

Course 4_Lab 1: Determine the Difference Between Normal Activity and an Incident

Scenario

Recently, the security team discovered two threat findings relating to suspicious activity with user accounts. The threat findings were promptly investigated and remediated. One of the findings was determined to be benign user activity while the other finding was confirmed as malicious. Your team lead, Chloe, has tasked you with examining the details behind each finding so that you can understand the difference between normal activity and malicious activity. To do this, you'll recreate the malicious activity to trigger IAM detectors, analyze the logs associated with both threat findings, and then remediate the malicious finding.

Here's how you'll do this task: **First**, you'll grant permissions to an external account to trigger an Event Threat Detection IAM finding. **Then**, you'll use the Security Command Center to access the two IAM findings. **Next**, you'll analyze details of the findings using Security Command Center and Cloud Logging to determine which finding is benign activity and which is anomalous. **Finally**, you'll remediate the finding related to the malicious IAM activity by adjusting the IAM settings.

MY WORK:

Task 1: Grant permissions to an external account

In this lab, the focus is to determine the difference between normal activity and an incident. In this task, I granted permission to an external account in order to learn the difference.

Permissions for project "qwklabs-gcp-02-6099bdc4a14f"

These permissions affect this project and all of its resources. [Learn more](#)

☐ Include Google-provided role grants ⓘ

View by principals View by roles

[Grant access](#) [Remove access](#)

Filter Enter property name or value

Type	Principal ↑	Name	Role	Security insights ⓘ
<input type="checkbox"/>	1086529375906-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	✎
<input type="checkbox"/>	admin@qwklabs-services-prod.iam.gserviceaccount.com		Owner	✎
<input type="checkbox"/>	bad.actor.demo@gmail.com		Owner ⚠	✎
<input type="checkbox"/>	qwklabs-gcp-02-6099bdc4a14f@qwklabs-gcp-02-6099bdc4a14f.iam.gserviceaccount.com	Qwklabs User Service Account	BigQuery Admin	✎
			Owner	
			Storage Admin	
<input type="checkbox"/>	student-03-3ee5f4aa5125@qwklabs.net	student 51361000	BigQuery Admin	✎
			Logging Admin	
			Owner	
			Viewer	
<input type="checkbox"/>	student-04-01e50a5f1ccf		Owner	✎

Policy updated

Quick tip: Review the prerequisites before you run the lab

End Lab 01:26:47

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 1
student-03-3ee5f4aa5125i

Google Cloud password
9w9Dav53Pwrs

Google Cloud username 2
student-04-01e50a5f1ccf

Google Cloud project ID
qwklabs-gcp-02-6099bdc4a14f

- On the **View By Principals** tab, click **Grant Access**. The **Grant access** dialog displays.
- Under the **Add principals** section, in the **New principals** field, type **bad.actor.demo@gmail.com**.
- Expand the **Select a role** drop-down menu, select **Basic**, and then select **Owner**.
- Click **Save**.

You have now assigned the owner role to the external user bad.actor.demo@gmail.com. This will trigger a finding in SCC because this user is outside of the qwklabs.net organization.

Click **Check my progress** to verify that you have completed this task correctly.

Grant permissions to an external account

[Check my progress](#)

You have successfully completed this task.

In this task, an anomalous grant was detected with a high severity.



Quick tip: Review the prerequisites before you run the lab

End Lab 01:19:37

[Open Google Cloud console](#)

Google Cloud username 1
student-03-3ee5f4aa5125f

Google Cloud password
9e90av53Pwrs

Google Cloud username 2
student-04-01e9b5af1ccf

Google Cloud project ID
qwiklabs-gcp-02-6099bdc

- In the **Findings query results** panel, in the **Category** column, click on the **Persistence: IAM Anomalous Grant** findings record with the latest event time.
- Note the value on the **Principal email** row. This is the user account email address that granted the owner role to the user.
- Click **Source Properties** tab, and expand **properties > sensitiveRoleGrant > members**. You should notice the user account `bad.actor.demo@gmail.com`, which is an external user account. With this information, you can establish that this finding is associated with an unauthorized and malicious actor.

Which user was granted the owner role in the Persistence: IAM Anomalous Grant finding with the latest event time?

☐ None of these options

☒ The external bad.actor.demo@gmail.com user

☐ The default Compute Engine service account

☐ A student user belonging to the qwiklabs.net organization

Submit

Quick tip: Review the prerequisites before you run the lab

End Lab 01:18:59

[Open Google Cloud console](#)

Google Cloud username 1
student-03-3ee5f4aa5125f

Google Cloud password
Dav53Pwrs

Google Cloud username 2
student-04-01e9b5af1ccf

Quick tip: Review the prerequisites before you run the lab

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

Which Persistence: IAM Anomalous Grant finding is a genuine incident?

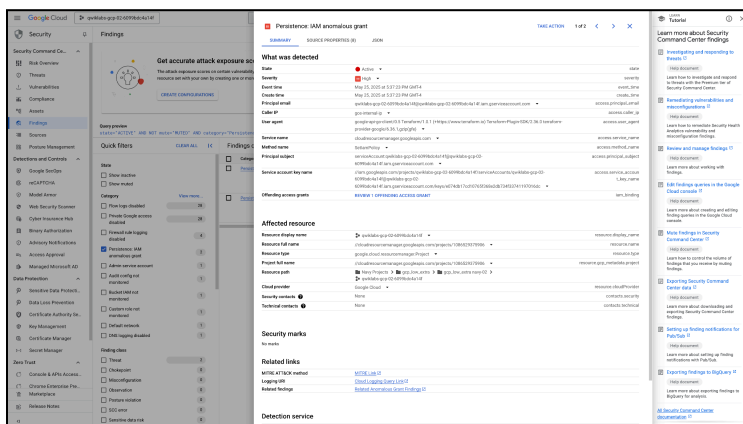
☐ None of these options

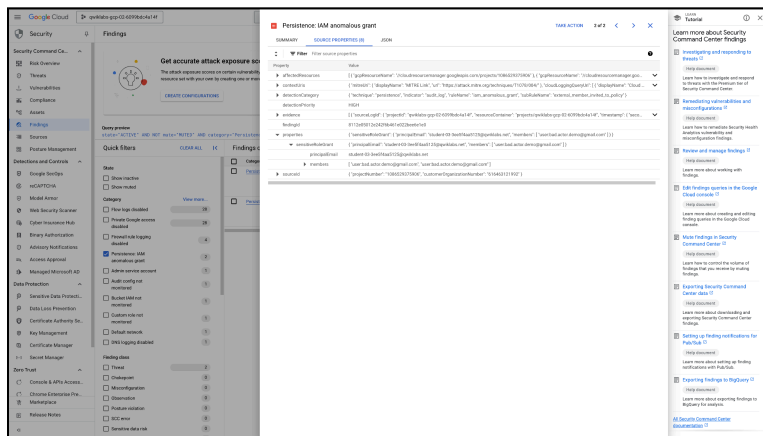
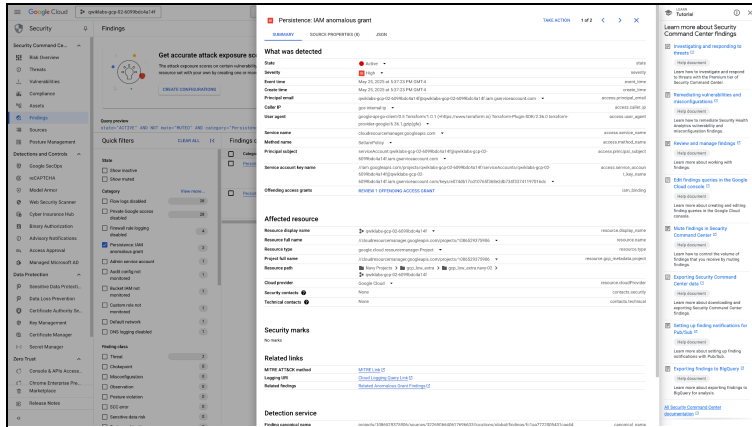
☒ The finding with the latest event time

☐ The finding with the earlier event time

☐ Both findings are genuine incidents

Submit





Task 4: Access the findings in Cloud Logging

In this task, I was able to use Logs Explorer and run a query to determine who granted access to the suspicious user.

Quick tip: Review the prerequisites before you run the lab

End Lab **01:14:06**

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 1
student-83-3ee5f4aa5125i

Google Cloud password
9w9Dav53PWRs

Google Cloud username 2
student-04-01e58a5f1cef1

Google Cloud project ID
qwiklabs-gcp-02-6099bdcv

You can now examine the details of the anomalous request event including information such as:

- authenticationInfo:** The email of the user who made the request.
- request:** The email identity of the user the anomalous grant was made to.
- request Metadata:** The IP address of the system where the request was made, the browser user agent of the web browser that was used.

This information can be vital when investigating whether an event is normal activity or an actual threat event.

Which user account made the request to grant the project owner role to the bad.actor@gmail.com user?

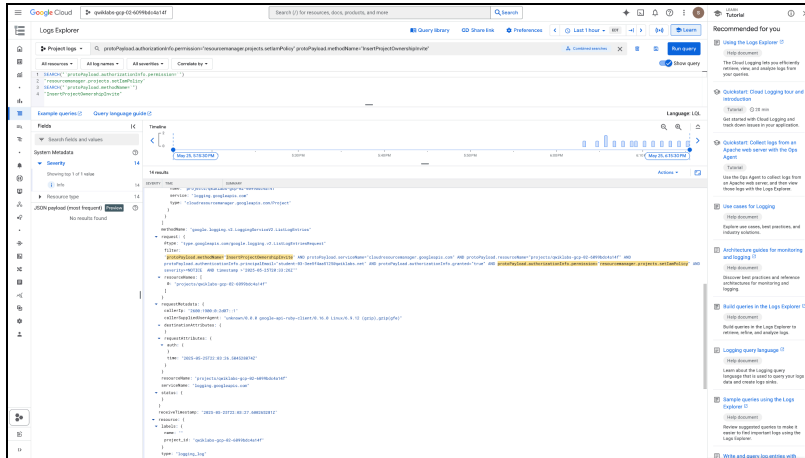
☐ An external@gmail.com account

☐ A Google Cloud IAM service account

☐ None of these options

☒ A student user belonging to the qwiklabs.net organization

[Submit](#)



Task 5: Fix the finding

To fix the finding, I deleted the permission in the IAM tab connected to the external account.

Quick tip: Review the prerequisites before you run the lab

End Lab **01:12:41**

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 1
student-03-3ee5f4aa5125f

Google Cloud password
9w9Dav53PWrs

Google Cloud username 2
student-04-01e50a5f1ccfi

Google Cloud project ID
qwiklabs-gcp-02-6899bdcv

In this task, you'll remediate the malicious **Persistence: IAM Anomalous Grant** finding by removing the project owner role that you had previously assigned to the external user.

1. In the Google Cloud console, in the **Navigation menu** (☰), click **IAM & Admin** > **IAM**. The **IAM** page opens.
2. Next to the **bad.actor.demo@gmail.com** user, click the **Edit principal** (✎) icon. The **Edit permissions** page opens.
3. Click the **Delete** (🗑️) icon to delete the owner role.
4. Click **Save**.

The policy will be updated, and the owner role removed from the bad.actor.demo@gmail.com user.

Click **Check my progress** to verify that you have completed this task correctly.

Fix the finding

[Check my progress](#)

You have successfully completed this task.

My Assessment

Knowing the difference between normal activity and an incident was the focus for this lab. There are a number of ways to determine if activity isn't normal and possibly an incident, such as, as suspicious logins during irregular hours and locations. Another way to detect abnormal activity is multiple login attempts from the same user or a successful login from a user in a location where they are not actually present.