

Visual Report:

This is a document demonstrating how I addressed and remediated vulnerabilities in the Cloud of Cymbal Bank using Google Cloud’s Security Command Center. Screenshots throughout the report showcase each step of the remediation process, providing a visual walkthrough of how I improved the security posture of the environment.

I began the investigation by leveraging Security Command Center’s Risk Overview panel to assess the simulated bank’s current threat exposure. I prioritized findings based on severity and focused on public bucket access, overly insecure firewall rules, and under-protected service accounts. This critical triage step aligns with security best practices in asset risk classification.

Google Cloud

qwiklabs-gcp-01-0b88d757971c

Search (/) for resources, docs, products, and more

Search

5

Security

Risk overview

FEEDBACK

SETTINGS

LEARN

Security Command Ce...

Risk Overview

Threats

Vulnerabilities

Compliance

Assets

Findings

Sources

Posture Management

Detections and Controls

Google SecOps

reCAPTCHA

Model Armor

Web Security Scanner

Cyber Insurance Hub

Binary Authorization

Marketplace

Release Notes

FINDINGS BY CATEGORY

FINDINGS BY RESOURCE TYPE

FINDINGS BY PROJECT

Filter

Resource types

| Resource Type           | Critical Findings | High Severity Findings | Medium Severity Findings | Low Severity Findings | Unspecified Severity Findings |
|-------------------------|-------------------|------------------------|--------------------------|-----------------------|-------------------------------|
| Bucket                  | 0                 | 1                      | 1                        | 1                     | 0                             |
| compute.Instance        | 0                 | 1                      | 3                        | 0                     | 0                             |
| compute.Project         | 0                 | 0                      | 1                        | 0                     | 0                             |
| Firewall                | 0                 | 2                      | 4                        | 0                     | 0                             |
| Network                 | 0                 | 0                      | 2                        | 0                     | 0                             |
| resourcemanager.Project | 0                 | 0                      | 2                        | 9                     | 0                             |
| ServiceAccountKey       | 0                 | 0                      | 1                        | 0                     | 0                             |
| Subnetwork              | 0                 | 0                      | 0                        | 56                    | 0                             |

Identity and access findings

Top severity identity and access findings by category.

| Severity | Finding category                 | Cloud Provider | Total findings |
|----------|----------------------------------|----------------|----------------|
| High     | Public bucket ACL                | Google         | 1              |
| Medium   | Admin service account            | Google         | 1              |
| Medium   | Default service account used     | Google         | 1              |
| Medium   | Primitive roles used             | Google         | 1              |
| Medium   | User managed service account key | Google         | 1              |

AI Workload findings

Review violations to Secure AI policies, drift from intended AI policies, and security issues detected on AI resources

VULNERABILITIES

POLICY DRIFT

| Category | Severity | Resource |
|----------|----------|----------|
|          |          |          |

I reviewed the Compliance tab in Security Command Center to identify all failed control checks across the environment. These included missing VPC Flow Logs, disabled firewall logging, and overly permissive inbound rules.

Google Cloud

qwiklabs-gcp-01-0b88d757971c

Search (/) for resources, docs, products, and more

Search

Security

Compliance detail

SETTINGSLEARN

Security Command Ce...

Risk Overview

Threats

Vulnerabilities

Compliance

Assets

Findings

Sources

Posture Management

Detections and Controls

Google SecOps

reCAPTCHA

Model Armor

Web Security Scanner

Cyber Insurance Hub

Binary Authorization

Marketplace

Release Notes

Filter

Enter property name or value

| Control | Status        | Rule  | Severity | Findings | Resources scanned |
|---------|---------------|---|----------|----------|-------------------|
| 10.1    | Non-compliant |   |          | 33       |                   |
|         | Non-compliant | VPC Flow logs should be Enabled for every subnet in VPC Network   | High     | 28       | 28                |
|         | Non-compliant | Firewall rule logging should be enabled so you can audit network access   | Medium   | 4        | 4                 |
|         | Non-compliant | Cloud Audit Logging should be configured properly across all services and all users from a project                            | High     | 1        | 1                 |
|         | Compliant     | Stackdriver Monitoring should be Enabled on Kubernetes Engine Clusters  | High     | 0        | -                 |
| 10.2    | Non-compliant |   |          | 33       |                   |
|         | Non-compliant | VPC Flow logs should be Enabled for every subnet in VPC Network   | High     | 28       | 28                |
|         | Non-compliant | Firewall rule logging should be enabled so you can audit network access   | Medium   | 4        | 4                 |
|         | Non-compliant | Cloud Audit Logging should be configured properly across all services and all users from a project                            | High     | 1        | 1                 |
|         | Compliant     | Stackdriver Monitoring should be Enabled on Kubernetes Engine Clusters  | High     | 0        | -                 |
| 1.2.1   | Non-compliant |   |          | 2        |                   |
|         | Non-compliant | Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389                                     | High     | 1        | 4                 |
|         | Non-compliant | Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22                                      | High     | 1        | 4                 |
|         | Compliant     | Firewall rules should not allow connections from all IP addresses on TCP ports 7000-7001, 7199, 8888, 9042, 9160, 61620-61621 | High     | 0        | 4                 |
|         | Compliant     | Firewall rules should not allow connections from all IP addresses on  | High     | 0        | 4                 |

I discovered that the cloud storage bucket was publicly accessible, creating a major data exposure risk. Buckets accessible to *allUsers* without restriction pose a high likelihood of sensitive data leaks which violates the principle of least privilege (PoLP).

Google Cloud

qwiklabs-gcp-01-0b88d757971c

Search (/) for resources, docs, products, and more

Search

Cloud Storage

Bucket details

Go to pathRefresh

Overview

Buckets

Monitoring

Settings

Storage Intelligence

Insights datasets

Configuration

Marketplace

Release Notes

qwiklabs-gcp-01-0b88d757971c\_bucket

Public to internet: This bucket is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. Remove these principals to stop public access.

Edit accessDismiss

Location

Storage class

Public access

Protection

us-east1 (South Carolina)

Standard

Public to internet

Soft Delete

Objects

Configuration

Permissions

Protection

Lifecycle

Observability

New

Inventory Reports

Operations

Folder browser

qwiklabs-gcp-01-0b88d757971c\_bucket

Buckets > qwiklabs-gcp-01-0b88d757971c\_bucket

Create folderUploadTransfer dataOther servicesLearn

Filter by name prefix only

Filter

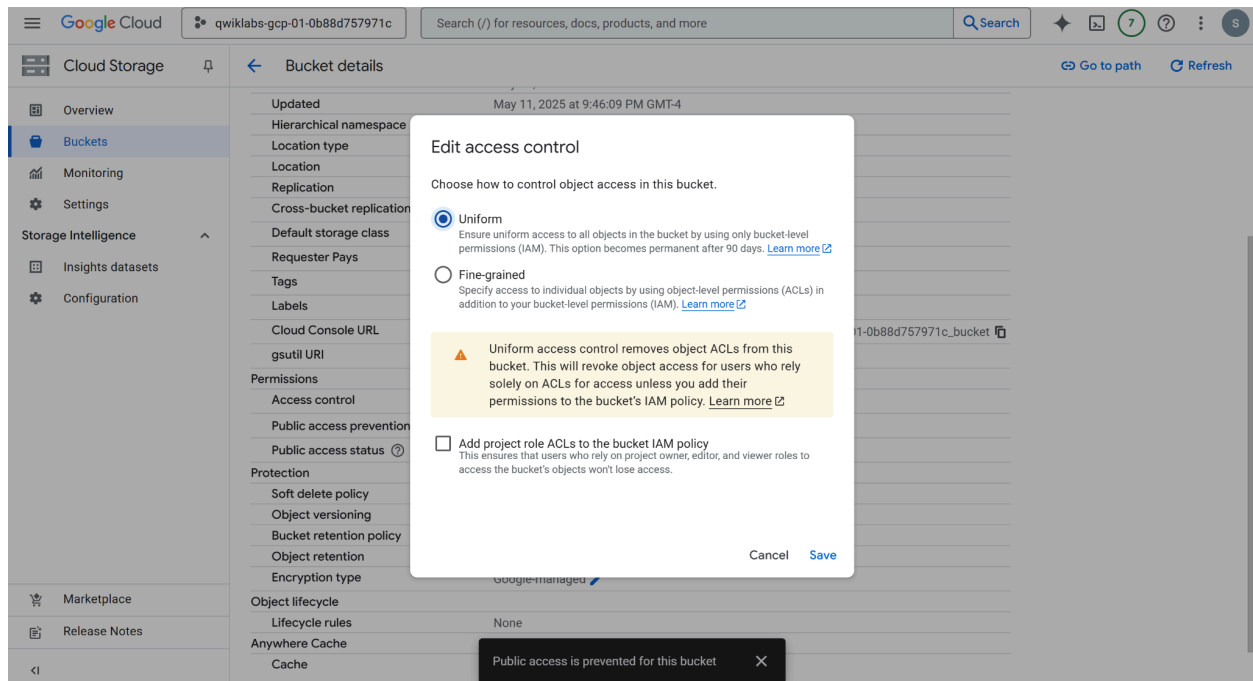
Filter objects and folders

Show

Live objects only

| Name       | Size    | Type                     | Created              |  |
|------------|---------|--------------------------|----------------------|--|
| myfile.csv | 11.5 KB | application/octet-stream | May 11, 2025, 7:19:2 |  |

To mitigate the storage threat, I enforced uniform bucket-level IAM policies and revoked object-level ACLs (Access Control Lists) that granted public access.



To reduce exposure, I created a custom rule that allows SSH (TCP port 22) only from a trusted IP range (35.235.240.0/20). Instead of using Google Cloud's default rules, I specified exact parameters: source IPs, target tags, direction, protocols, and ports, essentially enforcing least privilege and zero trust principles to restrict access to just what's needed.

Google Cloud | qwiklabs-gcp-01-0b88d757971c | firewall r

### Create a firewall rule

Name \*  
firewall-rule-for-limited-access  
Lowercase letters, numbers, hyphens allowed

Description

Logs  
Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)  
☐ On  
☒ Off

Network \*  
default

Priority \*  
1000 [Compare](#)  
Priority can be 0 - 65535

Direction of traffic  
☒ Ingress  
☐ Egress

Action on match  
☒ Allow  
☐ Deny

Targets  
Specified target tags

Targets  
Specified target tags

Target tags \*  
cc

Source filter  
IPv4 ranges

Source IPv4 ranges \*  
35.235.240.0/20 for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter  
None

Destination filter  
None

Protocols and ports  
☐ Allow all  
☒ Specified protocols and ports

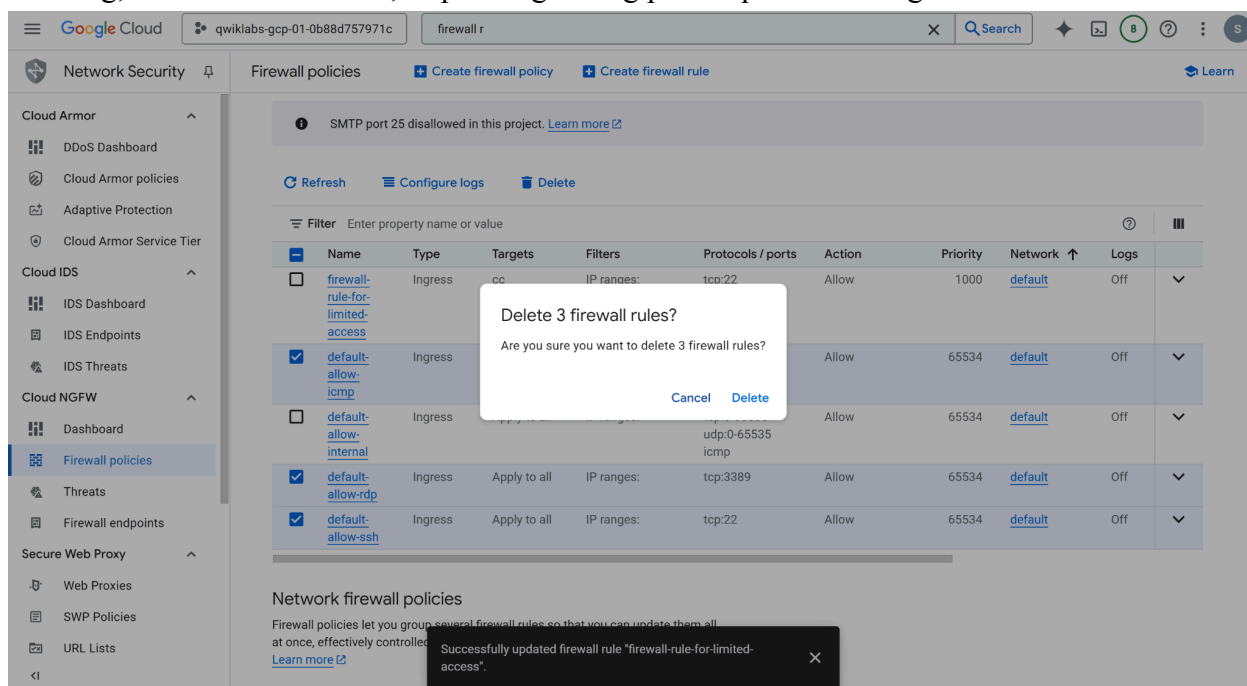
☒ TCP  
Ports  
22  
E.g. 20, 50-60

☐ UDP  
Ports  
E.g. all

☐ SCTP  
Ports

Successfully updated firewall rule "firewall-rule-for-limited-access".

I removed default firewall rules (allow-ssh, allow-rdp, allow-internal) that permitted unrestricted traffic across dangerous ports. These broad rules often leave cloud environments vulnerable to scanning, unauthorized access, or pivoting during post-exploitation stages.



I turned on firewall logging to record all incoming connection attempts matching my firewall rules. This allows for real-time monitoring and threat detection as patterns can be easily monitored through log records.

