Course 2_Lab 2: Using Google Security Command Center reports to remediate findings

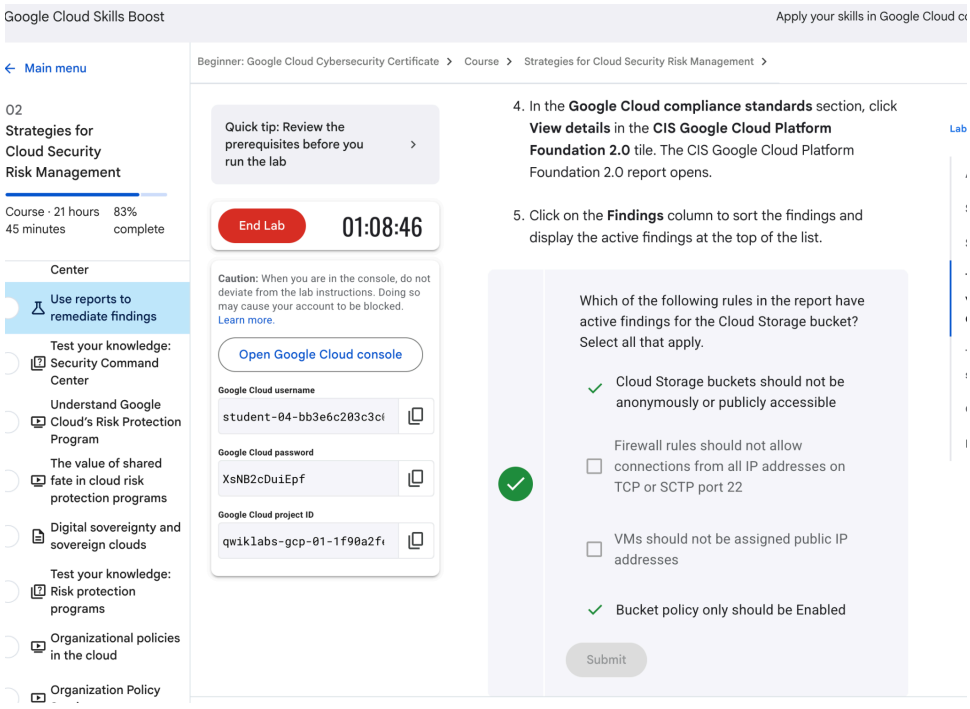
Scenario:

In your role as a newly appointed junior cloud security analyst at Cymbal Bank, one of your critical responsibilities includes identifying and mitigating threats and vulnerabilities in a timely and effective manner. Your team lead, Chloe, has approached you with a report that highlights security concerns on the company network. Specifically, they have recently discovered that there is a Cloud Storage bucket within the organization that contains sensitive documents and is incorrectly configured. You'll need to correctly configure the bucket and verify that the issues have been resolved.

Here's how you'll do this task: **First**, you'll use the Security Command Center to identify and verify the security threats. **Then**, you'll remediate the high and medium risk issues. **Finally**, you'll run a compliance report to verify that the remediation has been successful.

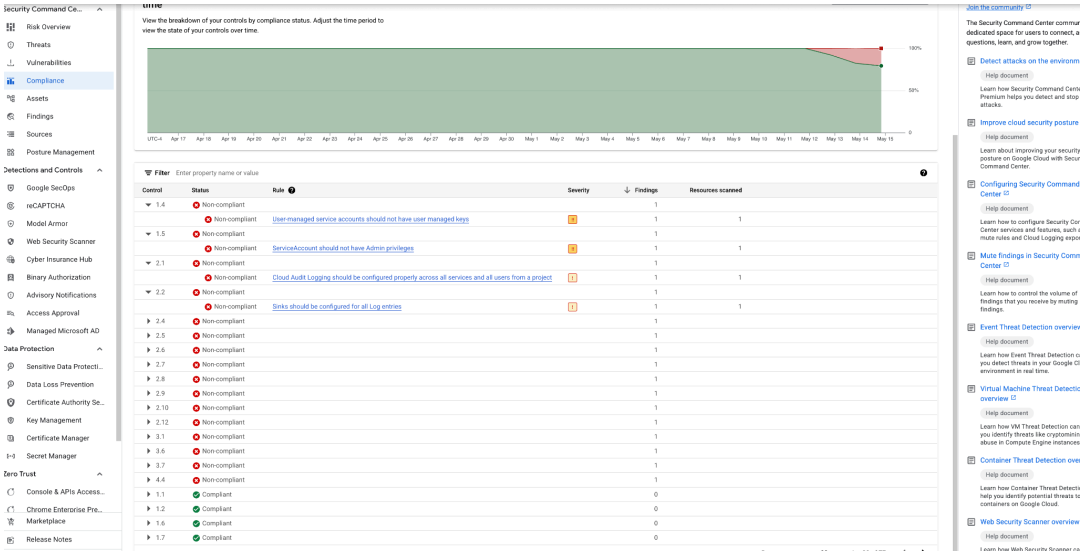
MY WORK:
Task 1: Identify the vulnerabilities with Security Command Center (SCC)

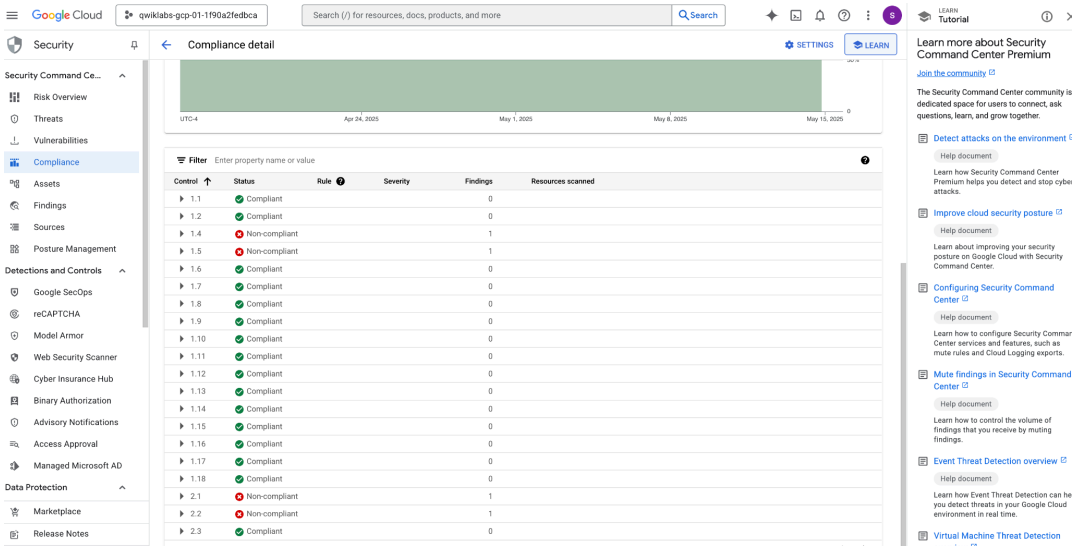
The image below is a scored reflection after reviewing reports within the Security Command Center. In the reports, buckets were able to be publicly accessed as well as anonymously accessed and did not have any policies enabled. The primary concern in a situation such as this is unauthorized access to data, data leakage, and data integrity. Security misconfigurations and broken access controls are the root of vulnerabilities in this scenario that could potentially lead to a security breach.

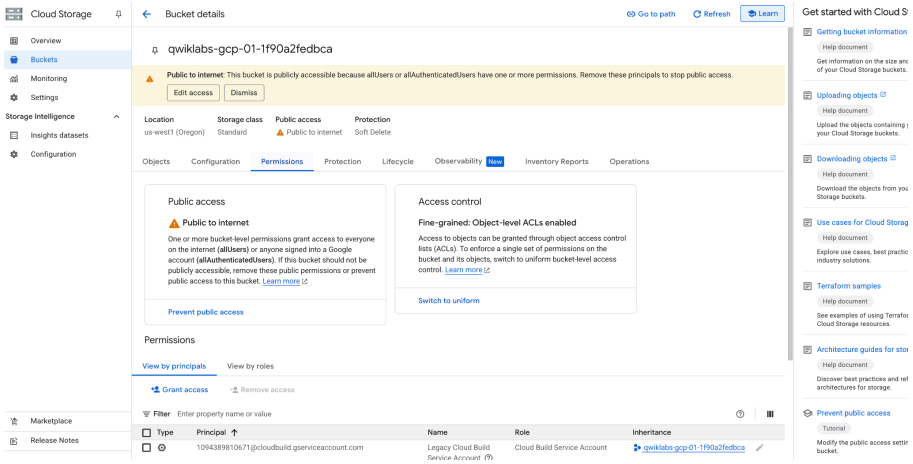


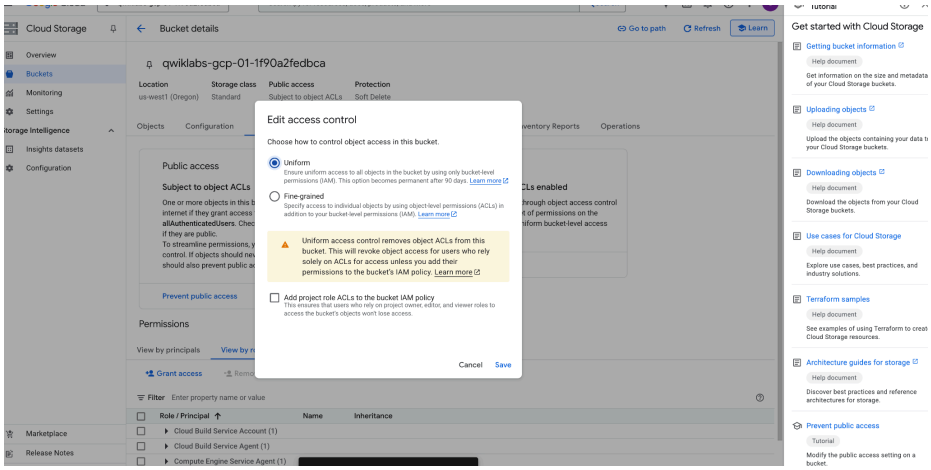
Task 2. Remediate the security vulnerabilities

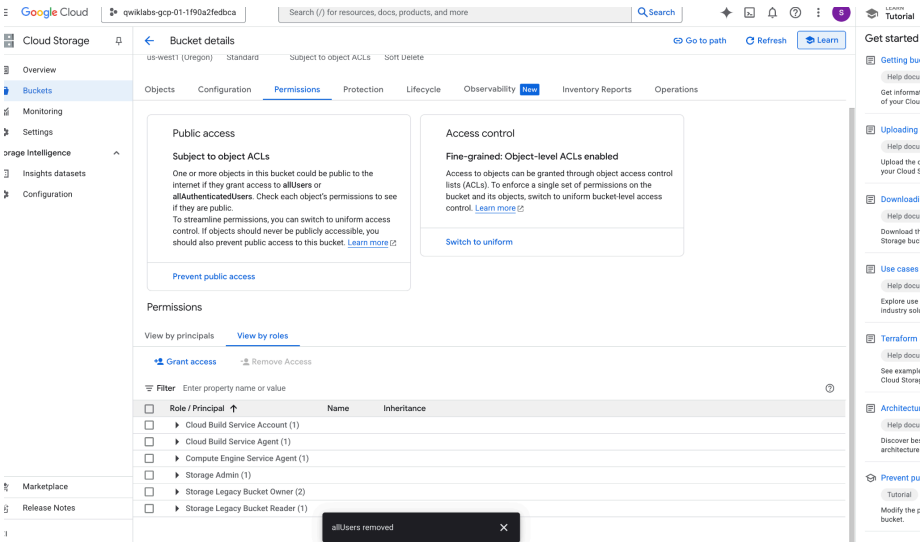
In order to remediate the vulnerabilities in the images below the cloud security analyst must modify the Permissions in the Google Cloud Platform. Removing access and changing the bucket policy to a uniform single set of permissions remediates the vulnerabilities mentioned in this scenario.











Access control lists have been updated for buckets that required changes for this lab.

My Self-Assessment:
In this lab, reviewing reports focused on bucket policies, roles, and permission were necessary to remediate the findings to prevent potential data breaches. It's important to uphold security compliance standards to maintain integrity, maintain trust with users and clients, while also protecting organizational information. A number of vulnerabilities existed such as security misconfigurations, unrestricted file uploads, etc.