Start Lab 01:30:00

Analyzing Findings with Security Command Center

Lab 1 hour No cost Intermediate

GSP1164

Google Cloud Self-Paced Labs

Security Command Center

Lab 1 hour No cost Intermediate

GSP1164

Google Cloud Self-Paced Labs

Prerequisites

It is recommended the learner has familiarity with the following before starting this lab:

- Fundamental understanding of cloud computing concepts.
- Familiarity with the Google Cloud console.
- Familiarity with severity classifications for findings is recommended, but not required.
- Familiarity with Pub/Sub and BigQuery is recommended, but not required.

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 will be made available to you.

This hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that 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 or private browser window to run this lab. This prevents any 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:** If you already have your own personal Google Cloud account or project, do not use it for this lab to avoid extra charges to your account.

How to start your lab and sign in to the Google Cloud console

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is the **Lab Details** panel with the following:
    - The **Open Google Cloud console** button
    - Time remaining
    - The temporary credentials that you must use for this lab
    - Other information, if needed, to step through this lab
2. Click **Open Google Cloud console** (or right-click and select **Open Link in Incognito Window** if you are running the Chrome browser).

    The lab spins up resources, and then opens another tab that shows the **Sign in** page.

    Tip: Arrange the tabs in separate windows, side-by-side.

    > **Note:** If you see the **Choose an account** dialog, click **Use Another Account**.

3. If necessary, copy the **Username** below and paste it into the **Sign in** dialog.

    ```
    "Username"
    ```

    You can also find the **Username** in the **Lab Details** panel.

4. Click **Next**.
5. Copy the **Password** below and paste it into the **Welcome** dialog.

    ```
    "Password"
    ```

You can also find the **Password** in the **Lab Details** panel.

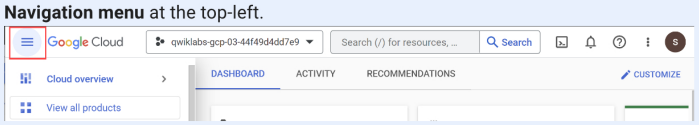
6. Click **Next**.

> **Important:** You must use the credentials the lab provides you. Do not use your Google Cloud account credentials.

> **Note:** Using your own Google Cloud account for this lab may incur extra charges.

7. Click through the subsequent pages:
    - Accept the terms and conditions.
    - Do not add recovery options or two-factor authentication (because this is a temporary account).
    - Do not sign up for free trials.

After a few moments, the Google Cloud console opens in this tab.

> **Note:** To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left.


Activate Cloud Shell

Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud. Cloud Shell provides command-line access to your Google Cloud resources.

1. Click **Activate Cloud Shell** at the top of the Google Cloud console.

When you are connected, you are already authenticated, and the project is set to your **Project_ID**, `PROJECT_ID`. The output contains a line that declares the **Project_ID** for this session:

```
Your Cloud Platform project in this session is set to "PROJECT_ID"
```

`gcloud` is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

2. (Optional) You can list the active account name with this command:

```
gcloud auth list
```

3. Click **Authorize**.

Output:

```
ACTIVE: *
ACCOUNT: "ACCOUNT"

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

4. (Optional) You can list the project ID with this command:

```
gcloud config list project
```

Output:

```
[core]
project = "PROJECT_ID"
```

Note: For full documentation of `gcloud`, in Google Cloud, refer to the gcloud CLI overview guide.

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.

Cymbal Bank is interested in integrating a centralized security monitoring platform to help monitor threats and remediate vulnerabilities across their Google Cloud resources in their corporate banking applications. As a Cloud Security Engineer, you are tasked with learning about Security Command Center's export and analytics features so you can deliver a presentation to the CTO on the services' benefits.

Task 1: Create a continuous export pipeline to Pub/Sub.

Security Command Center can export security findings to external resources using several methods, including:

- Continuous exports to a BigQuery dataset.
- Continuous exports to Pub/Sub.
- One-time exports to CSV files.
- One-time exports to Cloud Storage buckets as JSON files.

In this task, you will configure continuous exports of findings to Pub/Sub.

Note: Continuous exports findings work only for newly created findings.

Continuous exports to Pub/Sub are usually used for forwarding findings to external

security management systems such as Splunk or QRadar.

In this task, you will export your findings to a Pub/Sub topic and then simulate an application by fetching the messages from a Pub/Sub subscription.

> **Note:** You can check this documentation page to learn more about the basics of Pub/Sub.

Before we start configuring an SCC export, we need to create a Pub/Sub topic and subscription.

1. Open the navigation menu and under the **Analytics** header, click **Pub/Sub > Topics**.
2. Click the **Create Topic** button located near the top of the page.
3. Enter in **export-findings-pubsub-topic** for the Topic ID.
4. Keep the other default settings and click **Create**.

This will automatically kick off the creation of both a Pub/Sub topic and an associated subscription.

5. Click **Subscriptions** from the left-hand menu.
6. Click on **export-findings-pubsub-topic-sub**.

This will provide you with a dashboard of statistics and metrics related to the messages published in this subscription.

7. Open the navigation menu and select **Security > Security Command Center > Overview > Settings**.
8. Click on the **Continuous Exports** tab.
9. Click the **Create Pub/Sub Export** button.
10. For the continuous export name, enter in **export-findings-pubsub**.
11. For the continuous export description, enter in **Continuous exports of Findings to Pub/Sub and BigQuery**.
12. For the project name, select the `____` Project ID of the project you are working in (*do not* select Qwiklabs Resources).
13. From the "Select a Cloud Pub/Sub Topic" dropdown, select **export-findings-pubsub-topic**.
14. Set the findings query to the following:

```
state="ACTIVE"
AND NOT mute="MUTED"
```

This query ensures that all new `ACTIVE` and `NOT MUTED` findings will be forwarded to the newly created Pub/Sub topic.

> **Note:** You might see the message that there are several findings matched. Remember that existing findings will **not** be forwarded to the Pub/Sub topic.

15. Now click **Save**.

You have now successfully created a continuous export from Security Command Center to Pub/Sub. You will now create new findings and check how they are exported to Pub/Sub.

16. Open a new Cloud Shell session (▶).

17. Run the following command to create a new virtual machine:

```
gcloud compute instances create instance-1 --zone=lab zone \
--machine-type e2-micro \
--scopes=https://www.googleapis.com/auth/cloud-platform
```

18. Ensure you receive a similar output:

```
NAME: instance-1
ZONE: us-central-a
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.128.0.2
EXTERNAL_IP: 34.69.82.225
STATUS: RUNNING
```

Note: If you get an error message that says `ERROR: (gcloud.compute.instances.create) You do not currently have an active account selected.`, re-run the command again.

This command will create a new VM instance with a Public IP address and a default Service Account attached.

This activity will immediately generate three new vulnerability findings:

- Public IP address
- Default service account used
- Compute secure boot disabled

19. Open the navigation menu and under the **Analytics** header, click **Pub/Sub > Subscriptions**.

20. Select the **export-findings-pubsub-topic-sub** subscription.

21. Select the **Messages** tab from the center of the Console.

22. Click the **Enable ack messages** checkbox.

23. Click on the **Pull** button.

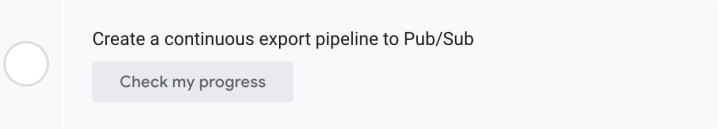
You should see messages in this subscription that relate to the public IP address, default service account used, and compute secure boot disabled vulnerabilities.

Note: You may have to click the **Pull** button a couple times to see the messages mentioned above come in.

By pulling the messages from the Pub/Sub subscription you have simulated behavior of an application that can forward these messages to another security monitoring system like Splunk.

In the next task, you will learn how to export and analyze SCC findings with BigQuery.

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



Task 2: Export and Analyze SCC findings with BigQuery

SCC findings can also be exported to a BigQuery dataset. This might be useful for building analytical dashboards used for checking what type of findings appear in your organization most often.

As of now, configuring continuous exports can only be set using the Command Line Interface (not in the Console).

1. In your Cloud Shell session, run the following command to create a new BigQuery dataset:

```
PROJECT_ID=$(gcloud config get project)
bq --location=lab region --apilog=/dev/null mk --dataset \
$PROJECT_ID:continuous_export_dataset
```

2. We have not used an SCC command line interface in this project yet, so we need to enable the SCC service in this project:

```
gcloud services enable securitycenter.googleapis.com
```

3. Now create a new export by entering this command:

```
gcloud scc bqexports create scc-bq-cont-export --
dataset=projects//datasets/continuous_export_dataset --
project=PROJECT_ID
```

4. Ensure you receive a similar output message:

```
Created.
dataset: projects/qwiklabs-gcp-04-
571fad72c1e8/datasets/continuous_export_dataset
mostRecentEditor: student-03-fbc57ac17933@qwiklabs.net
name: projects/102856953036/bigQueryExports/SCC-bq-cont-export
principal: service-org-616463121992@gcp-sa-scc-
notification.iam.gserviceaccount.com
updateTime: '2023-05-31T15:44:22.097585Z'
```

Once new findings are exported to BigQuery, SCC will create a new table. You will now initiate new SCC findings.

5. Run the following commands to create 3 new service accounts without any IAM permissions and create 3 user-managed service account keys for them.

```
for i in {0..2}; do
gcloud iam service-accounts create sccp-test-sa-$i;
gcloud iam service-accounts keys create /tmp/sa-key-$i.json \
--iam-account=sccp-test-
sa-$i@PROJECT_ID.iam.gserviceaccount.com;
done
```

Once new findings are created in SCC, they will be exported to BigQuery. For storing them, the export pipeline will create a new table “findings”.

6. Fetch from BigQuery information about newly created finding using BigQuery CLI:

```
bq query --apilog=/dev/null --use_legacy_sql=false  \
"SELECT finding_id,event_time,finding.category FROM
continuous_export_dataset.findings"
```

7. Soon after you should receive the following output:

```
student_03_c8b8df86b01c@cloudshell:~ (qwiklabs-gcp-00-5332bb2a0c9f)$ bq query --apilog=/dev/null
+----------------------------------+--------------------+-------------------------------+
|           finding_id             |     event_time     |           category            |
+----------------------------------+--------------------+-------------------------------+
| 044b431ef50c42a43f50e0087b5fe59c | 2023-06-06 19:15:18 | USER_MANAGED_SERVICE_ACCOUNT_KEY |
| 44fa647170b36fa8970b26c064c52308 | 2023-06-06 19:15:22 | USER_MANAGED_SERVICE_ACCOUNT_KEY |
| ab813bc4a200c8360c04c91b1e972757 | 2023-06-06 19:15:15 | USER_MANAGED_SERVICE_ACCOUNT_KEY |
| e2e1f1ff90827893600bdde60a5b84d4 | 2023-06-06 19:15:25 | USER_MANAGED_SERVICE_ACCOUNT_KEY |
| 7b90ad33c93d57a6d4126e1cab199bcb | 2023-06-06 19:15:28 | USER_MANAGED_SERVICE_ACCOUNT_KEY |
+----------------------------------+--------------------+-------------------------------+
student_03_c8b8df86b01c@cloudshell:~ (qwiklabs-gcp-00-5332bb2a0c9f)$
```

Note: It may take **10+ minutes** for these findings to be generated. Rerun the above command if you don't receive a similar output.

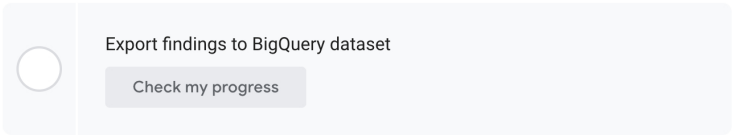
Very often Security Command Center is enabled in pre-existing and mature Google Cloud infrastructure.

As soon as the SCC is enabled, it starts scanning existing vulnerabilities and eventually might report thousands of findings on existing infrastructure.

The SCC interface might not provide the best way to sort and filter those findings, so exporting these findings to a BigQuery database is a common practice for running analytics against findings.

Direct exporting of findings to BigQuery is not supported yet. Instead, you can use a Google Cloud Storage bucket as interim storage.

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



To export *existing* findings to a BigQuery interface, we will need to export them first to a GCS bucket.

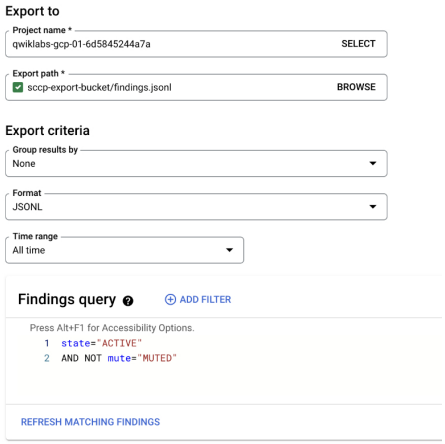
8. Open the navigation menu and select **Cloud Storage > Buckets.**
9. Click the **Create** button.
10. Every bucket name in Google Cloud must be unique. Set the bucket name to **scc-export-bucket-**`PROJECT_ID`.
11. Click **Continue**.
12. Set Location type to **Region**.
13. Choose `lab region` for the location.
14. Do not change any other settings and click **Create**.
15. Press the **Confirm** button when asked about Enforce public access prevention on this bucket.
16. Open the navigation menu and select **Security > Security Command Center > Findings**.
17. Click the **Export** button.
18. From the dropdown list, select **Cloud Storage**.
19. For the project name, select the Project ID `PROJECT_ID` (*do not* select Qwiklabs Resources).
20. Then select the Export path by clicking the **BROWSE** button.
21. Click the arrow next to the **scc-export-bucket-**`PROJECT_ID` button.
22. Set the filename to `findings.jsonl` then click **SELECT**.

23. In the Format drop-down list select **JSONL**.

24. Change the Time Range to **All time**.

25. Do not modify the default findings query.

26. Final "Export to" form might look similar to:



27. Now click the **Export** button.

28. Open the navigation menu and select **BigQuery > BigQuery Studio**.

29. From the left-hand "Explorer" menu, click on the **+ADD** button.

30. In a new "Add" window click on the "Google Cloud Storage" and the set the following parameters:

Setting	`Value`
Create table from	`Google Cloud Storage`
Select the file from GCS bucket	`scc-export-bucket-PROJECT_ID/findings.jsonl`
File format	`JSONL`
Dataset	`continuous_export_dataset`
Table	`old_findings`
Schema	Enable the "Edit as text" toggle

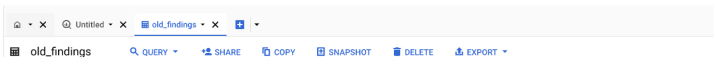
31. Now paste in the following schema:

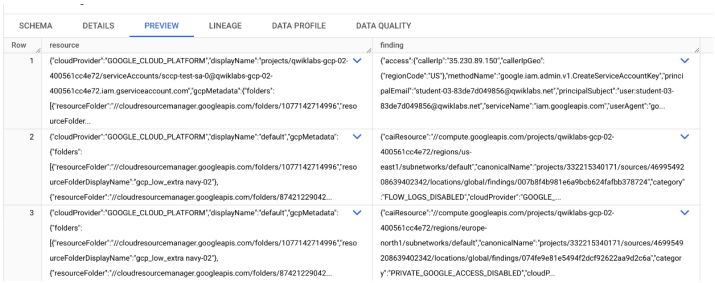
```
[
  {
    "mode": "NULLABLE",
    "name": "resource",
    "type": "JSON"
  },
  {
    "mode": "NULLABLE",
    "name": "finding",
    "type": "JSON"
  }
]
```

32. Then click the **CREATE TABLE** button.

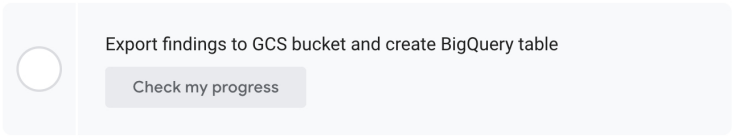
33. When the new table is created, click the link **GO TO TABLE**.

34. Click the preview tab and confirm you can view your existing findings:





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



Congratulations!

Throughout this lab, you learned about Security Command Center's analyzed assets and export features.

Next steps / Learn more

- Check out the lab titled Identify Application Vulnerabilities with Security Command Center.

Google Cloud training and certification

...helps you make the most of Google Cloud technologies. Our classes include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. Certifications help you validate and prove your skill and expertise in Google Cloud technologies.

Manual Last Updated April 26, 2024

Lab Last Tested March 18, 2024