

## 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.

Google Cloud Skills Boost

Apply your skills in Google Cloud c

← Main menu

02

Strategies for Cloud Security Risk Management

Course · 21 hours 45 minutes 83% complete

Center

Use reports to remediate findings

Test your knowledge: Security Command Center

Understand Google Cloud's Risk Protection Program

The value of shared fate in cloud risk protection programs

Digital sovereignty and sovereign clouds

Test your knowledge: Risk protection programs

Organizational policies in the cloud

Organization Policy

Beginner: Google Cloud Cybersecurity Certificate > Course > Strategies for Cloud Security Risk Management >

Quick tip: Review the prerequisites before you run the lab

End Lab 01:08:46

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)

Open Google Cloud console

Google Cloud username  
student-04-bb3e6c283c3ci

Google Cloud password  
XsNB2cDuiEpF

Google Cloud project ID  
qw1klabs-gcp-01-1f90a2ft

4. In the **Google Cloud compliance standards** section, click **View details** in the **CIS Google Cloud Platform Foundation 2.0** tile. The CIS Google Cloud Platform Foundation 2.0 report opens.

5. Click on the **Findings** column to sort the findings and display the active findings at the top of the list.

Which of the following rules in the report have active findings for the Cloud Storage bucket? Select all that apply.

☒ Cloud Storage buckets should not be anonymously or publicly accessible

☐ Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22

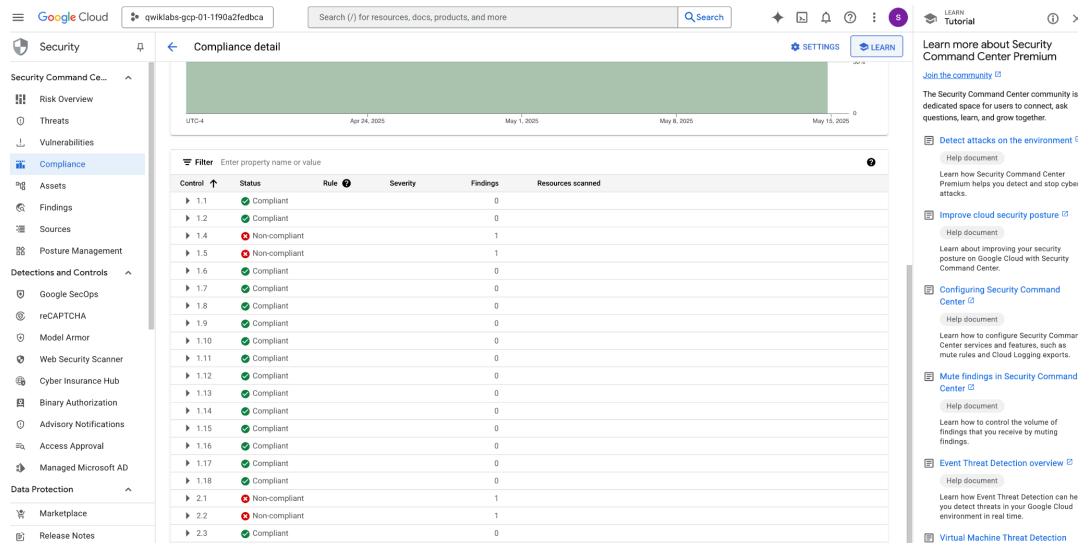
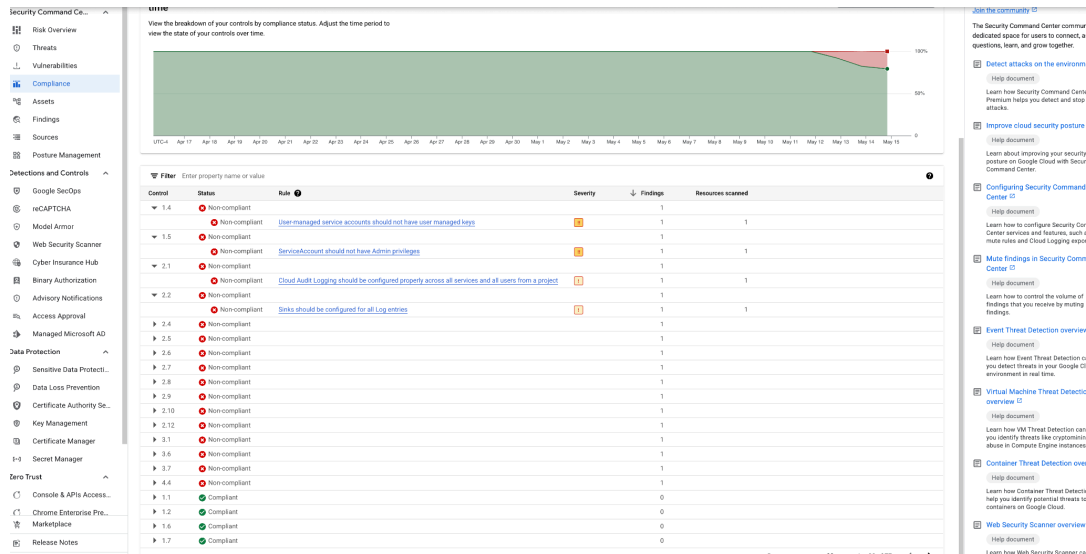
☐ VMs should not be assigned public IP addresses

☒ Bucket policy only should be Enabled

Submit

## 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.



Cloud Storage Bucket details for `qwiklabs-gcp-01-1f90a2fedbca`. The bucket is currently **Public to internet**, which is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. A warning banner at the top indicates this state and provides a link to [Edit access](#).

The **Public access** section shows the bucket is **Public to internet**. It explains that one or more bucket-level permissions grant access to everyone on the internet (allUsers) or anyone signed into a Google account (allAuthenticatedUsers). It advises that if the bucket should not be publicly accessible, these public permissions should be removed to prevent public access. A [Learn more](#) link is provided.

The **Access control** section shows **Fine-grained: Object-level ACLs enabled**. It states that access to objects can be granted through object access control lists (ACLs). To enforce a single set of permissions on the bucket and its objects, it suggests switching to uniform bucket-level access control. A [Learn more](#) link is provided. A [Switch to uniform](#) button is also present.

The **Permissions** section shows a table of permissions. The table has columns for **Type**, **Principal**, **Name**, **Role**, and **Inheritance**. The table lists the `1094389110671@gcpcloudbuild.gserviceaccount.com` as a principal with the `Legacy Cloud Build Service Account` role, inheriting from `qwiklabs-gcp-01-1f90a2fedbca`.

Cloud Storage Bucket details for `qwiklabs-gcp-01-1f90a2fedbca`. The bucket is currently **Public to internet**. A modal dialog titled **Edit access control** is open, showing options to choose how to control object access in the bucket.

The modal dialog has two radio buttons: **Uniform** (selected) and **Fine-grained**. The **Uniform** option is described as "Choose uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days." The **Fine-grained** option is described as "Selectively access to individual objects by using object-level permissions (ACL) in addition to your bucket-level permissions (IAM)." A warning message states: "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." There is a checkbox for **Add project role ACLs to the bucket IAM policy**, which ensures that users who rely on project owner, editor, and viewer roles to access the bucket's objects won't lose access. The modal has **Cancel** and **Save** buttons.

Cloud Storage Bucket details for `qwiklabs-gcp-01-1f90a2fedbca`. The bucket is currently **Public to internet**. The **Public access** section shows the bucket is **Subject to object ACLs**. It explains that one or more objects in this bucket may be public to the internet if they grant access to allUsers or allAuthenticatedUsers. It advises that to streamline permissions, control if objects should never be publicly accessible, you should also prevent public access to this bucket. A [Learn more](#) link is provided.

The **Access control** section shows **Fine-grained: Object-level ACLs enabled**. It states that access to objects can be granted through object access control lists (ACLs). To enforce a single set of permissions on the bucket and its objects, it suggests switching to uniform bucket-level access control. A [Learn more](#) link is provided. A [Switch to uniform](#) button is also present.

The **Permissions** section shows a table of permissions. The table has columns for **Role / Principal**, **Name**, and **Inheritance**. The table lists several roles, including `Cloud Build Service Account`, `Cloud Build Service Agent`, `Compute Engine Service Agent`, `Storage Admin`, `Storage Legacy Bucket Owner`, and `Storage Legacy Bucket Reader`.

A notification banner at the bottom states **allUsers removed**.

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.