As a cloud security analyst, one is responsible for evaluating controls against established standards to ensure that an organization's security posture is effective, compliant and aligned with industry best practices. This evaluation process is crucial for helping with risk management, compliance and continuous security improvements, ultimately helping organizations protect sensitive data, systems and their overall reputation.

PROJECT DESCRIPTION

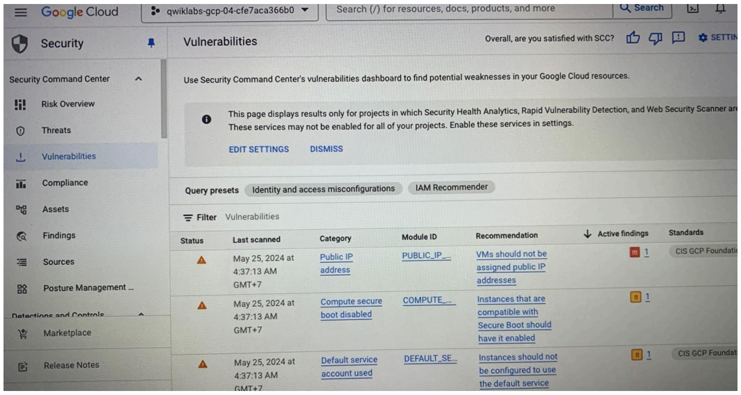
In this lab, I used the Security Command Center interface to identify and remediate threats and vulnerabilities and confirm that the issues have been resolved.

SCENARIO

I am to use a report that highlights security concerns on a company's network.
Specifically, they have recently discovered that there is a Cloud Storage bucket within the organization that contains sensitive documents and is incorrectly configured. I'll need to correctly configure the bucket and verify that the issues have been resolved.
Here's how I did this ;

First Step: Identify the Vulnerabilities with SCC

I used the Security Command Centre to check the compliance status of my project and identify the high and medium risk vulnerabilities that need to be remediated.



Use Security Command Center's vulnerabilities dashboard to find potential weaknesses in your Google Cloud resources.

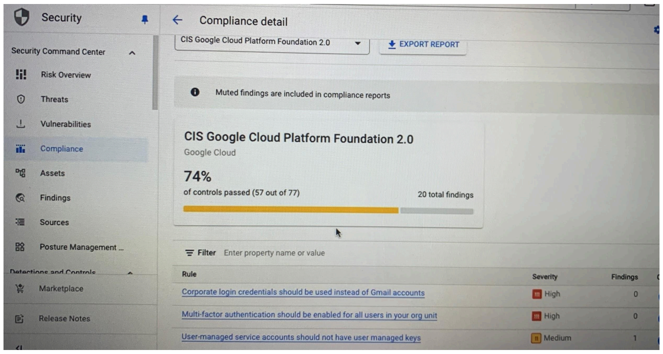
This page displays results only for projects in which Security Health Analytics, Rapid Vulnerability Detection, and Web Security Scanner are
These services may not be enabled for all of your projects. Enable these services in settings.

Status	Last scanned	Category	Module ID	Recommendation	↓ Active findings	Standards
▲	May 25, 2024 at 4:37:13 AM GMT+7	Public IP address	PUBLIC_IP_...	VMs should not be assigned public IP addresses	1	CIS GCP Foundati
▲	May 25, 2024 at 4:37:13 AM GMT+7	Compute secure boot disabled	COMPUTE_...	Instances that are compatible with Secure Boot should have it enabled	1	
▲	May 25, 2024 at 4:37:13 AM GMT+7	Default service account used	DEFAULT_SE...	Instances should not be configured to use the default service	1	CIS GCP Foundat

There were many active vulnerabilities listed. I used the filter to search for the specific findings using the **Module ID.** I focused on the following active findings listed for my storage bucket:

1. **Public bucket ACL (PUBLIC_BUCKET_ACL):** This entry indicates that there is an Access Control List(ACL) entry for the storage bucket that is publicly accessible which means that anyone on the internet can read files stored in the bucket. This is a high–risk security vulnerability that needs to be prioritized for remediation.
2. **Bucket policy only disabled (BUCKET_POLICY_ONLY_DISABLED):** This entry indicates that uniform bucket level permissions are not enabled on a bucket. Uniform bucket level access provides a way to control who can access Cloud Storage buckets and objects, simplifying how access is granted to cloud storage resources. This is a medium risk vulnerability that must also be remediated.
3. **Bucket logging disabled (BUCKET_LOGGING_DISABLED):** This entry indicates that there is a storage bucket that does not have logging enabled. This is a low risk vulnerability that is not required to be remediated in this scenario.

I then viewed the details in the **CIS Google Cloud Platform Foundation 2.0** tile to sort the findings and display the active findings at the top of the list.



Compliance detail

CIS Google Cloud Platform Foundation 2.0

Muted findings are included in compliance reports

CIS Google Cloud Platform Foundation 2.0
Google Cloud
74%
of controls passed (57 out of 77)
20 total findings

Rule	Severity	Findings
Corporate login credentials should be used instead of Gmail accounts	High	0
Multi-factor authentication should be enabled for all users in your org unit	High	0
User-managed service accounts should not have user managed keys	Medium	1

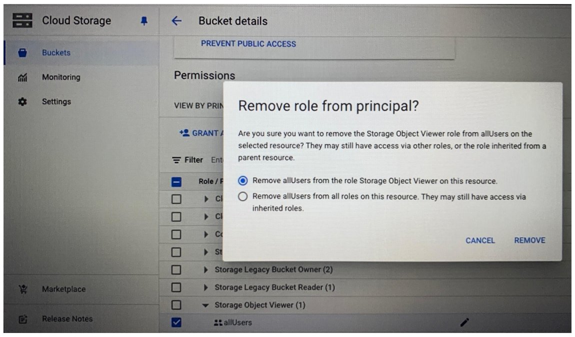
The following rules in the report have active findings for the cloud storage bucket

a. Cloud storage buckets should not be anonymously or publicly accessible.
b. Bucket policy only should be Enabled.

Second Step: Remediate the Security Vulnerabilities

Here, I remediated the security vulnerabilities identified in the previous step. Then, I checked the Security status of the Cloud storage bucket in the report to confirm that the issues have been remediated.

Firstly, I removed the public access to the cloud storage bucket.



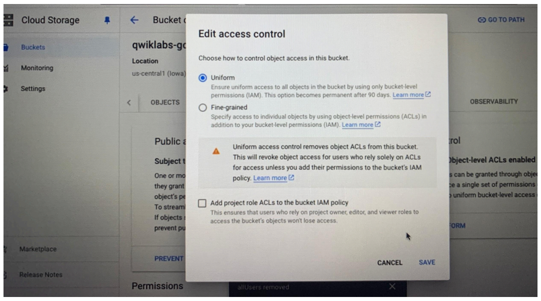
Remove role from principal?

Are you sure you want to remove the Storage Object Viewer role from allUsers on the selected resource? They may still have access via other roles, or the role inherited from a parent resource.

● Remove allUsers from the role Storage Object Viewer on this resource.
○ Remove allUsers from all roles on this resource. They may still have access via inherited roles.

CANCEL REMOVE

Next, I switched the access control to uniform. This will enforce a single(uniform) set of permissions for the bucket and its objects.



Edit access control

Choose how to control object access in this bucket.

● Uniform
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more

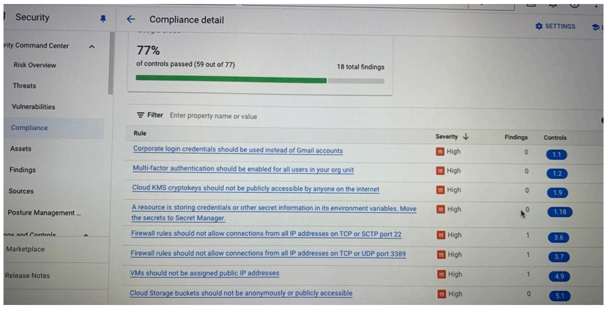
○ Fine-grained
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

Uniform access control removes object ACLs from this bucket. This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy. Learn more

□ Add project role ACLs to the bucket IAM policy
This ensures that users who rely on project owner, editor, and viewer roles to access the bucket's objects won't lose access.

CANCEL SAVE

Finally, I ran a compliance report to confirm that the vulnerability issues have been remediated.



77%
of controls passed (59 out of 77)
18 total findings

Rule	Severity ↓	Findings	Controls
Corporate login credentials should be used instead of Gmail accounts	High	0	1.1
Multi-factor authentication should be enabled for all users in your org unit	High	0	1.2
Cloud KMS cryptokeys should not be publicly accessible by anyone on the internet	High	0	1.9
A resource is storing credentials or other secret information in its environment variables. Move the secrets to Secret Manager.	High	0	1.18
Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22	High	1	3.6
Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	High	1	3.7
VMs should not be assigned public IP addresses	High	1	4.9
Cloud Storage buckets should not be anonymously or publicly accessible	High	0	5.1

The number of active findings for the **cloud Storage buckets** was not **anonymously or publicly accessible** and **Bucket policy only should be enabled** rules was now **0.** This indicates that the **public bucket ACL** and **Bucket policy only disabled** vulnerabilities for the cloud storage bucket have been remediated.

CONCLUSION

Through this lab activity, I have gained practical experience in identifying and prioritizing threats using the security Command Center(SCC). I also remediated the vulnerabilities identified for my project and generated a report to confirm that the vulnerabilities have been remediated.

By remediating the vulnerabilities and ensuring the compliance status of the cloud storage bucket, I’ve helped my organization to prevent data breaches, unauthorized access and data loss.