Mitigate Threats and Vulnerabilities with Security Command Center: Challenge Lab

[You Tube Video](https://www.youtube.com/watch?v=xcSscQiJOps)

**GSP382**

**Overview**

In a challenge lab you’re given a scenario and a set of tasks. Instead of following step-by-step instructions, you will use the skills learned from the labs in the course to figure out how to complete the tasks on your own! An automated scoring system (shown on this page) will provide feedback on whether you have completed your tasks correctly.

When you take a challenge lab, you will not be taught new Google Cloud concepts. You are expected to extend your learned skills, like changing default values and reading and researching error messages to fix your own mistakes.

To score 100% you must successfully complete all tasks within the time period!

This lab is recommended for students who have enrolled in the [Mitigate Threats and Vulnerabilities with Security Command Center](https://www.cloudskillsboost.google/course_templates/759) skill badge. Are you ready for the challenge?

Topics tested

* Create mute rules for Cymbal Bank
* Analyze and fix Cymbal Bank's high vulnerability findings
* Identify application vulnerabilities with SCC's security scanning features
* Export Cymbal Bank Findings to a Google Cloud Storage Bucket

**Setup and requirements**

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources are made available to you.

This hands-on lab lets you do the lab activities in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials you use to sign in and access Google Cloud for the duration of the lab.

To complete this lab, you need:

* Access to a standard internet browser (Chrome browser recommended).

**Note:** Use an Incognito (recommended) or private browser window to run this lab. This prevents conflicts between your personal account and the student account, which may cause extra charges incurred to your personal account.

* Time to complete the lab—remember, once you start, you cannot pause a lab.

**Note:** Use only the student account for this lab. If you use a different Google Cloud account, you may incur charges to that account.

**Challenge scenario**



Cymbal Bank is an American retail bank with over 2,000 branches in all 50 states. It offers comprehensive debit and credit services that are built on top of a robust payments platform. Cymbal Bank is a digitally transforming legacy financial services institution.

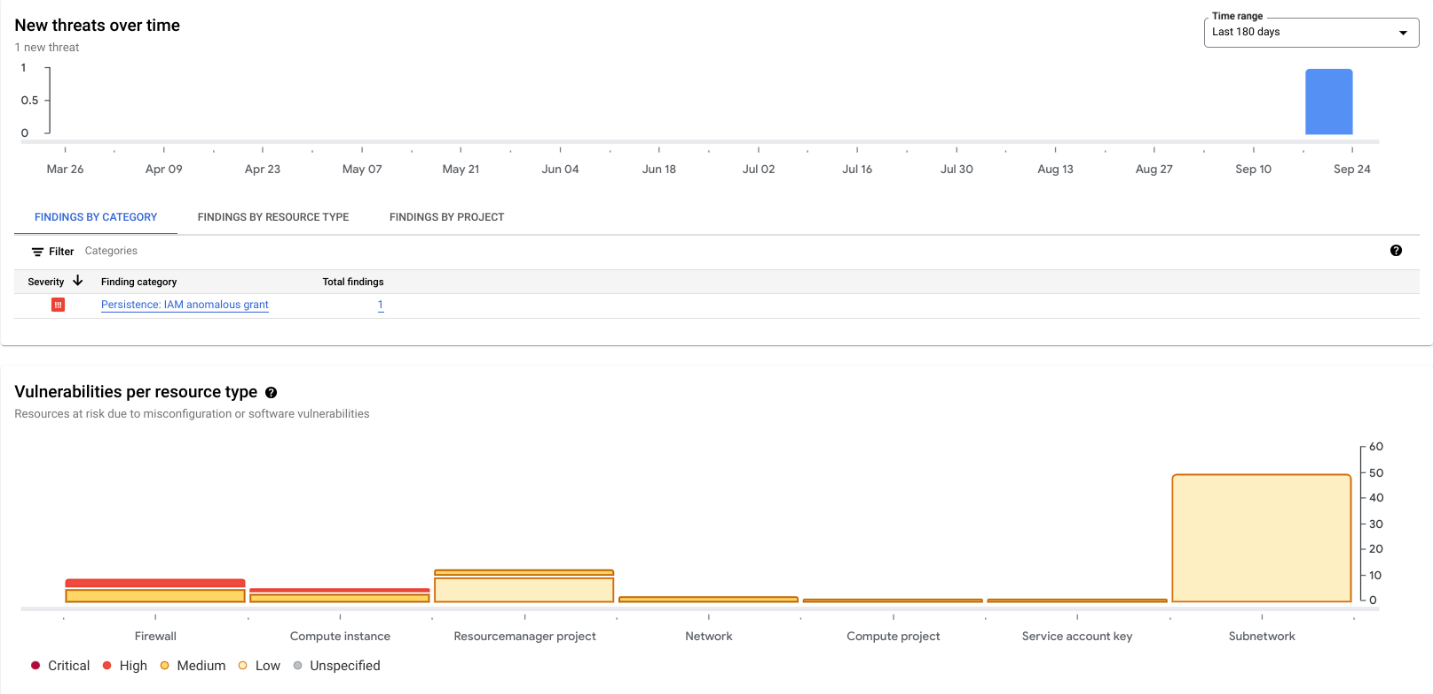
Cymbal Bank was founded in 1920 under the name Troxler. Cymbal Group acquired the company in 1975 after it had been investing heavily in Cymbal Group's proprietary ATMs. As the bank grew into a national leader, they put strategic emphasis on modernizing the customer experience both in-person at their branches and digitally through an app they released in 2014. Cymbal Bank employs 42,000 people nationwide and, in 2019, reported $24 billion in revenue.

In this challenge, you are a cloud security engineer tasked with securing Cymbal Bank's Google Cloud environment by leveraging Security Command Center's features. You have performed these tasks in previous labs. Now, it's your turn to demonstrate your proficiency with Security Command Center by implementing advanced threat detection and mitigation strategies, optimizing access controls, and ensuring compliance with industry regulations and best practices.

**Task 1. Configure the environment**

First, make some baseline configurations to Cymbal Bank's environment, so you can implement robust security controls with Security Command Center.

1. Open the navigation menu and select **Security > Security Command Center > Findings**.
2. From the time range selector, select **Last 180 days**. Your output should be similar to the following:

**Warning:** For all SCC interfaces you interact in this challenge lab, ensure that the time range selected is always set to 180 days! If you don't configure this properly, you may not be able to identify or verify any of the requirements for a task.

**Task 2. Create mute rules for Cymbal Bank**

Cymbal Bank is not interested in surfacing findings against certain resources in their Google Cloud environment.

1. For this task, create three mute rules that address the following:

|  |  |  |
| --- | --- | --- |
| **Name** | **Finding** | **Description** |
| muting-flow-log-findings | Flow logs disabled | Rule for muting VPC Flow Logs |
| muting-audit-logging-findings | Audit logging disabled | Rule for muting audit logs |
| muting-admin-sa-findings | Admin service account | Rule for muting admin service account findings |

**Warning:** Ensure that the time range selected is always set to 180 days! If you don't configure this properly, you may not be able to identify or verify any of the requirements for a task.**Note:** You can find what to place in your Finding Query by exploring the Finding's details in SCC.

Click **Check my progress** to verify the objective.

Assessment Completed!

Create mute rules for Cymbal Bank

Check my progress

*Assessment Completed!*

**Task 3. Analyze and fix Cymbal Bank's high vulnerability findings**

Cymbal Bank wants to remove two high severity Findings in their Google Cloud environment. You are tasked with using SCC to identify and follow the steps laid out to fix the following high severity Findings so they are no longer vulnerable:

* Open SSH port
* Open RDP port

Ensure that these rules are not facing the public internet. You can use the IP address 35.235.240.0/20 as a replacement for the ones facing the public internet.

Click **Check my progress** to verify the objective.

Assessment Completed!

Fix Cymbal Bank's high vulnerability findings

Check my progress

*Assessment Completed!*

**Task 4. Identify application vulnerabilities with SCC's security scanning features**

In addition to resolving any infrastructure findings, you also need to identify any application vulnerabilities. In many cases, application vulnerabilities can be introduced unknowingly, so as a cloud security engineer you want to be especially diligent of any new web applications running in your environment.

Cymbal Bank wants to test-run Web Security Scanner against a sample application deployed in this environment to ensure it is functioning properly. When you started this lab, a Terraform script deployed a sample banking web application running on a Google Compute Engine instance.

To run a Web Security scan, the External IP of the Compute Engine VM Instance needs to be static.

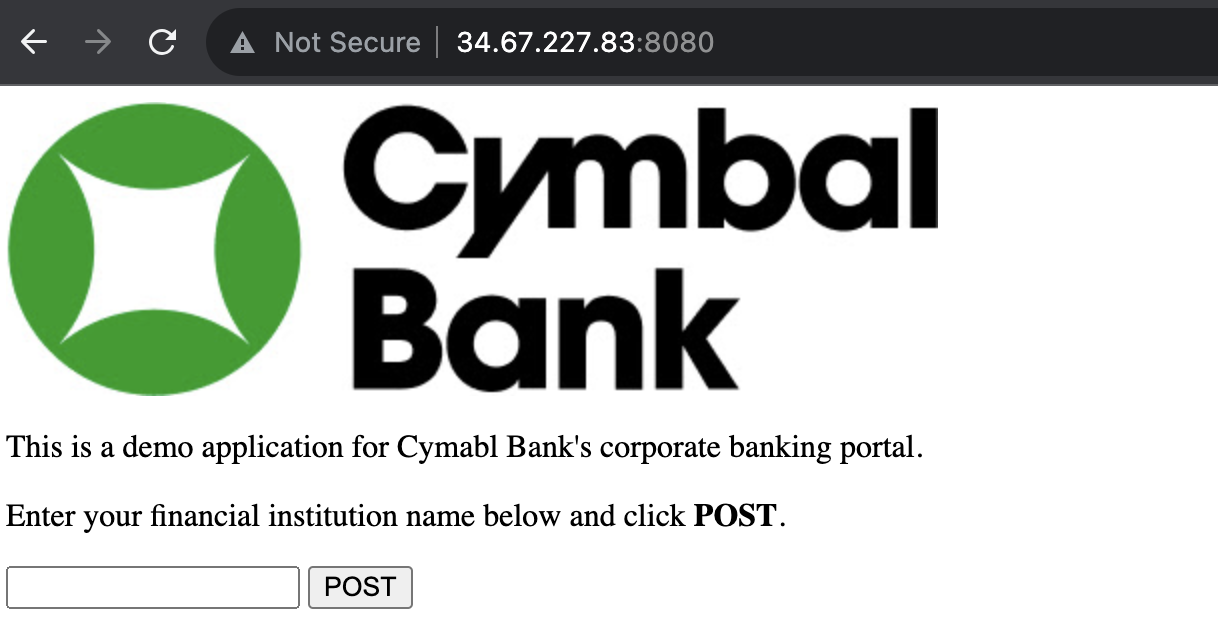
1. On the Navigation menu, select **Compute Engine** > **VM instances** > **cls-vm**. On the Details page, click **Edit**.
2. In the **Network Interface** section, expand the default network.
3. Click the "External IPv4 address" dropdown and click **Reserve Static External IP address** .
4. Give it the name static-ip and click **Reserve**.
5. Click **Save**.
6. Find the external IP address of the instance.
7. Replace YOUR\_EXTERNAL\_IP in the URL field below with that IP address, and open the URL in a new browser tab:

http://<YOUR\_EXTERNAL\_IP>:8080

Copied!

content\_copy

A Cymbal Bank corporate banking portal with a web form should appear.



For this task, run a Web Security scan against this application's URL (with port 8080).

Click **Check my progress** to verify the objective.

Assessment Completed!

Run a Web Security Scan

Check my progress

*Assessment Completed!*

**Task 5. Export Cymbal Bank Findings to Google Cloud Storage**

Cymbal Bank wants to keep information about security incidents, vulnerabilities and misconfigurations for several years for auditing purposes. As a Cloud Security Engineer, your final task is to export all existing Findings to a Google Cloud Storage Bucket with the following specifications:

* **Bucket name:** scc-export-bucket-qwiklabs-gcp-02-a22a568e6d9e
* **Location type:** regional
* **Location:** us-central1

The export should have the following properties:

* **Filename:** findings.jsonl
* **Format:** JSONL
* **Time Range:** All time

Click **Check my progress** to verify the objective.