ANALYZE AUDIT LOGS USING BigQuery

PROJECT DESCRIPTION

In this lab, I'll investigate audit logs to identify patterns of suspicious activity involving cloud resources.

SCENARIO

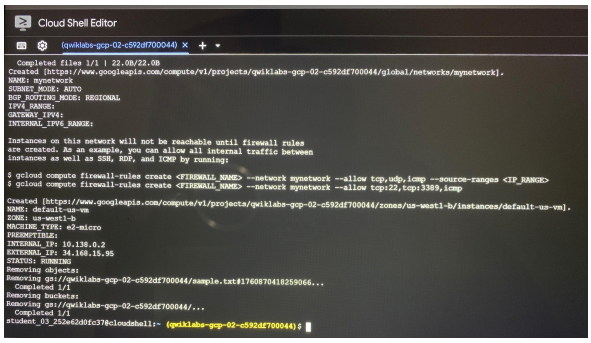
To get a better understanding of security incidents I have set up a test environment to recreate an incident and analyze the artifacts.

I will be using two separate accounts on the google cloud console: one account will generate the malicious activity and the other account will be used to investigate the activity.

First Step: Generate Account Activity

Here, I created and deleted cloud resources to generate account activity which I'll access as Cloud Audit logs.

I inputted the following command into the cloud shell terminal;



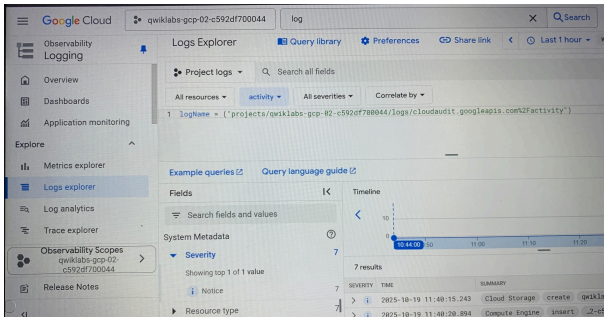
This command removes the google cloud storage bucket that was created earlier along with all of its contents.

Second Step: Export The Audit Logs

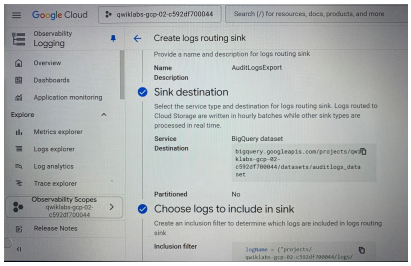
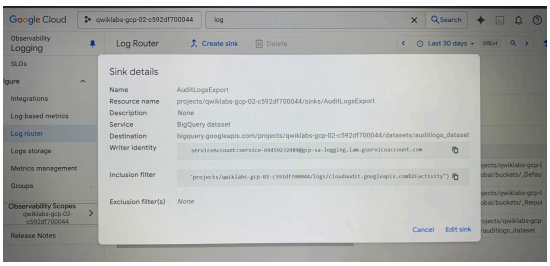
The activity I generated in the previous task was recorded as audit logs. Here, I'll export these logs to a BigQuery dataset for further analysis.

I inputted the following query into the Query builder.

logName = ("projects/Project ID/logs/cloudaudit.googleapis.com%2Factivity")



This query filters for Cloud Audit within your project.

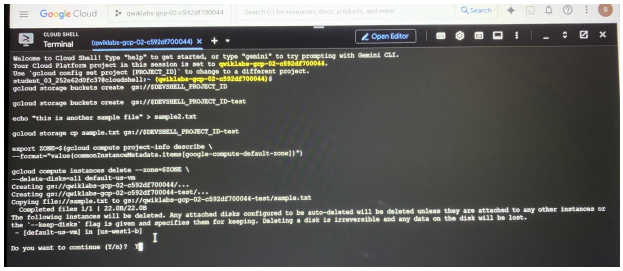



After creating an **AuditLogsExport** sink**,** all future logs will now be exported to BigQuery and the BigQuery tools can be used to perform analysis on the audit log data.

Third Step: Generate More Account Activity

Here, I created and deleted cloud resources to generate additional account activity which I'll then access in BigQuery to extract additional insights from the logs.

I inputted the following commands into the cloud shell terminal;



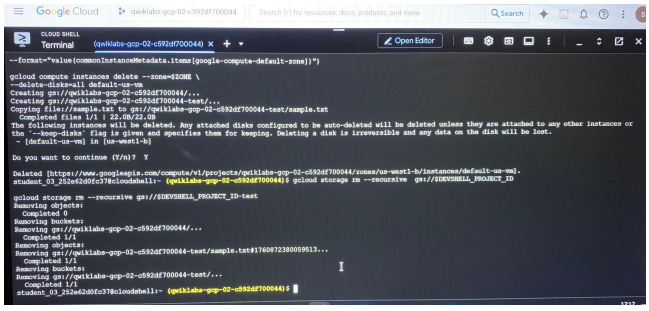
These commands generate more activity to view in the audit logs exported to BigQuery.

I was prompted to input **Y,** upon this I noticed I created two buckets and deleted a Compute Engine Instance.

When the prompt appeared after a few minutes, I continued by inputting the following commands into the cloud shell terminal.

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID

gcloud storage rm --recursive gs://$DEVSHELL_PROJECT_ID-test



With this, I deleted both buckets.

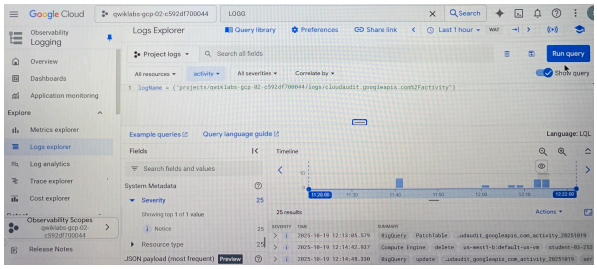
Fourth Step: Signed In As The Second User

I switched google cloud accounts by logging into the google cloud console using the second user account provided in the Lab details.

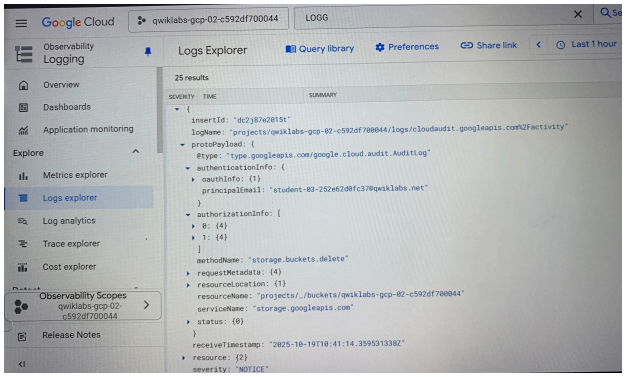
I used this account to analyze the logs.

Fifth Step: Analyze The Admin Activity Logs

Here, I'll review the admin activity logs generated in the previous step. My goal is to identify and apply filters to isolate logs that may indicate suspicious activity. This will enable me to export this subset of logs and streamline the process of analyzing them for potential issues.
I inputted the following command into the **Query builder** field;
logName = ("projects/"PROJECT_ID"/logs/cloudaudit.googleapis.com%2Factivity")

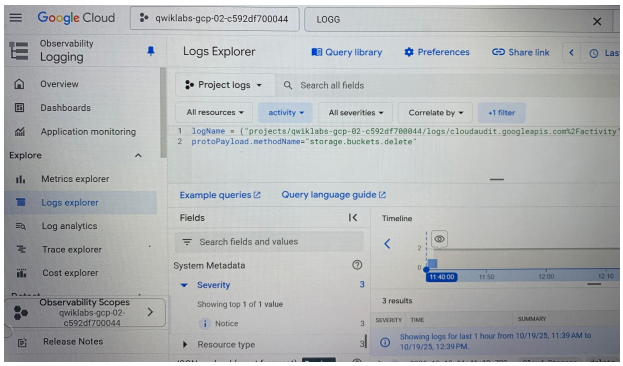


In the **Query results,** I located the entry indicating that a cloud storage bucket was deleted, it contained the **storage.bucket.delete** summary field. Summary fields are included in the log results to highlight important information about the log entry. This entry refers to **storage.googleapis.com,** which calls the **storage.buckets.delete** method to delete a bucket. The bucket name is the same name as my project : **PROJECT_ID**

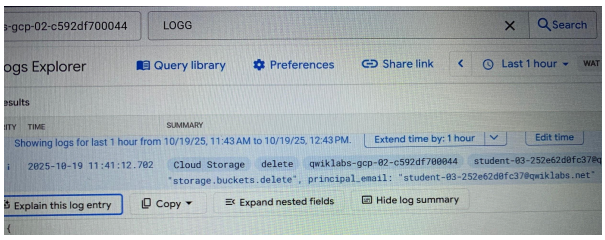


Within this entry, I clicked on the **storage.googleapis.com** text, and selected **Show matching entries**. The **Query results** now display only six entries related to **created and deleted** cloud storage buckets. In the Query editor field, I noticed the; **protoPayload.serviceName="storage.googleapis.com"** line was added to the query builder, this filters my query to entries only matching **storage.googleapis.com**. Within those query results, I clicked **storage.buckets.delete** in one of the entries, and selected

Show matching entries. I Notice another line was added to the Query builder text:

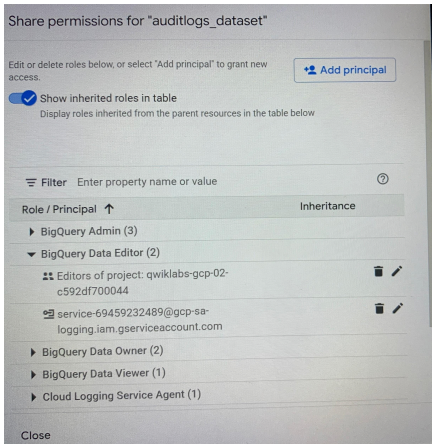


The **Query results** now display all entries related to deleted Cloud Storage buckets. I can use this technique to easily locate specific events. In the **Query results**, I expanded a **storage.buckets.delete** event and noticed the **principalEmail** field which displays the email address of the user account that performed this action which is the user 1 account I used to generate the user activity.

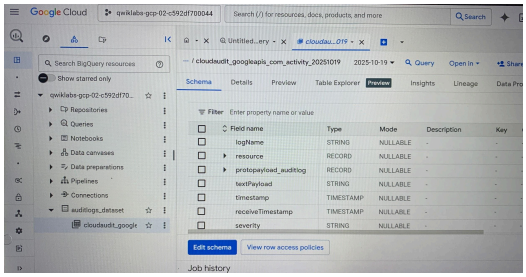


Final Step: Use BigQuery to analyze the audit log.

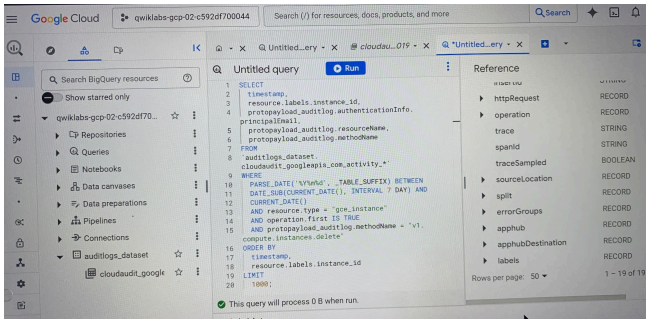
I've generated and exported logs to a BigQuery dataset. In this step, I'll analyze the logs using the Query editor. I expanded the **explorer** pane and the **auditlogs_dataset** dataset is displayed.**Next**, I verified that the BigQuery dataset has appropriate permissions to allow the export writer to store log entries.



Then, I expanded the **explorer** pane next to the **auditlogs_dataset** dataset to view the **cloudaudit_googleapis_com_acitivty** table. This table contains my exported logs. I selected the **cloudaudit_googleapis_com_acitivty** table. The table schema displays. I took a moment to review the table schema and details.



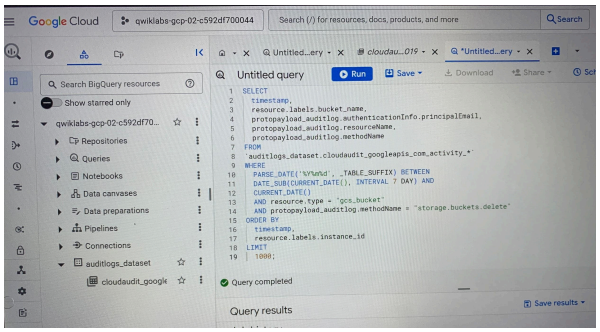
I Expanded the **Open in the drop-down** menu and selected **SQL Query > New tab**. In the **Untitled query** tab of the query builder, I deleted any existing text and inputted the following command:



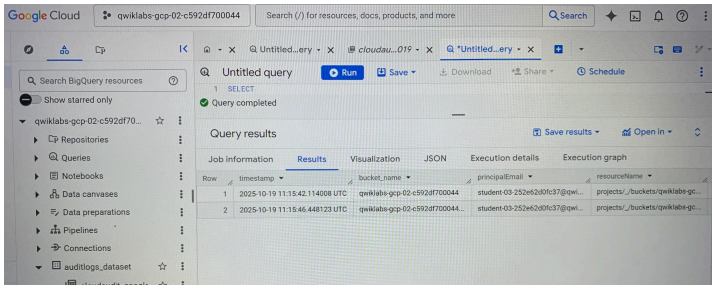
This query returns the users that deleted virtual machines in the last 7 days.

After a couple of seconds, BigQuery returns each time a user deleted a Compute Engine virtual machine within the past 7 days. I noticed one entry, which is the activity I generated in the previous steps as user 1. BigQuery shows only the activity that occurred after I created the export.

I Replaced the previous query in the **Untitled query** tab with the following:



This query returns the users that deleted Cloud Storage buckets in the last 7 days. I noticed two entries, which is the activity I generated in the previous Steps as user 1.



The ability to analyze audit logs in BigQuery is very powerful. In this lab activity, I viewed just two examples of querying audit logs.

CONCLUSION

I have successfully queried in Logs Explorer. I then exported logs and created a dataset that I analyzed in BigQuery. I have shown how I can use audit logs and filter for types of malicious activity and then further analyze those logs in BigQuery as a way to analyze the threats.