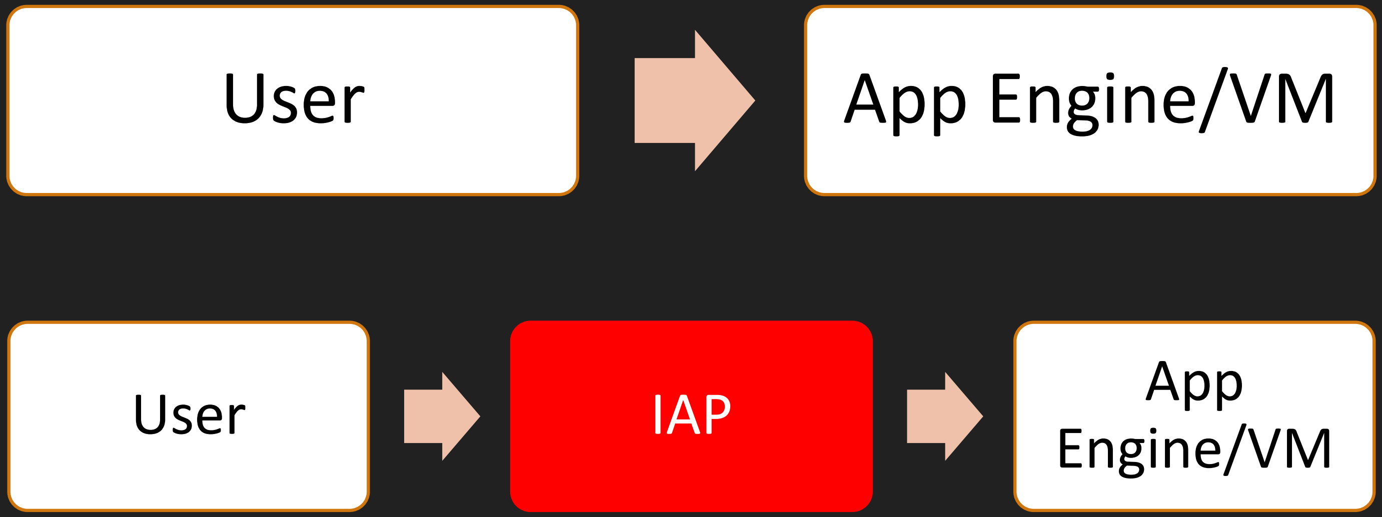

Org1
Project 1
Project 2
VPC1
VPC2
VPC3
VPC4
Org2
Project 3
Project 4
VPC5
VPC6
VPC7
VPC8

[Hands-on] VPC Peering

- Org
  - Project1
    - VM1
  - Project2
    - VM2
- Test Connectivity from VM1 to VM2
- create peering
- Test Connectivity from VM1 to VM2

IAP

- IAP - Identity aware proxy
- With IAP you can guard access to your applications and VMs.
- IAP can protect access to applications hosted on Google Cloud, other clouds, and on-premises.

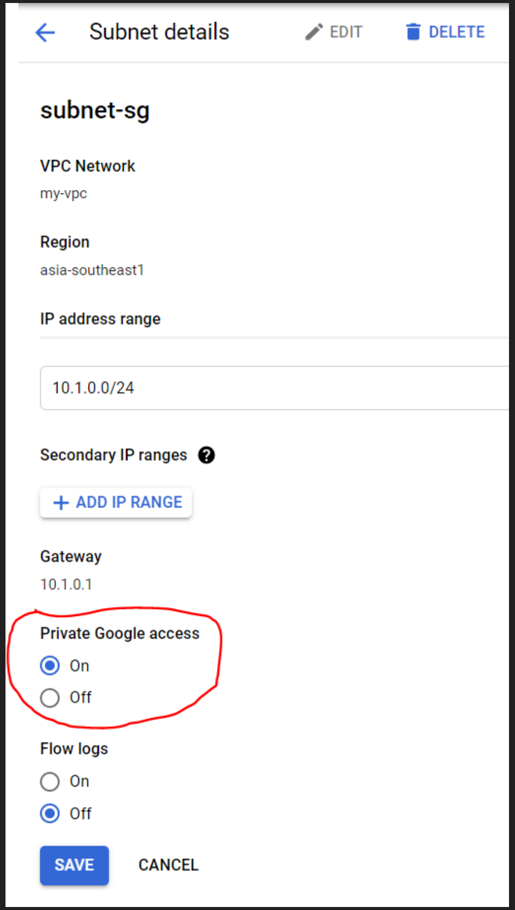


IAP - Demo

1. Secure App Engine Application – HTTP based
    1. Consent screen configuration
    2. Assign IAP web user role
2. Securely connect VM with Internal IP Address
    1. With External IP address
    2. Without external IP address – with tunneling

Google API Private Access

- Private access allow different subnetwork to use GCP services privately
- No external IP Address require
- Call Google APIs & Services with internal IP address
  - YouTube API, Cloud Storage etc…



Subnet details

subnet-sg

VPC Network
my-vpc

Region
asia-southeast1

IP address range
10.1.0.0/24

Secondary IP ranges ?

Gateway
10.1.0.1

Private Google access
● On
○ Off

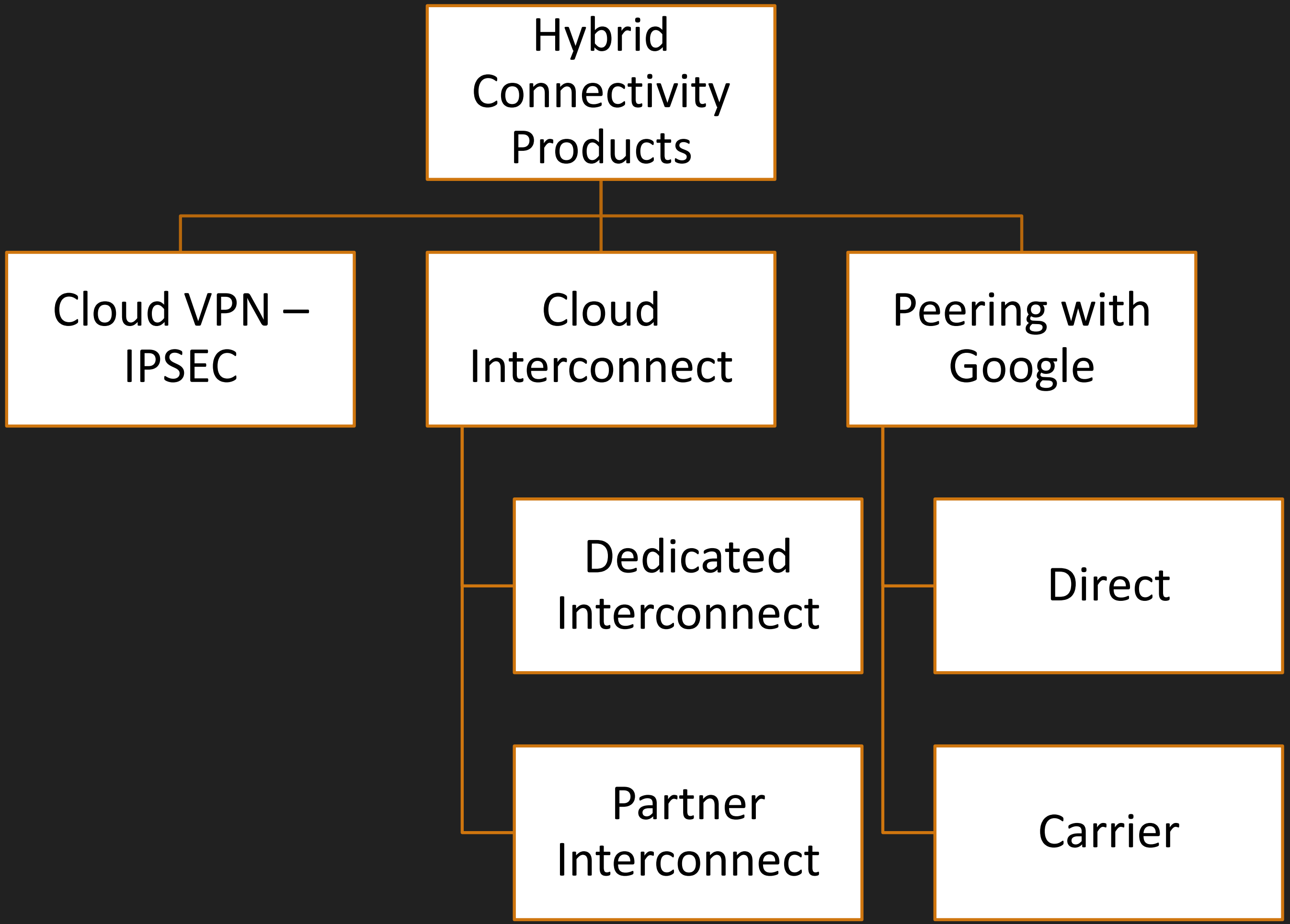
Flow logs
○ On
● Off

Private Access - Demo

1. Create VM with Default
2. Test connectivity with different APIs
3. Remove external IP
4. Step - 2
5. Make Private Google Access – On
6. Step - 2

GCP Hybrid Connectivity

- Connect your datacenter network with GCP network



Hybrid Connectivity Products

Cloud VPN – IPSEC

Cloud Interconnect

Peering with Google

Dedicated Interconnect

Partner Interconnect

Direct

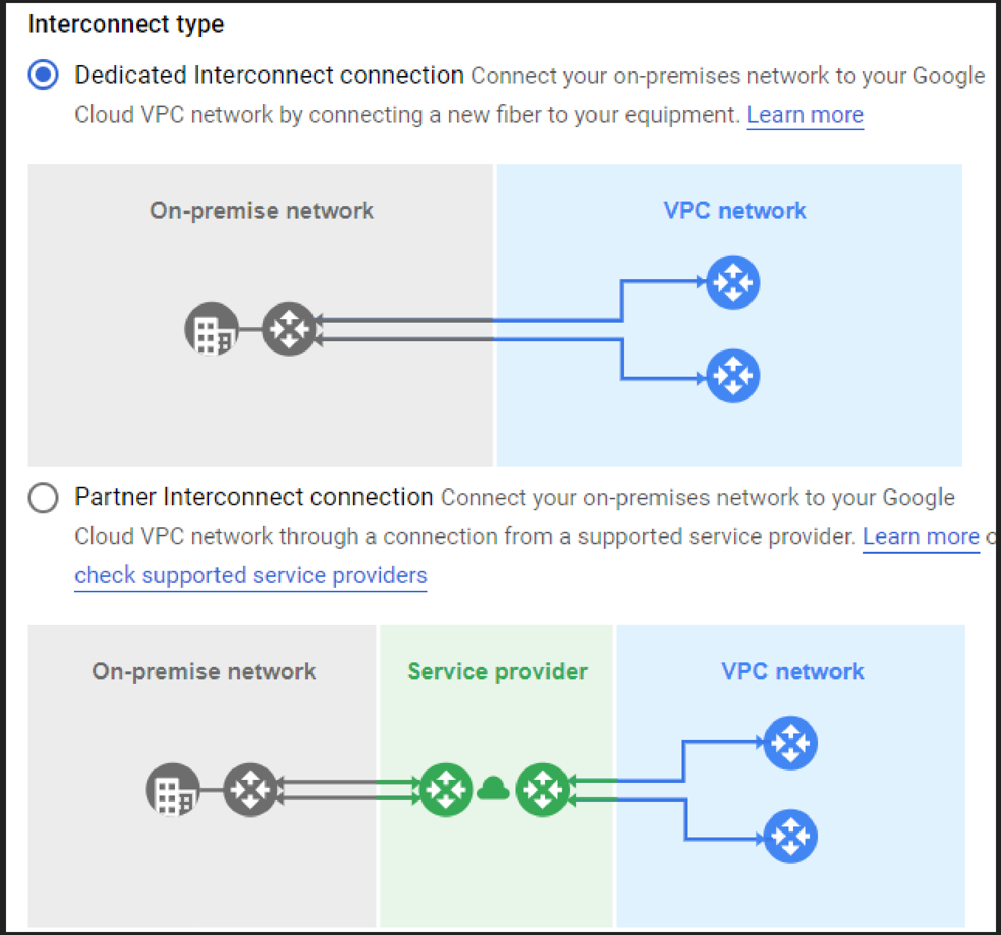
Carrier

Cloud VPN

- A virtual private network lets you securely connect your Google Compute Engine resources to your own private network.
- Cloud VPN securely connects your peer network to your Virtual Private Cloud (VPC) network through an **IPsec VPN**
- It works between
  - Google cloud & datacenter
  - Google cloud & other public cloud (AWS)
- If you want to **quickly** setup connectivity, Cloud VPN is good choice.
- Traffic is **encrypted** by one VPN gateway and then decrypted by the other VPN gateway.
- Traffic travelled over **public** internet
- Cloud VPN tunnel can support up to **3 Gbps**

Cloud Interconnect

- Extend your on premises VPC to GCP network
- highly available, low latency connection
- Access resource with Internal IP address only
- Require time for initial setup
- Once setup, it works with very low latency & with Internal IP address
- No encryption while traffic travelled



Interconnect type

● Dedicated Interconnect connection Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. Learn more

○ Partner Interconnect connection Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. Learn more o
check supported service providers

Create Cloud Interconnect Request

BY ANKIT MISTRY

Dedicated vs partner Cloud Interconnect

Dedicated Interconnect	Partner Interconnect
No Encryption	No Encryption
SLA : Your Datacenter & Google VPC	SLA : Your Datacenter & Google VPC
Pricing is high	Pricing is lower than dedicated
Bandwidth : 10 Gbps to 200 Gbps	Bandwidth : 50 Mbps to 10 Gbps
No Service Provider require	Service Provider require
Internal IP communication	Internal IP communication

DNSSEC

- DNS – Domain name system
- Phonebook of internet
  - google.com -> 172.217.12.142
  - msn.com -> 13.82.28.61
- DNS helps to travel packet from source to destination
- Packet is unencrypted, so can be hacked easily
- Need some layer of extra security on top of DNS
- Domain Name System Security Extensions- DNSSEC

3.Ensuring data protection

BY ANKIT MISTRY

Module 3

- Data loss prevention API
- Data Encryption – Cloud KMS

Data Loss Prevention API

BY ANKIT MISTRY

Data Loss Prevention API

- Fully managed service designed to help you discover, classify, and protect your most sensitive data.
- PII data
  - Person’s name, Credit Card Number, SSN
- Apply API on Cloud Storage, Big Query Data
- DLP work upon Free form Text, Structured & Unstructured data (image)
- What to do with this Data
  - Identify sensitive data
  - De-identify data
    - Masking and Encryption
  - re-identify (In case want to recover original data)

De-Identification of Data

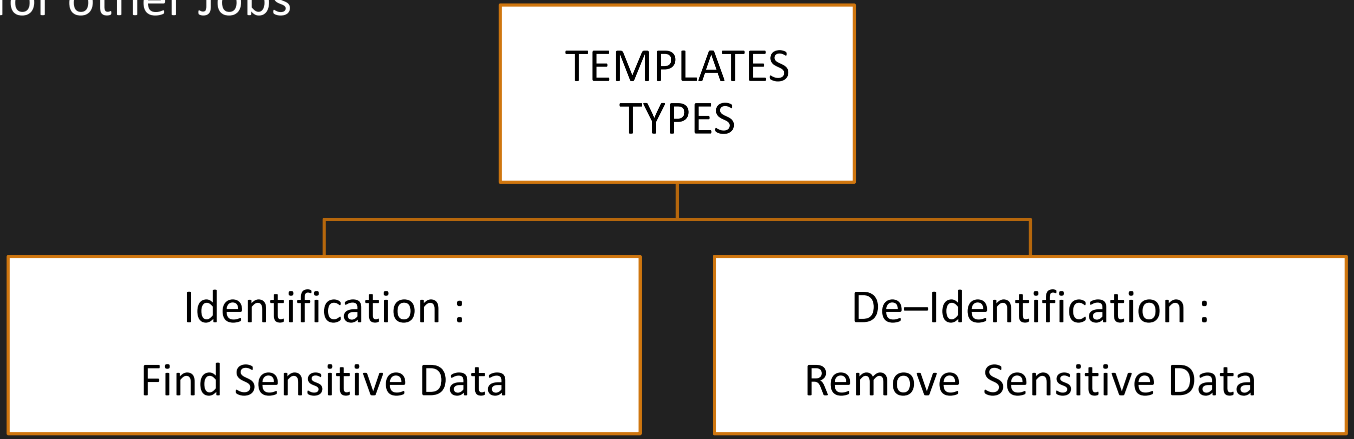
- Redacation – remove sensitive data
- Replacement – replace with some tokens (Like Info_type)
- Masking – Replace one/more character with some other char
- Encryption – Encrypt Sensitive Data

TEMPLETES, INFOTYPES & MATCH LIKELIHOOD

BY ANKIT MISTRY

TEMPLATES

- Configuration which define for
  - Inspection of Jobs
  - De-identification of Jobs
- Once Template defined , can be reused for other Jobs



TEMPLATES TYPES

Identification :

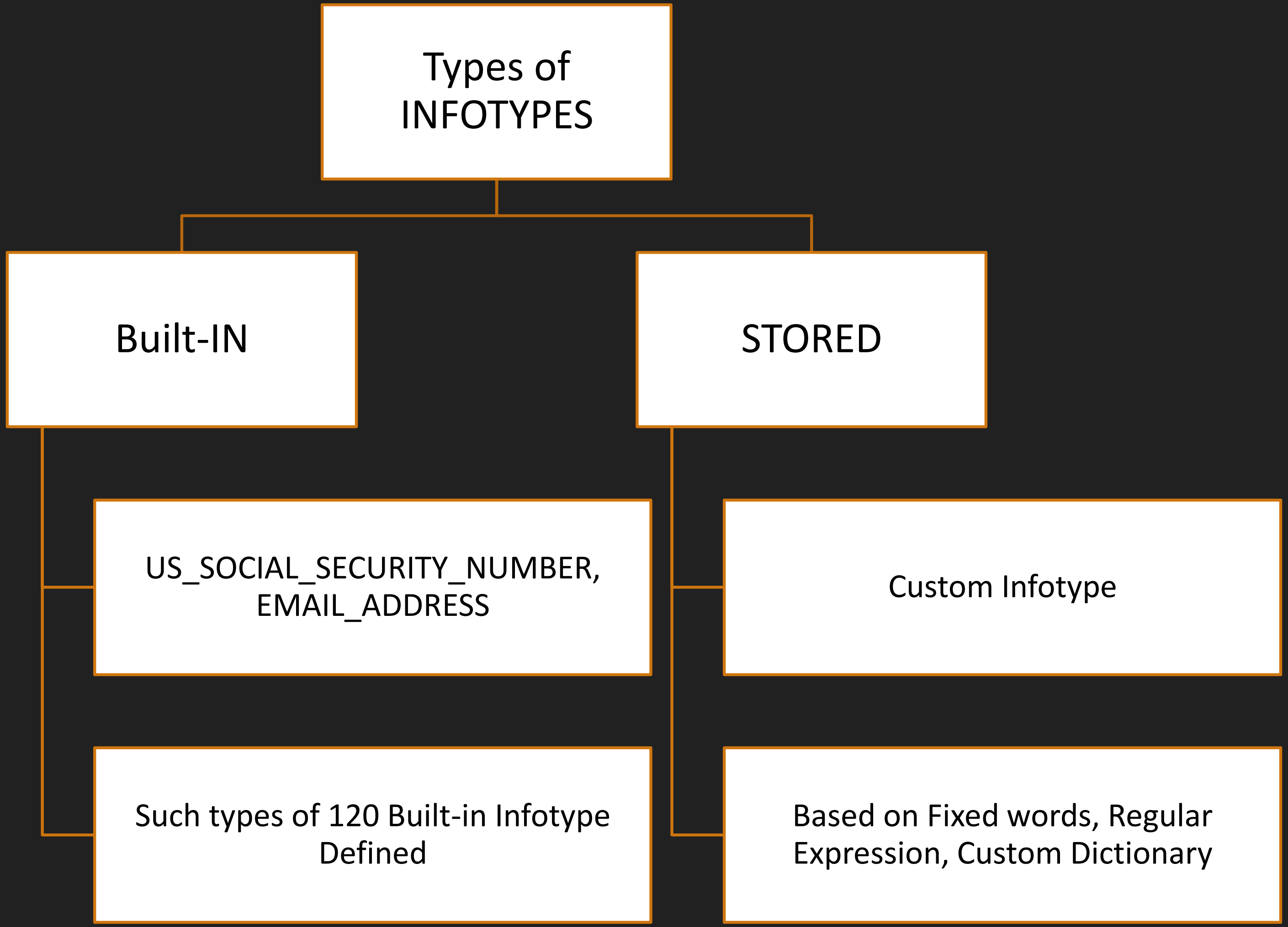
Find Sensitive Data

De–Identification :

Remove Sensitive Data

INFOTYPES

- What to Scan For
  - Like Credit Card
  - SSN
  - Age



Types of INFOTYPES

Built-IN

US_SOCIAL_SECURITY_NUMBER, EMAIL_ADDRESS

Such types of 120 Built-in Infotype Defined

STORED

Custom Infotype

Based on Fixed words, Regular Expression, Custom Dictionary

MATCH LIKELIHOOD

LIKELIHOOD_UNSPECIFIED	Default value; same as POSSIBLE.
VERY_UNLIKELY	It is very unlikely that the data matches the given InfoType.
UNLIKELY	It is unlikely that the data matches the given InfoType.
POSSIBLE	It is possible that the data matches the given InfoType.
LIKELY	It is likely that the data matches the given InfoType.
VERY_LIKELY	It is very likely that the data matches the given InfoType.

DLP API Demo

https://cloud.google.com/dlp/demo/#!/

BY ANKIT MISTRY

Create INFO_TYPE

(Hands-on)

BY ANKIT MISTRY

Create TEMPLETES (Hands-on)

BY ANKIT MISTRY

Create Job for Inspection (Hands-on)

BY ANKIT MISTRY

Create Template for De-identification

BY ANKIT MISTRY

Apply Some more rules to template

BY ANKIT MISTRY

Managing Encryption

BY ANKIT MISTRY

Data Encryption

- What is encryption
- When You should encrypt data – 3 Data States
- Cloud KMS
- Envelope Encryption
- Cloud Storage Encryption Options

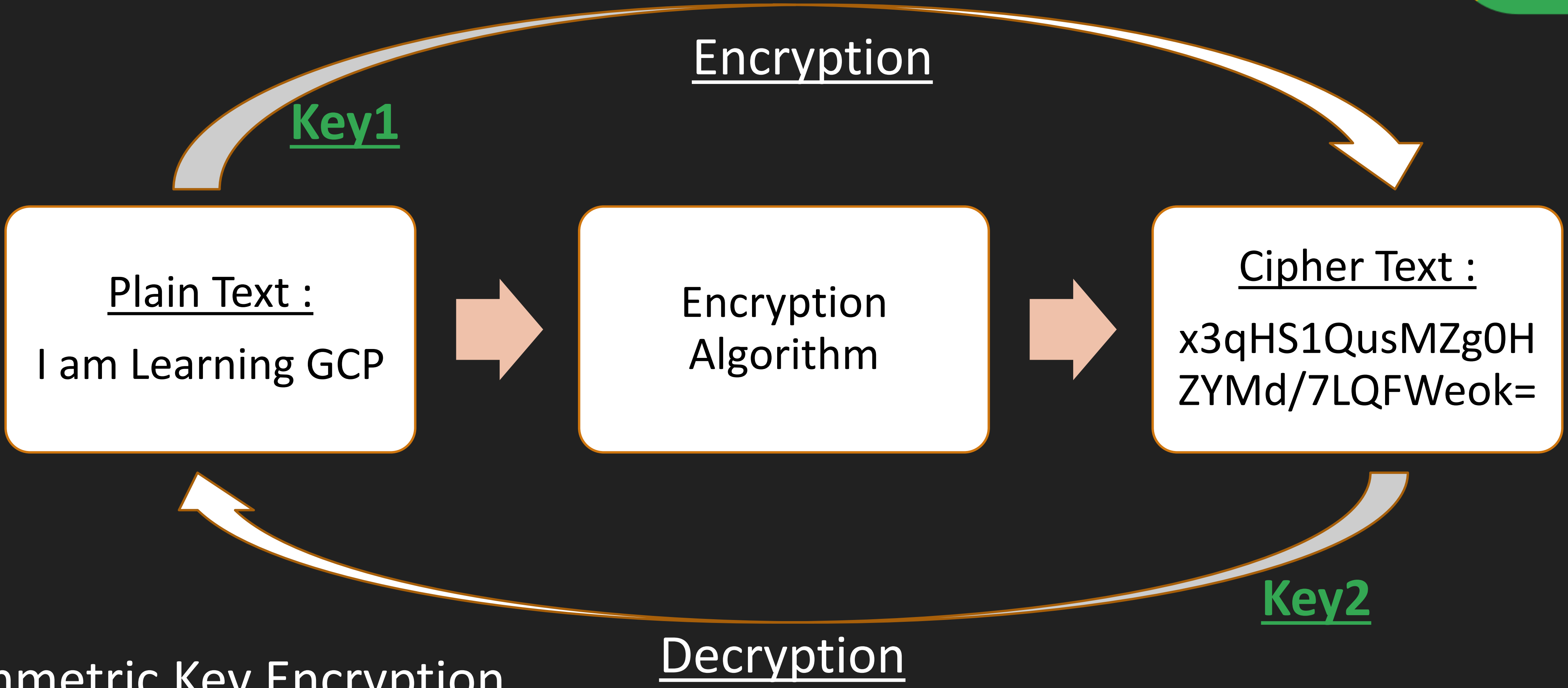
Encryption

BY ANKIT MISTRY

Why Encryption

- In GCP, Data stored at
  - GCS
  - Persistent Disk, SSD
  - File Server
  - Database File
- If Let’s say hacker get access to your hard Disk?

Encryption



Symmetric Key Encryption

Asymmetric Key Encryption

When Encryption

- Data at Rest
  - Data Situated at GCS, Database
- Data in Motion
  - Data transfer from one network to another
  - Within GCP or Outside of GCP
- Data in Use
  - Data situated in RAM.
  - Memory Store, In memory Data Processing

Cloud KMS

BY ANKIT MISTRY

What are the things need to encrypt

- What are the things need to encrypt
  - Data
  - Keys
    - Envelope Encryption
- Client Side
  - Encryption that occurs before data is sent to Cloud Storage - GCP.
- Server Side
  - Encryption that occurs after Google Cloud receives your data

Cloud KMS

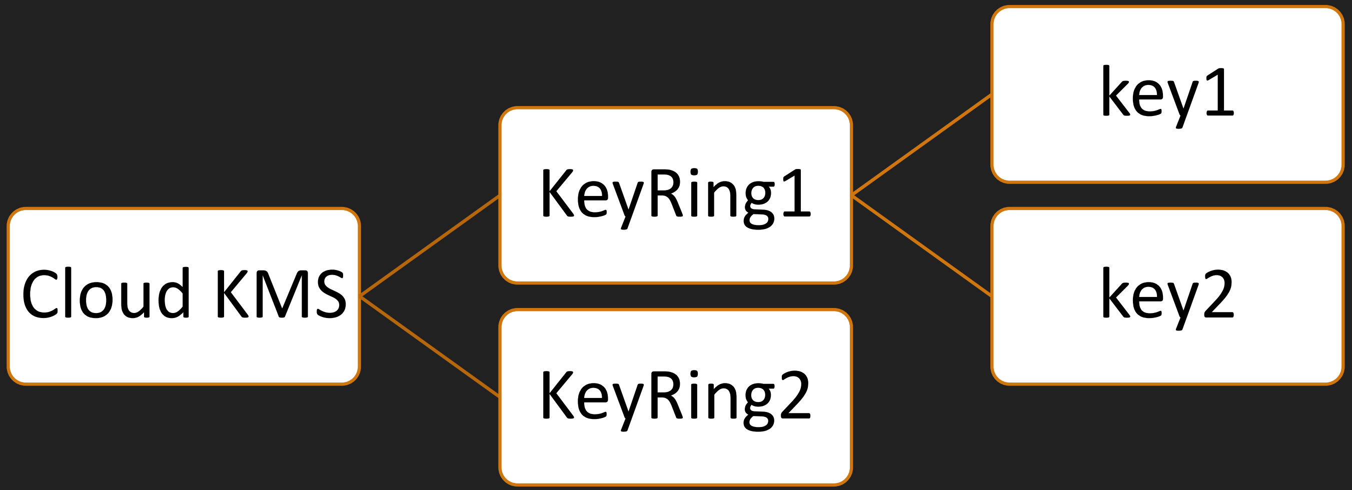
- Manage encryption keys on Google Cloud.
- 3 ways of managing keys
  - Google-managed encryption keys
  - Customer-managed encryption keys
  - Customer-supplied encryption keys

Google-managed encryption keys

- By Default Encryption
- Server side encryption – before data written to disk
- No Additional Configuration required
- Encrypt data using AES-256
- Google manage rotation policy

Customer-managed encryption keys

- Keys generated by Google Cloud KMS
- Customer has control over
  - Rotation policy
  - HSM/Software based keys



Customer-supplied encryption keys

- Complete control over encryption keys
- If keys lost, data can not be recovered
- To generate keys,
  - openssl rand -base64 32
- Can not create bucket from Cloud console
- gsutil -o 'GSUtil:encryption_key='**keys**

Object Lifecycle policy for cloud storage object

- You can create object lifecycle rule
- To create rule Define :
  - Action & Condition
- If condition met, Action will be executed
- Let’s see in Action

Application Secrets

- While building Application we need to store
  - Database password, Some API Keys
- It’s not good idea to store in code or some config file
- Solution : Secret manager
- Dynamically grab secret inside code from secret manager
- Let’s see in action

Get App Secret inside Cloud Function

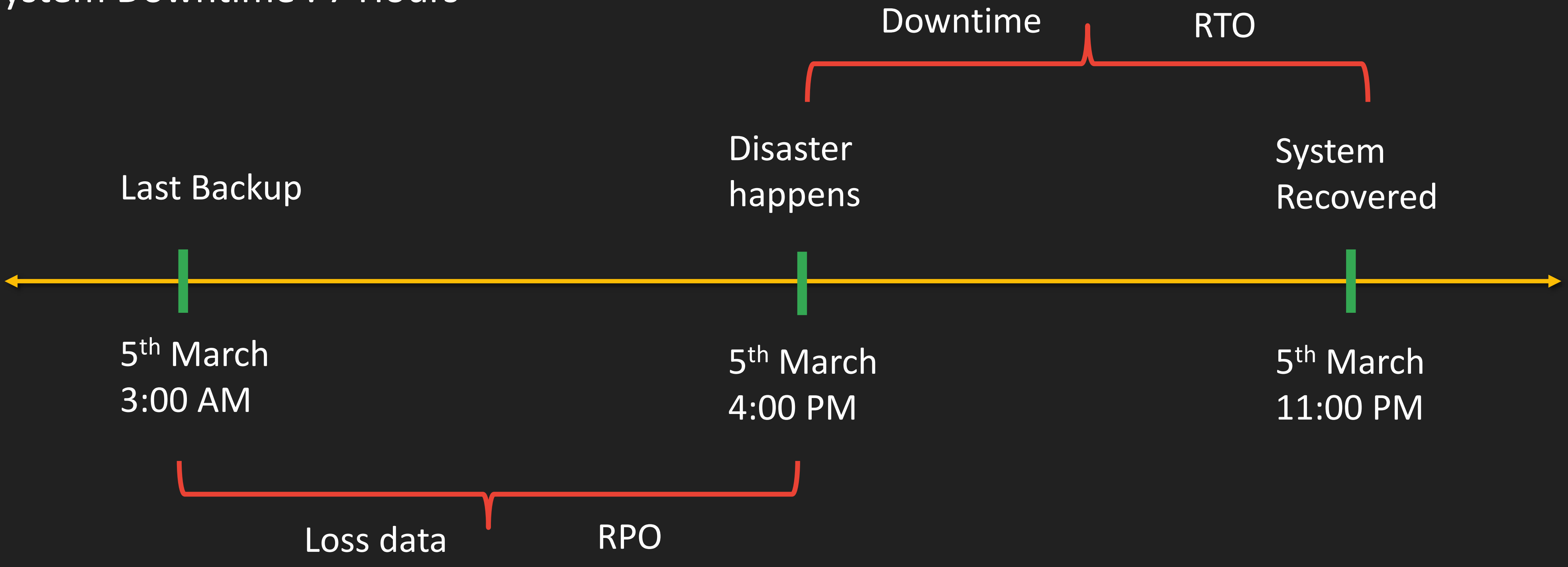
BY ANKIT MISTRY

4-5. Managing operations within a cloud solution environment, Ensuring compliance

BY ANKIT MISTRY

RTO & RPO

- Data loss : 13 hours
- System Downtime : 7 Hours



Downtime RTO

Last Backup

5th March
3:00 AM

Disaster
happens

5th March
4:00 PM

System
Recovered

5th March
11:00 PM

Loss data RPO

RTO & RPO

- RTO – Recovery Time objective
  - Maximum time for which system can be down
- RPO - Recovery Point objective
  - Maximum time for which organization can tolerate Dataloss

Data backup

- Copying a discrete amount of data from one place to another
- Data backups have a small to medium RTO and a small RPO
- Your can be at
  - On-premise
  - Google Cloud
  - Other Public Cloud
- Services :
  - SQL instances
  - Cloud Storage – blob file
  - Cloud native Services

Data at On-Premises

- Cloud Storage

  -
    ```
    gsutil -m cp -r [SOURCE_DIRECTORY] gs://[BUCKET_NAME]
    ```

  -
    ```
    gsutil -m rsync -r [SOURCE_DIRECTORY] gs://[BUCKET_NAME]
    ```
- Cloud Interconnect
- Transfer Services
- Transfer Appliance

Data at Public Cloud

- Storage Transfer Service
- Support for Amazon S3, Azure Storage to Google Cloud Storage
- Let’s See in Action

Data at GCP

- Different bucket & Region
- Take backup with different Tiered storage
  - NearLine, ColdLine, Archieve
- Persistent Disk/VM backup
  - Take Snapshot
  - Build Custom image

Database Backup

- If your database is at on-premise or Other public cloud
  - For each vendor, method to export data varies
  - Upload to GCS
  - Import data to Database Instance
- Cloud SQL instance – Inside GCP
  - on-demand backup
  - Scheduled backup
- Let’s see in action

Cloud Logging

- Real time Log Management tool
- Fully managed - No server management
- Massive volume of data can be store
- Log can stored, search, analyze
  - Use query to search Logs
- Nice visualization with Log Dashboard
- Ingest log from on-primes also

- Collect Log from App Engine, Cloud Function, GKE
- Install Logging agent to collect log from GCE – VM
- Route Logs to different Destination
  - Cloud Storage, BigQuery, Pubsub etc…
- Is it free?

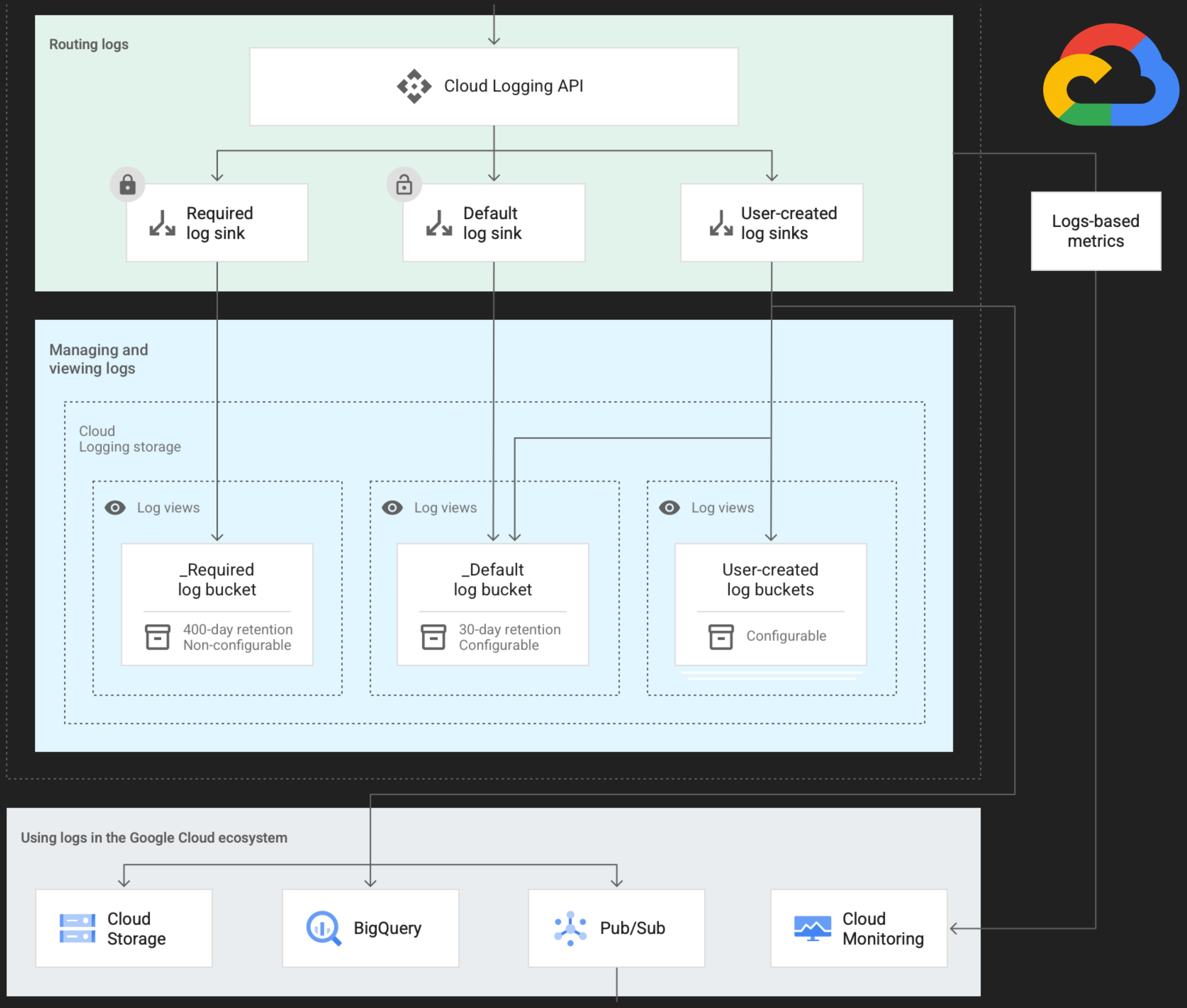
Types of Logs

Admin activity Logs	System Event Logs	Data Access Logs	Policy Denied Logs
By Default Enabled	By Default Enabled	By Default **Not** Enabled	By Default Enabled
400 days	400 days	30 days	30 days
Free	Free	**Not** Free	**Not** Free
Create VM, Delete VM	VM Migration, Auto Restart	Create Object in Bucket	Security violation

Explore Cloud Logging

BY ANKIT MISTRY

Cloud Log Router-Sinks



Container scanning API

- Container images can have vulnerabilities
- Scanning vulnerabilities inside container
- Enable Container scanning API
- It works with
  - Container Registry
  - Artifact Registry

Binary Authorization

- Policy
  - Ensures that trusted images are deployed to GCP
- Enable Binary Authorization
- Works with
  - GKE
  - Cloud Run
- Let's see in action

Forseti Security

- 3 Resources inside GCP
- Easy to monitor few resources manually
- 1000’s of VM need to monitor
- Forseti Security is a collection of community-driven, open-source tools to help you improve the security of your Google Cloud Platform (GCP) environments.
- systematically monitor your GCP resources to ensure that access controls are set as you intended

How Forseti Security Works

- Inventory
- Scanner
- Enforcer
- Explain
- Notification
- https://forsetisecurity.org/docs/latest/concepts/architecture.html

How Forseti Security Works

A. Inventory collects information about your GCP resources and G Suite.

B. Inventory stores information in Cloud SQL for your review and use by other Forseti modules.

C. Scanner compares the data collected by Inventory to the policy rules you set.

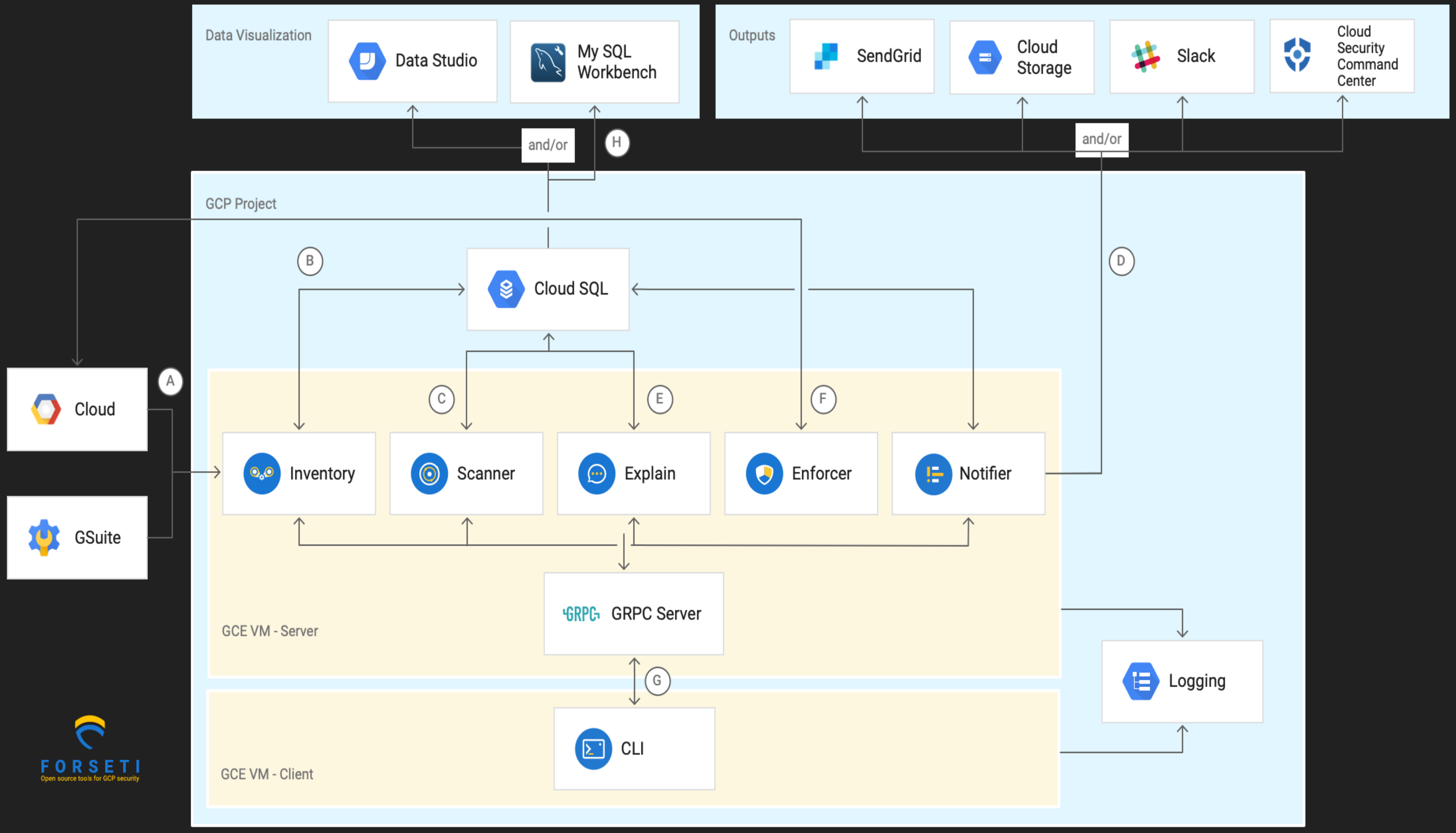
D. Notifier sends Scanner & Inventory results to one or more of the following channels you configure: Cloud Storage, SendGrid, Slack and Cloud Security Command Center.

E. You use Explain to query and understand your Cloud IAM policies.

F. Enforcer uses Google Cloud APIs to make sure policies match your desired state.

G. You use the command-line interface to query Forseti data using gRPC.

H. You use Data Studio or MySQL Workbench to visualize the Forseti data stored in Cloud SQL.



Web Security Scanner

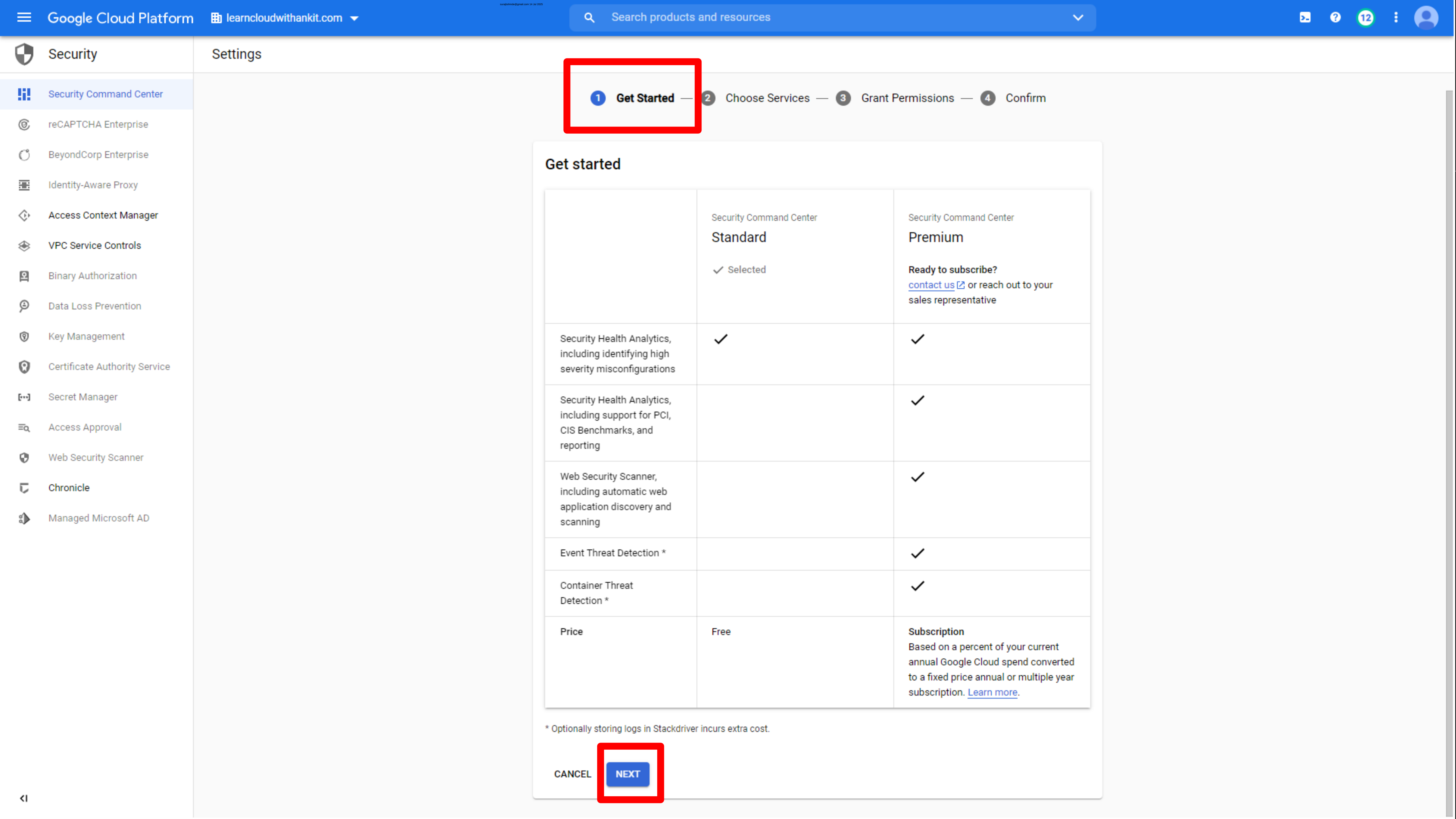
- Identify vulnerabilities in Web Application (App Engine, Compute engine, GKE) by running security tests.
  - Scan Types :Cross-site scripting (XSS)
  - CLEAR_TEXT_PASSWORD
  - INVALID_HEADER
  - MIXED_CONTENT
  - OUTDATED_LIBRARY
  - Complete List : https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview
- Web Security Scanner only supports public URLs and IPs

Security Command Center

- Centralized place to see security of GCP via Dashboard
- It has number of services to analyze security
- It has two Tiers :
  - Standard tier
  - Premium tier
  - https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview

Configure Security Command Center

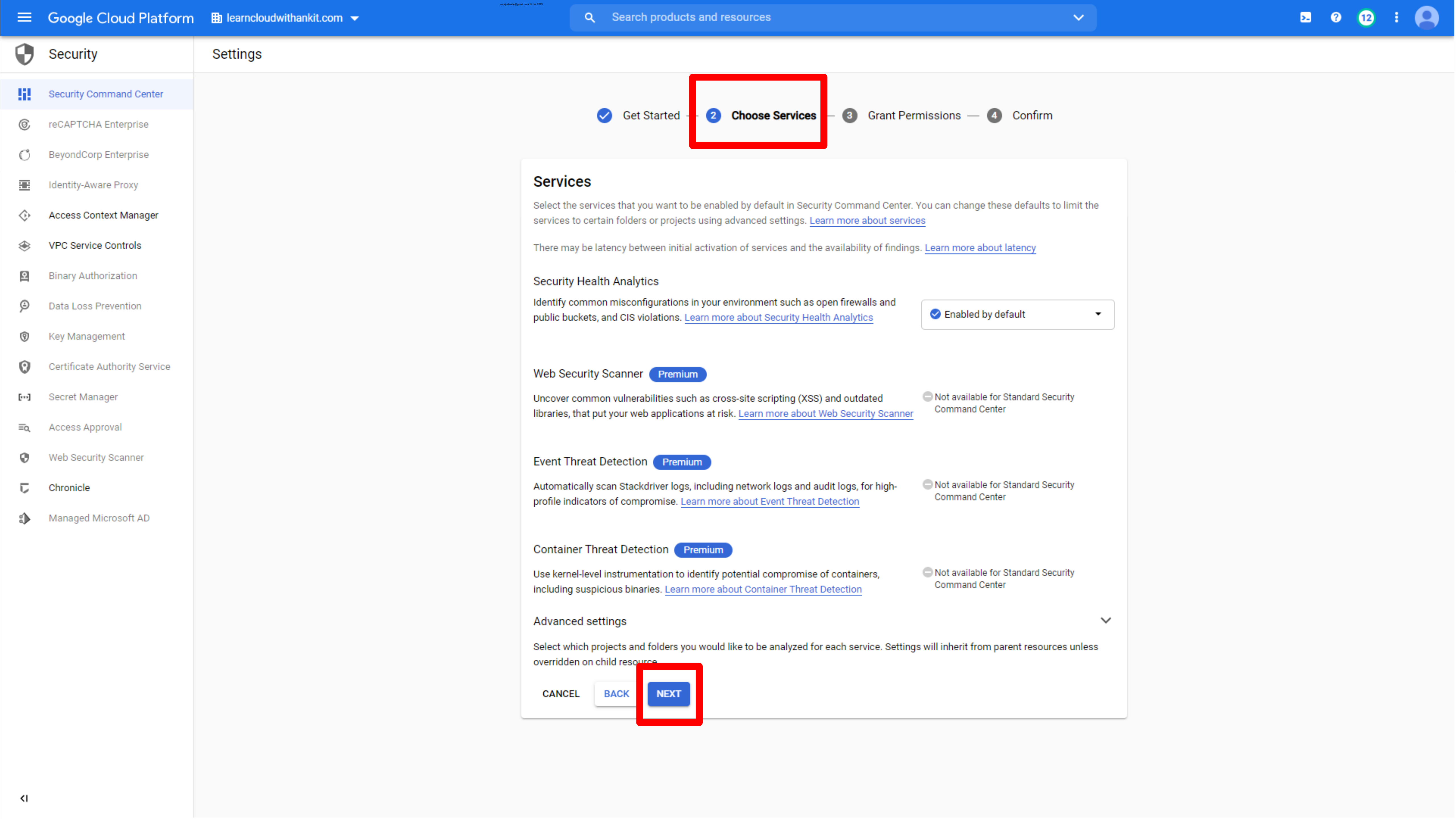
BY ANKIT MISTRY



Get started

	Security Command Center Standard ✓ Selected	Security Command Center Premium **Ready to subscribe?** contact us or reach out to your sales representative
Security Health Analytics, including identifying high severity misconfigurations	✓	✓
Security Health Analytics, including support for PCI, CIS Benchmarks, and reporting		✓
Web Security Scanner, including automatic web application discovery and scanning		✓
Event Threat Detection *		✓
Container Threat Detection *		✓
Price	Free	**Subscription** Based on a percent of your current annual Google Cloud spend converted to a fixed price annual or multiple year subscription. Learn more.

* Optionally storing logs in Stackdriver incurs extra cost.



Services

Select the services that you want to be enabled by default in Security Command Center. You can change these defaults to limit the services to certain folders or projects using advanced settings. Learn more about services

There may be latency between initial activation of services and the availability of findings. Learn more about latency

Security Health Analytics

Identify common misconfigurations in your environment such as open firewalls and public buckets, and CIS violations. Learn more about Security Health Analytics

✓ Enabled by default

Web Security Scanner Premium

Uncover common vulnerabilities such as cross-site scripting (XSS) and outdated libraries, that put your web applications at risk. Learn more about Web Security Scanner

Not available for Standard Security Command Center

Event Threat Detection Premium

Automatically scan Stackdriver logs, including network logs and audit logs, for high-profile indicators of compromise. Learn more about Event Threat Detection

Not available for Standard Security Command Center

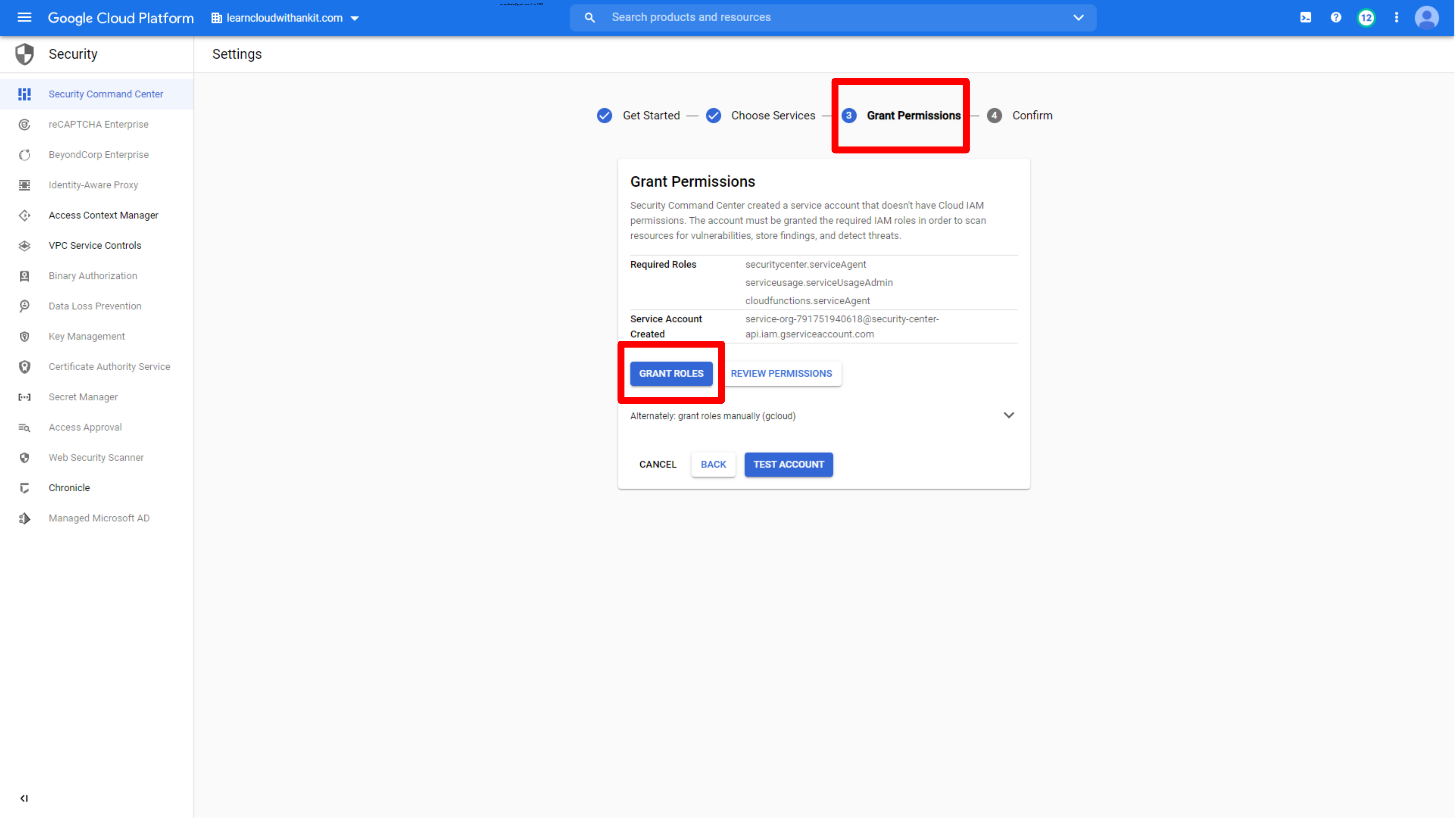
Container Threat Detection Premium

Use kernel-level instrumentation to identify potential compromise of containers, including suspicious binaries. Learn more about Container Threat Detection

Not available for Standard Security Command Center

Advanced settings

Select which projects and folders you would like to be analyzed for each service. Settings will inherit from parent resources unless overridden on child resource.

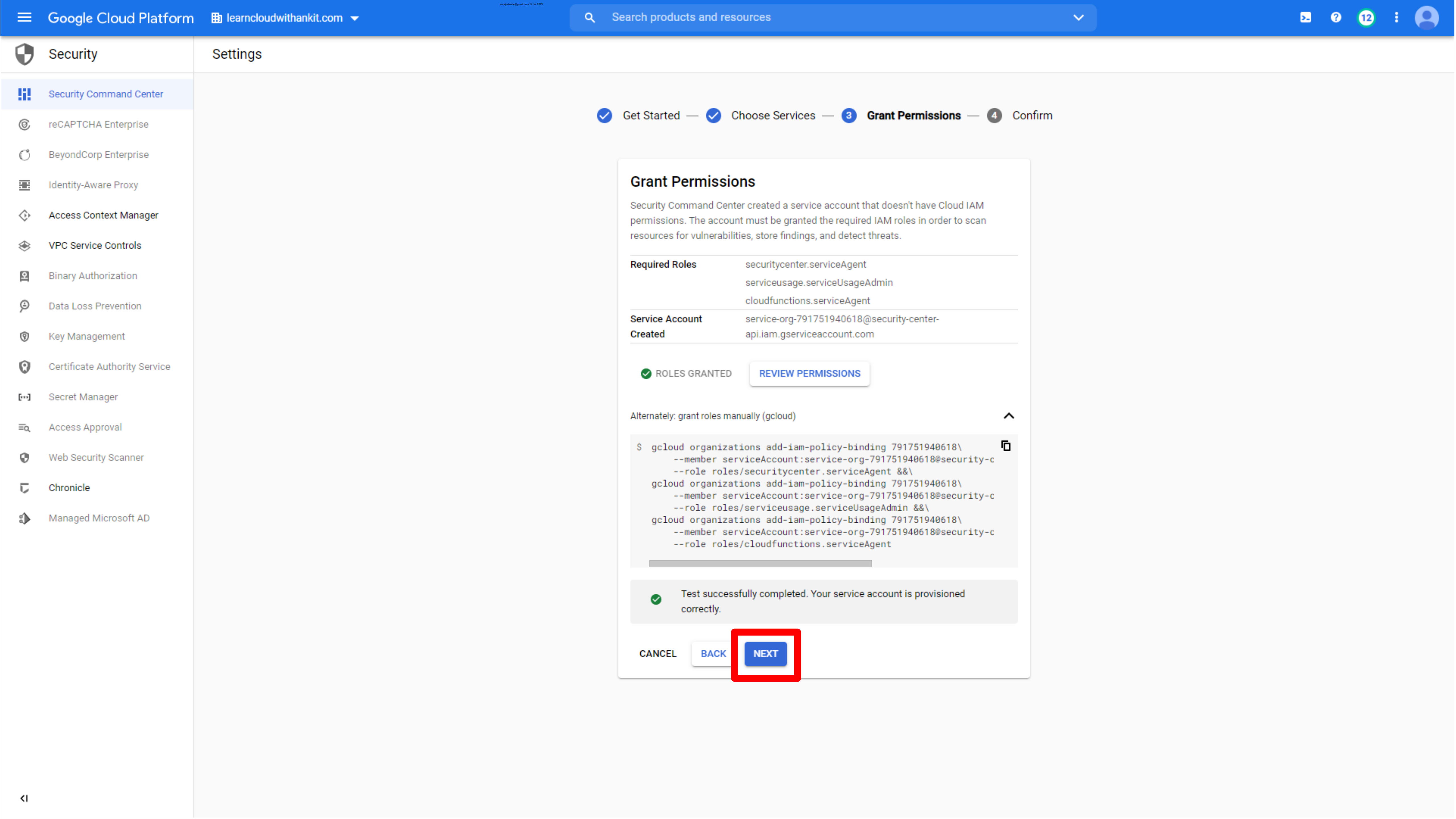


Grant Permissions

Security Command Center created a service account that doesn't have Cloud IAM permissions. The account must be granted the required IAM roles in order to scan resources for vulnerabilities, store findings, and detect threats.

Required Roles	securitycenter.serviceAgent serviceusage.serviceUsageAdmin cloudfunctions.serviceAgent
Service Account Created	service-org-791751940618@security-center-api.iam.gserviceaccount.com

Alternately: grant roles manually (gcloud)



Grant Permissions

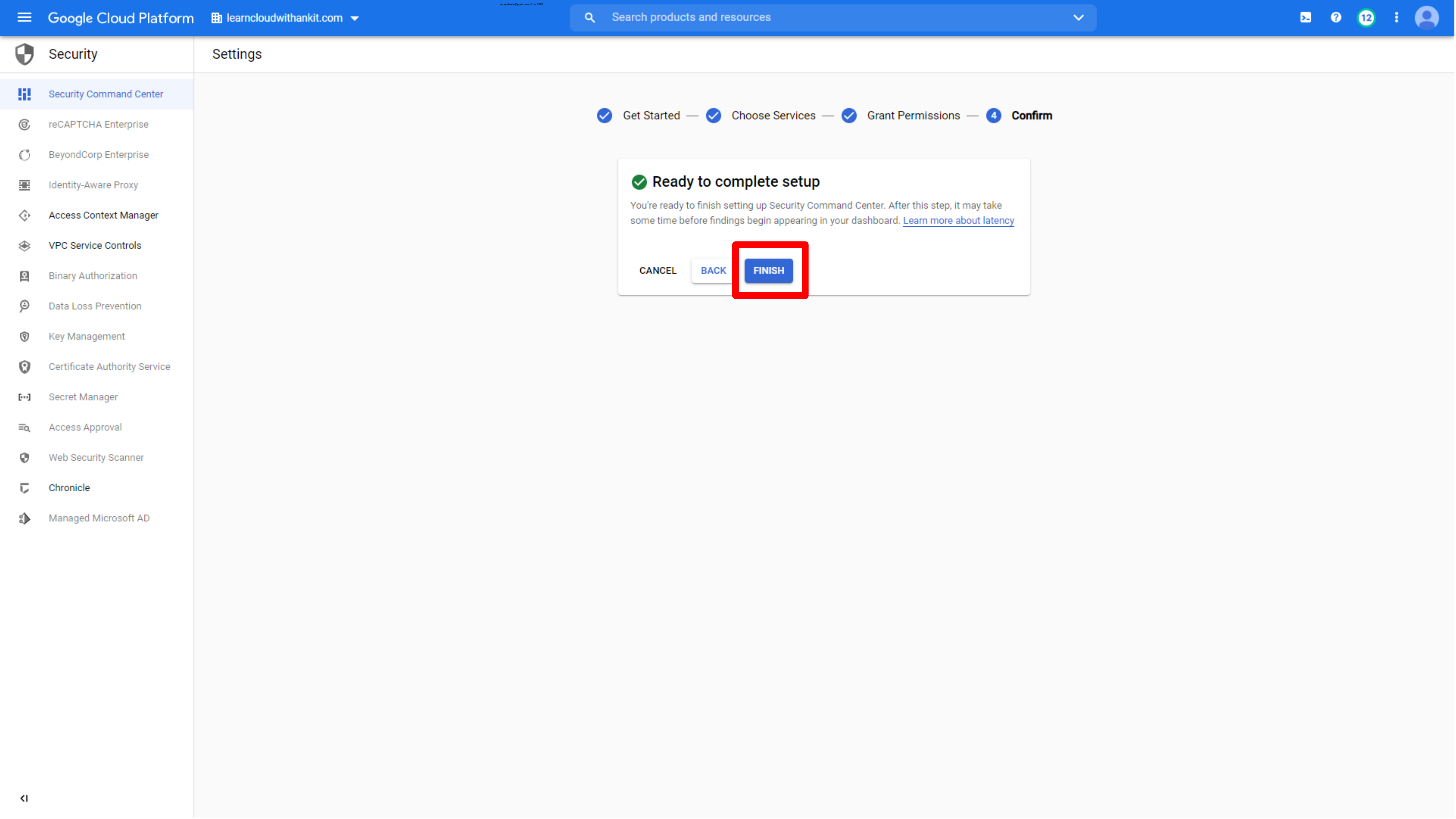
Security Command Center created a service account that doesn't have Cloud IAM permissions. The account must be granted the required IAM roles in order to scan resources for vulnerabilities, store findings, and detect threats.

Required Roles	securitycenter.serviceAgent serviceusage.serviceUsageAdmin cloudfunctions.serviceAgent
Service Account Created	service-org-791751940618@security-center-api.iam.gserviceaccount.com

Alternately: grant roles manually (gcloud)

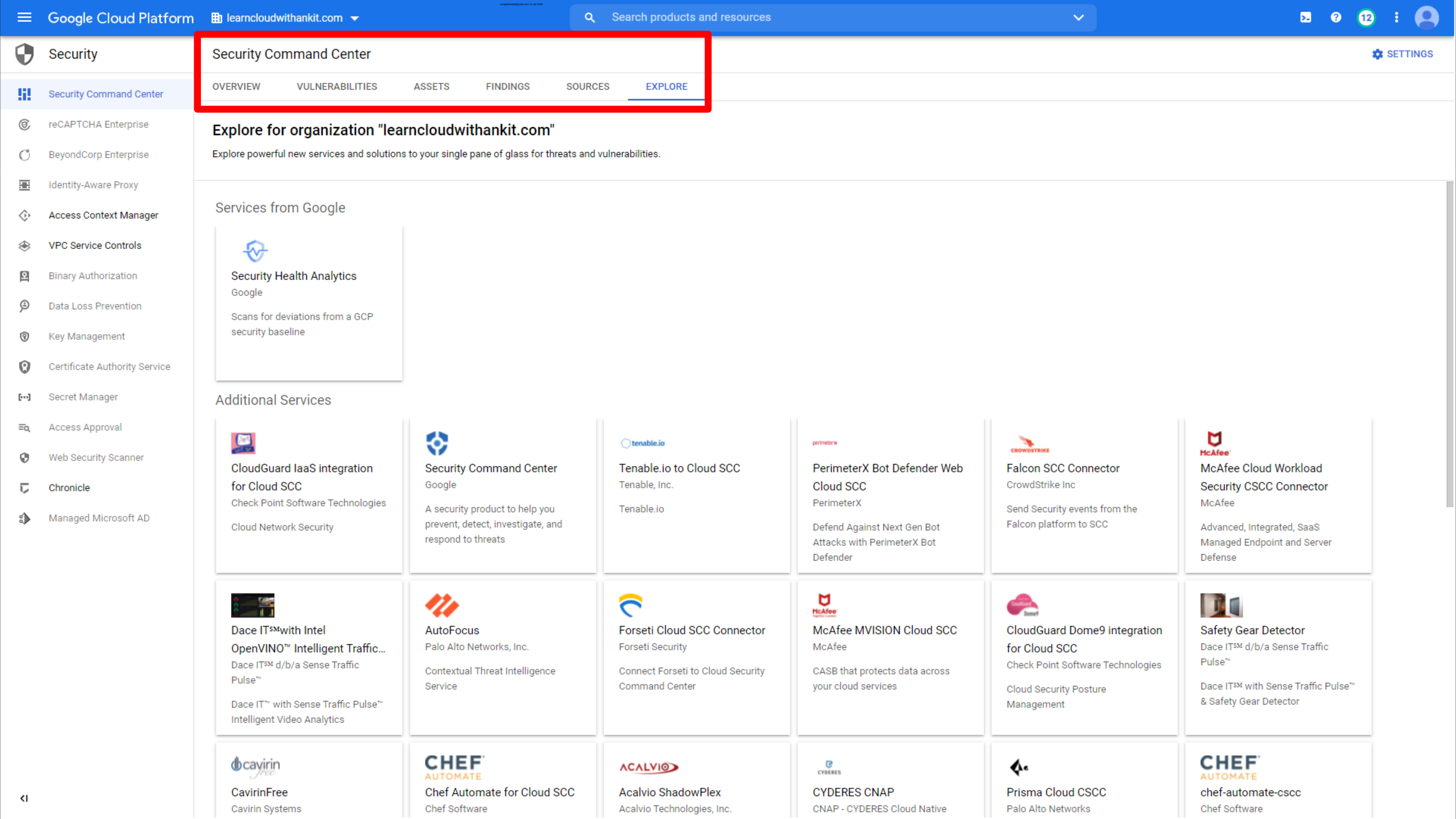
```
$ gcloud organizations add-iam-policy-binding 791751940618\
      --member serviceAccount:service-org-791751940618@security-c
      --role roles/securitycenter.serviceAgent &&\
  gcloud organizations add-iam-policy-binding 791751940618\
      --member serviceAccount:service-org-791751940618@security-c
      --role roles/serviceusage.serviceUsageAdmin &&\
  gcloud organizations add-iam-policy-binding 791751940618\
      --member serviceAccount:service-org-791751940618@security-c
      --role roles/cloudfunctions.serviceAgent
```

Test successfully completed. Your service account is provisioned correctly.



Ready to complete setup

You're ready to finish setting up Security Command Center. After this step, it may take some time before findings begin appearing in your dashboard. Learn more about latency



Explore for organization "learncloudwithankit.com"

Explore powerful new services and solutions to your single pane of glass for threats and vulnerabilities.

Services from Google

Security Health Analytics
Google
Scans for deviations from a GCP security baseline

Additional Services

CloudGuard IaaS integration for Cloud SCC
Check Point Software Technologies
Cloud Network Security

Security Command Center
Google
A security product to help you prevent, detect, investigate, and respond to threats

Tenable.io to Cloud SCC
Tenable, Inc.
Tenable.io

PerimeterX Bot Defender Web Cloud SCC
PerimeterX
Defend Against Next Gen Bot Attacks with PerimeterX Bot Defender

Falcon SCC Connector
CrowdStrike Inc
Send Security events from the Falcon platform to SCC

McAfee Cloud Workload Security CSCC Connector
McAfee
Advanced, Integrated, SaaS Managed Endpoint and Server Defense

Dace IT℠ with Intel OpenVINO™ Intelligent Traffic...
Dace IT℠ d/b/a Sense Traffic Pulse™
Dace IT™ with Sense Traffic Pulse™ Intelligent Video Analytics

AutoFocus
Palo Alto Networks, Inc.
Contextual Threat Intelligence Service

Forseti Cloud SCC Connector
Forseti Security
Connect Forseti to Cloud Security Command Center

McAfee MVISION Cloud SCC
McAfee
CASB that protects data across your cloud services

CloudGuard Dome9 integration for Cloud SCC
Check Point Software Technologies
Cloud Security Posture Management

Safety Gear Detector
Dace IT℠ d/b/a Sense Traffic Pulse™
Dace IT℠ with Sense Traffic Pulse™ & Safety Gear Detector

CavirinFree
Cavirin Systems

Chef Automate for Cloud SCC
Chef Software

Acalvio ShadowPlex
Acalvio Technologies, Inc.

CYDERES CNAP
CNAP - CYDERES Cloud Native

Prisma Cloud CSCC
Palo Alto Networks

chef-automate-cscc
Chef Software

THANK YOU

Google Cloud Certified
PROFESSIONAL
CLOUD SECURITY ENGINEER